

**WHAT'S THAT NOISE?
OR, A CASE AGAINST DIGITAL PRIVACY AS A MATTER
OF REGULATION AND CONTROL**

THOMAS N. COOKE

**A DISSERTATION SUBMITTED TO
THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY**

**GRADUATE PROGRAM IN COMMUNICATION & CULTURE
YORK UNIVERSITY
TORONTO, ONTARIO**

AUGUST 2017

© THOMAS N. COOKE, 2017

ABSTRACT

Digital privacy is typically understood as the restriction of access to personal information and user data. This assumes *regulation* and *control* on the part of governments and corporations, realized through various laws and policies. However, there exists another realm bearing on digital privacy. This realm involves a wider network of actors carrying out practices and techniques beyond merely governmental and corporate means: *users* who engage and manipulate digital privacy software that is created by *coders*, as well as *the software itself* for the ways in which it mediates the relationship between *users* and *coders*. The dissertation argues that by focusing attention on this other realm – of coders, users and software interacting with one another – we as analysts develop alternative understandings of digital privacy, specifically by attending to each actor’s *noisemaking*: the deliberate (or even incidental) process of obfuscating, interrupting, precluding, confusing or misleading access to digital information. The dissertation analyzes how each of these three actors engage in noisemaking across three different types of encrypted Internet systems: *The Onion Router* web browser; the *WhatsApp* instant messaging service; the *SpiderOak One* file hosting service. These relatively taken-for-granted actors instruct the academy that digital privacy is less about *regulating* and *controlling* information as much as it is about *surrendering* control over information management and security. The dissertation demonstrates that digital privacy thus ought to be understood as a reflection of the variegated, contingent and incidental nature of social and political forces unfolding at the edge of – and even beyond – the purview of governments and corporations.

DEDICATIONS

To my late grandparents: Norman Bonnell, Thomas Cooke and Vera Cooke,

Your love encourages me to pursue my dreams. I miss you, dearly.

To my brother: Riley,

TOUCHDOWN!

I quite literally could not get to this point without you.

You've always been there for me, especially when I was at my worst.

You're a game changer, man. Thank you for being you.

To my loving parents: Cindy and Tom Sr.,

The two of you have been endlessly supportive.

I can't properly express how deeply touched I am by your continued belief in my abilities.

Perhaps now I can expand upon those abilities, get a real job and pay you back.

I used your credit card to print 30 copies of the project. Beans ate 27 of them.

To my beautiful partner: Cristina,

Thank you for being my homing beacon. Thank you for listening to me jabber endlessly.

Thank you for making me stronger physically, emotionally, mentally and mindfully.

Just before handing in my dissertation,

I submitted ten of our favourite puns to a local newspaper pun contest, hoping one would win.

Unfortunately, no pun in ten did.

ACKNOWLEDGEMENTS

First and foremost, to my supervisor, Robert Latham. Robert, since day one you have gone well beyond the call of duty. You have invested countless phone hours and keystrokes into guiding, shaping and advising me. This project is not only a reflection of your wisdom, but also your exceptionally positive influence. Thank you for pushing me, harder than anyone has, to grow. Thank you for really showing me the value of theory and critique. Thank you for teaching me how to signpost, for teaching me how to engage the world reflexively and for teaching me how to navigate any and all hurdles with an unyieldingly productive embrace. Thank you for taking me under your wing and truly being a world class mentor. I will only begin to appreciate the magnitude of your impression in the years to come. I am eternally grateful.

Thank you, Edward Jones-Imhotep. You have been on this ride – enthusiastically and graciously – since day one. You were the first person I met and worked with at York, and you set the bar very, very high – not only through your brilliance and commitment, but also through your first-rate attitude and kindness. When I left STS, I never thought so much of my project would come back to STS. I am so very grateful that this project has thus come ‘round full circle, and much of that is owed to your infectious passion for our subject matter. Your demeanour and professionalism are unrivaled and incredibly inspiring. And thank you for teaching me that chairs can kill. I may have borrowed this for my own lectures at UWO. Will probably happen again.

To Jan Hadlaw, thank you for teaching me to squint. I can’t tell you how useful this has been – throughout my course work, my comprehensive exams, my lecturing, my radio work and this project. Your ability to ground massive abstractions during our seminars together really fueled my passion for theory. Your seminar was the first place I felt truly confident as a young scholar, and for that I will always be grateful. I also owe you a big thanks for showing me how to build fruitful connections between Communications Studies and the Sociology and History of Technology. Thank you for your wisdom and wonderful teachings, Jan.

To Benjamin Muller. There is not enough room here to express my gratitude. I have already re-written this entry twice. It is impossible to communicate how much of a role you have played in my development. But what I can communicate with certainty is that graduate school was impossible without you. You identified something in me that I didn’t know I had, even when I was trolling your senior undergraduate seminars with half-hearted effort. Throughout my MA, my PhD, my teaching, my networking and my personal life – as a mentor, teacher, role model, colleague and best friend – you have been there every step of the way, as has been your beautiful family. You really need to start wearing a cape, my friend.

To Athina Karatzogianna, David Cecchetto and Steven Bailey – thank you so much for being on the committee. To the professionals who restored my mind after two head injuries this past year – Nicole, Brad, Joanne, Dr. Sargo and Dr. Svec – thank you. To Raffi and Tree, thanks so very much for your patience! To Gabriel and Nettie Ionituiu, thank you so very much! Eash, Daru, Anthony, Tina, Cami, Chris, Nathan, Danial, Victor, Gbenga and Jimmy <3. To David Grondin, Samer Abboud, Mark Salter, Xavier Guillaume, Marc Doucet, Can “Big Society” Mutlu, Miguel de Larrinaga, Philippe Frowd and Jen Mustapha – you are my heroes. Noe Cornago, David Wellman, Frédéric Ramel and my dear friend Sophia Dingli – you are inspirational. Al Coombs, Mike Stubbs, Nick Chenosky, Carmi Levy – I adore you. Z, Carol and Tom H., Richie G., Dano M., Shelver, James B., A.T. Kingsmith, Karl P., Chris McInerney, Jad Ayoub, Jason and Mikey Chan, Caley Suds, Will J., Stevey J., Julian V.B. – thank you so much! Guy, Cathy, Emmo, Jode, Dan, Tyler, Orla, Kodie, T.T., Jazzdee and Spanman – love you guys!

TABLE OF CONTENTS

Abstract.....	ii
Dedications.....	iii
Acknowledgements.....	iv
Table of Contents.....	v
List of Tables.....	vii
List of Illustrations.....	viii
Chapter One: Introduction.....	1
Theoretical Framework.....	8
Methodological Framework.....	22
Outline.....	33
Chapter Two: Literature Review.....	35
Part One: Overarching Argument.....	35
Part Two: Historical & Contemporary Privacy-Oriented Literature.....	38
Part Three: Noise-Oriented Literature.....	54
Part Four: Michel Serres – <i>Parasite</i>	67
Part Five: Gaps.....	71
Part Six: Conclusion.....	75
Chapter Three: Case Study One – <i>The Onion Router</i> (Tor).....	77
Part One: Tor, at a glance.....	78
Part Two: Users, Coders and Software Making Noise.....	84
Part Three: Tor as a Socio-Technical System.....	105
Part Four: Conclusion.....	111
Chapter Four: Case Study Two – <i>WhatsApp</i>	115
Part One: <i>WhatsApp</i> , at a glance.....	117
Part Two: Users, Coders and Software Making Noise.....	121
Part Three: <i>WhatsApp</i> as a Socio-Technical System.....	136
Part Four: Conclusion.....	145
Chapter Five: Case Study Three – <i>SpiderOak One</i>	151
Part One: <i>SpiderOak One</i> , at a glance.....	154
Part Two: Users, Coders and Software Making Noise.....	158
Part Three: <i>SpiderOak One</i> as a Socio-Technical System.....	176
Part Four: Conclusion.....	182
Chapter Six: Case Study Comparison.....	188
Noises.....	188
Socio-Technical Systems.....	198
Digital Privacy.....	204

TABLE OF CONTENTS

Chapter Seven: Conclusion.....	214
Contributions	218
 Bibliography	 226
 Appendices.....	 244
Appendix A: Tor Anonymity Protocol Vulnerability Disclaimer	244
Appendix B: Tor User Browsing Habit Warning.....	245
Appendix C: Tor Browser Startpage.....	246
Appendix D: Tor Browser Security Setting – Low.....	247
Appendix E: Tor Browser Security Setting – Medium.....	248
Appendix F: Tor Browser Security Setting – High.....	249
Appendix G: <i>WhatsApp</i> ‘Encryption by Default’ Advertisement.....	250
Appendix H: <i>WhatsApp</i> Mobile ‘App’ Settings Menu.....	251
Appendix I: <i>WhatsApp</i> Mobile ‘App’ Privacy Settings Submenu.....	252
Appendix J: <i>WhatsApp</i> Mobile ‘App’ Message Status System.....	253
Appendix K: ‘ <i>WikiHow</i> ’ – ‘How to Know if Someone Has Blocked You’.....	254
Appendix L: <i>SpiderOak One</i> Version 3; Multiplatform Synchronization.....	255
Appendix M: <i>SpiderOak One</i> Version 1.0; Original Release, 2007.....	256
Appendix N: <i>DropBox</i> File Synchronization Status System.....	257

LIST OF TABLES

Table One: Most Visited Websites on Tor.....	97
Table Two: Application Usage on Tor.....	97

LIST OF ILLUSTRATIONS

Illustration One: How Tor Works.....100

Chapter One: Introduction

Digital privacy is typically understood as the restriction of access to personal information and user data. This assumes *regulation* and *control* on the part of governments and corporations, realized through various laws and policies. However, there exists another realm bearing on digital privacy. This realm involves a wider network of actors carrying out practices and techniques beyond merely governmental and corporate means: *users* who engage and manipulate digital privacy software that is created by *coders*, as well as *the software itself* for the ways in which it mediates the relationship between *users* and *coders*. The dissertation argues that by focusing attention on this other realm – of coders, users and software interacting with one another – we as analysts develop alternative understandings of digital privacy, specifically by attending to each actor's *noisemaking*: the deliberate (or even incidental) process of obfuscating, interrupting, precluding, confusing or misleading access to digital information. The dissertation analyzes how each of these three actors engage in noisemaking across three different types of encrypted Internet systems: *The Onion Router* web browser; the *WhatsApp* instant messaging service; the *SpiderOak One* file hosting service. These relatively taken-for-granted actors instruct the academy that digital privacy is less about *regulating* and *controlling* information as much as it is about *surrendering* control over information management and security. The dissertation demonstrates that digital privacy thus ought to be understood as a reflection of the variegated, contingent and incidental nature of social and political forces unfolding at the edge of – and even beyond – the purview of governments and corporations.

Focusing upon the noisemaking capacity of each actor – *users*, *coders* and *software* – the dissertation encourages increased empirical and methodological consideration of the consequences and by-products of seemingly infinitesimal social developments in and around

popular Internet-based communications, browsing and file storage systems. These consequences and by-products can be categorized in two ways. The first is the way in which the noise¹ each actor makes affects how other actors understand, behave and relate to themselves and one another. Like the way in which an Internet user installs ‘plug-ins’ designed to confuse hackers and tracking mechanisms from determining her location in the world. The user here makes, or emits, ‘noise’ – she extends her own privacy by introducing an element of confusion into anyone or anything’s attempt to correlate her browsing location with her browsing behaviour. But noisemaking and noise itself do not exist in a vacuum. Noisemaking and noise also affect the way in which a browser’s coders perceive users’ browsing preferences. This in turn affects how coders understand and manage information.

The second category of consequence and by-product is how noises, and noisemaking activities themselves, *clash* or *coalesce* with other noises and noisemaking activities. For example, even if users install their own browser ‘plug-ins’ to enhance their own privacy, the process can inadvertently render the location protection mechanism (i.e. a piece of coding that randomly distributes the information leaving a user’s computer in order to prevent hackers from deducing their origin) embedded inside the software itself from working. As discussed in the case on *The Onion Router*, some users developed a habit of introducing ‘extra’ privacy enhancing ‘plug-ins’ despite the company telling users that using ‘plug-ins’ could create a conflict within the programming of the software itself. This would essentially render the software incapable of effectively hiding the user’s browsing location. It is a *clash* of noises in the sense

¹ The project does not engage a comprehensive review of the meaning of ‘noise’. Rather, the dissertation deploys and understands ‘noise’ vis-à-vis Serres’ (1982) *Parasite*. The reasons for which are articulated further on page seven. ‘Noise’ here refers to the condition and status of access, legibility and discernibility of digital content information. The project renders ‘noise’ as a byproduct of social actions waged by actors in an attempt to obfuscate, interrupt, conceal, prevent or distract other actors from controlling and regulating any data that is perceived to be ‘personal’ or ‘private’.

that both the user and the software are attempting to hide the user's location, alas their efforts essentially 'cancel' one another out. In this particular scenario, we observe that coders working on *The Onion Router* purposely program the software to ignore many of the 'plug-ins' users install because the coder believes many 'plug-ins' conflict with *The Onion Router's* encryption protocols. It is not merely the case that the coder is punishing the user, but rather that they are making a decision *for the user* – one that they feel more effectively and efficiently enhances their privacy. And so, by preventing the usage of such 'plug-ins', we observe that the coder is essentially making noise as well – a decision to intervene upon users' plug-in-oriented noisemaking. As these noises intersect, they clash. This clash has implications. As the case study on *The Onion Router* discusses, some users to continue finding alternative 'plug-ins' – a pursuit that perpetuates coder intervention. In other cases, we see that the perpetuation compels many users to simply give up their pursuit.

What is particularly important about the way in which noises clash or coalesce is how this clashing and coalescing signals a difference in our perception of digital privacy. The coder and user prioritize, value and understand digital privacy in very different ways. To us as analysts, the empirical endeavour of tracking each actor's noisemaking activity constellates a way of conceptualizing the 'how' and 'what' of digital privacy in excess of and beyond the realm of corporate and governmental policymaking. Noisemaking reveals that digital privacy also exists in a realm constituted by numerous layers of tension and negotiation between various different actors.

Noisemaking also reveals to us as analysts that digital privacy must be understood through the inextricability of 'technical' and 'social' processes. As noise emits across each system, we begin to understand as analysts that each privacy network cannot be reduced to the

merely computational processes, such as End-to-End encryption programming. Rather, we understand that noisemaking makes legible the how intimately imbricated social processes are with technical processes. For example, like the way in which many of Tor's users prefer 'plugins', they can – at times and in particular circumstances – make the software's encryption protocols work more efficiently. But they can also make the software fail entirely. Whether the software 'works' or 'fails' is case specific. This case specificity reflects not only technical considerations, but also details of where the user is heading online, what she is doing and how she is doing it. These details are not merely a reflection of technical details. They are a reflection of the user's preferences and habits, and her subsequent awareness and willingness to change her behaviour in light of the software's technical constraints. The question of improving privacy in this case, so to speak, thus compels analytical consideration of both technical and social dynamics around software design and user cognition together. And from this observation, we as analysts are able to abstract our analyses to 'bigger picture' considerations of the stakes of digital privacy on Tor. The 'how' and 'what' of digital privacy begins demanding consideration of systemic-level phenomena such as collective user awareness, coding cultures and so on. Our methodological orientation shifts accordingly, so much so that we begin attending to digital privacy as *socio-technical* systems.²

Throughout each case study, each actor's noisemaking activities are identified and discussed. They are then intersected as systems, socio-technical systems to be precise – ones that are inextricably social and technical in nature. And from these socio-technical systems, each case

² The term 'socio-technical system' (also stylized as 'sociotechnical'), frequently deployed in the fields of the history of science, the history of technology, the sociology of science and the sociology of technology, refers to the simultaneously 'social' and 'technical' dimension of systems that may otherwise be considered essentially 'technical'. The term is particularly important to the purpose of the dissertation because it compels critical consideration of how, for example, an air transportation system includes airplanes, airports and flight control towers as much as it does personnel to manage and maintain said system. See Wiebe E., Hughes, Thomas P. and Trevor Pinch's *The Social Construction of Technological Systems* (1993).

study offers alternative understandings about digital privacy. Understandings that reveal how the outcome of digital privacy is as much about the *surrender* of information management to interests, actions and desires of actors outside the purview of governmental control. In some cases, such as *WhatsApp*, we see that the company who owns it (*Facebook*) retains a tremendous amount of control over information flow. They regulate and oversee much of the technical *and* social developments within the network. From this observation, we learn that a different modality of digital privacy emerges therein, one that escapes conventional analyses of such networks as merely reflections of technical and legislative parameters. This is one of the many contributions that the dissertation makes upon the study of privacy.

The dissertation also raises the stakes for several fields of study. For privacy policy analysts within Communications Studies, Political Studies and even Legal Studies, the dissertation implies that approaching ‘digital privacy’ as the sole preoccupation of governmental and corporate preoccupation valorizes and reifies normative³ modalities of privacy diagnosis and prescription. For example, while Tor’s coders stipulate that ‘digital privacy’ is a reflection of ‘onion routing’ technical processes that take place outside of the purview and concern of the user herself, the dissertation’s case studies reveal that users create their own noise in the name of their own privacy. This noisemaking directly affects how and whether many users not only experience privacy itself or whether many users are able to visit certain websites, this noisemaking affects how we as analysts develop and carry out our empirical duties. Once we make legible individual users’ noisemaking processes, we acknowledge the extents to which digital privacy is *also* constitutive of user experimentation, concern and preference.

³ The usage of ‘normative’ in the dissertation is derived from political philosophy in general and the fields of International Relations and International Political Sociology in particular. The term is used throughout the dissertation to identify and classify academic orientations, frameworks and arguments that tend to evaluate their subject and object matter via value judgements. For example, in terms of what is perceived as ‘good’ versus ‘bad’.

The stakes for computer programmers and information security analysts with the fields of Computer Science and Cryptography are as equally high. As discussed in the dissertation's literature review, many Computer Science approaches to digital privacy offer 'definitional' perspectives that are highly dependent upon ontological assumptions about who and what is responsible for participating in and design digital privacy. The case study on Tor demonstrates that many users do not use Tor the way it was intended. In fact, numerous academic studies reveal that the majority of Tor's network traffic is done off of the so-called 'Internet' and on what is popularly referred to as the *Deep Web*: a realm of websites and corresponding addresses that are not accessible nor registered on the World Wide Web. The majority of the websites visited on Tor are illegal websites, which tend to offer Black Market services such as human smuggling. How Tor conceals users' location and encrypts their information functions very differently in the Deep Web than the World Wide Web. How users switch between each realm when using Tor changes how and whether these encryption processes work altogether. Some users switch covertly and for nefarious purposes. Others switch out of curiosity, and for research purposes. Some users purposely switch to hide within illegal traffic flows in order to manipulate Tor's encryption process in order to make it more reliable. Computer Science approaches to digital privacy on Tor tend not to consider the variability and degree of change in user behaviour as factors in user privacy. As such, there is a distinct gap between computational understandings of digital privacy on Tor and user-designed/user-experienced understandings of digital privacy on Tor. Accordingly, the dissertation encourages Computer Sciences approaches to digital privacy to become more interdisciplinary, specifically so as to close the gap between scientific and social perspectives, expectations and experiences with digital privacy.

The largest contribution the dissertation makes upon how we as analysts think about digital privacy is to create awareness about the gap between policy-oriented understandings of digital privacy with digital privacy ‘in the wild’ or ‘as it happens’, so to speak. Or perhaps more simply, we as analysts cannot afford to approach digital privacy as a matter of controlling and securing information flow. Each case study demonstrates, rather conversely, that much information flow is not controllable whatsoever. When we attend to the network of relations between actors (such as the coders, the users and the software itself), in terms of the noises each actor makes, we see that each network has momentum (Hughes, 1987). Each network, or socio-technical system, shrinks and grows. They regress and progress. But never one without the other. Systems do not merely stand still or exist in permanence. They are constantly undergoing changes. Although many of those changes are minuscule, they are not meaningless. Small changes are markers of slow but eventual systemic change. When user tolerance for software problems decreases, and coders’ desire to implement gradual changes in the software’s receptivity of changes in user expectation, we can reasonably identify the creation of socio-technical norms that are mutually expressed between two entirely different groups of actors. The coalescing of these efforts can dramatically change the nature of experience for both groups, and dimensions of digital privacy in tandem. We thus also learn as analysts that these socio-technical dynamics are different in every system we analyze. Part of the goal of the dissertation is thus to demonstrate that digital privacy – from system to system – is highly differentiated in shape, evolution, content, direction, design, purpose and influence. Our understandings of digital privacy, from case to case, are variegated and as such, never the same. And in order to arrive at such differentiated ways of accounting, the dissertation builds an adaptive theoretical framework.

Theoretical Framework

The dissertation's theoretical framework is derived from seven sources. The primary source is Serres' (1982) *Parasite*. It offers logics about the effect of socially produced noise – particularly upon social systems. His work does not consider contemporary contexts and so Lundblad's (2004), Bolton (2013) and Paddison, Philo, Routledge and Sharp (2000) assist accordingly. The fifth, sixth and seventh sources are derived from the field of Science and Technology Studies (STS), as such adding three crucial theoretical elements. The first is Latour (2007) vis-à-vis Actor-Network Theory to aide in situating privacy technologies themselves as actors in the digital privacy process. The second is vis-à-vis Oodshorn and Pinch's (2005) *How Users Matter: The Co-Construction of Users and Technology* for the ways in which it assists in describing how user action and agency, and ultimately noisemaking, plays an intimate role in not only the behavior and outcome of the systems they interact with, but also for the role they play in the outcome of digital privacy altogether. The third is Pinch, Bijker and Hughes' (Eds.) *The Social Construction of Socio-Technical Systems: New Directions in the History and Sociology of Science and Technology* (1993), for the ways in which it weds together all actors' noisemaking activities within a larger-scale context of analysis, specifically as socio-technical systems.

Beginning with Serres, his work contributes a logic about social life: all social beings make noise through their actions and interactions. Serres is not merely referring to the sound somebody makes when they shuffle their feet. Nor is he referring merely to physical phenomena. Serres more generally argues that *any* and *all* social activity – including conversation and interaction – affects how objects and people relate to and experience themselves, others and the spaces around them. The consequence of social activity is what Serres refers to as *noise*. For example, by knocking on a door during dinner, the visitor's physical act of 'knocking' interrupts

the dinner. The sound of the knock thus also signals that the conversation over the dinner table will invariably change due to the potential that visitor will join the dinner table or converse with the diners if only for a moment. But the sound of the knock to Serres is also a type of information – a signal to the diners that something or someone else requires their attention. And so, Serres' notion of noise is not merely reduced to a physical action for it inextricably refers to the series of ideological effects the physical activity creates as well. What Serres also contributes to the dissertation is thus a logic about how noise can create social systems and/or affect existing social systems as well.

When any actor makes noise, that noise interrupts existing relations. For example, imagine two actors represented as dots on a sheet of paper. They have a relationship to one another, which is represented by a line connecting the dots together. When a noise is made, it comes from an actor outside of this relationship between the two original dots. A new dot appears on the page. It is the source of the noise. This third dot, or noisemaker, forces herself into the already-existing relationship on the page. A line is drawn from the third dot, and intersects the line representing the relationship between the other two dots. A triangulation is created, a relationship between three actors now exists. But that noisemaker has a unique and disproportionate opportunity to influence the triangulation. She can simply observe it. She can slightly alter it. She can interrupt message flow. She can destroy the system she has created or even make it stronger. The position of this noisemaker is particularly important to Serres because it highlights the social effect of noise. This is particularly recognizable when we as analysts conclude that the previously existing relationship – of two dots and one line, an otherwise isolated relationship – can never be the same. A new social system, so to speak, emerges (Serres, 1982, 4-5). And so, when extrapolated into an analysis of social systems themselves, the logic

becomes elucidating when thinking about, for example, digital social systems.

Messages are sent and received. Relations are established between stations. They grow, they expand and they multiply. New pathways expand structure. These systems are characterized by their flow, which also means that these flows are subject to changes, metamorphosis and degradation. As a message passes, parasites can prevent it from being heard, or they can make the process of receiving, interpreting and sending more efficient to the benefit of some while at the cost or detriment of others. Parasites intercept flow. Perhaps most importantly, Serres' theory infers that systems *are never static*. They are constantly reverberating at different frequencies (Serres, 1982, 14). As systems oscillate and reverberate, they constantly undergo change. To connect Serres' work in contemporary, digital examples such as digital privacy, three pieces of literature are particularly important: Lundblad's "Privacy in a Noise Society" (2004), which brings together privacy and noise in a digital context; Bolton's "Digital Parasites: Reassessing Notions of Autonomy and Agency in Posthuman Subjectivity" (2013), which uses Serres' notion of the noisemaking parasite as a metaphor for the ways in which humans create structures of affect and meaning on their own terms; Paddison, Philo, Routledge and Sharp's *Entanglements of Power: Geographies of Domination/Resistance* (2000), which argues vis-à-vis Serres that humans make noise online in ways that create and extend social systems.

Lundblad's "Privacy in a Noise Society" (2004) weds privacy and noise together in a contemporary digital context on two different registers. The first conceptualizes the Internet itself as an exceptionally noisy environment due to the ubiquitous nature of data information volume and flow. Lundblad points towards two developments worth noting. First, of the ways in which the excess creation and collection of information threatens digital privacy by eroding ambiguity about the details of an Internet user's behavior, including shopping, travel,

professional and hobby preferences. The notion itself is not isolated to Lundblad's mind. Noise is often used to characterize the abundance of information across the Internet in numerous contexts. For example, feminist analysis of the deployment of methods used to counteract terrorism recruitment efforts online point towards the deliberate usage of noisemaking mechanisms (Aly, Weimann-Saks and Weimann, 2014). Other scholars point towards government surveillance preoccupations as sources of noise for the ways in which they interfere with the flow of data (Schneier, 2016). Tumarkin and Whitelaw (2001) point towards social media itself as noisemakers, while Takasyu, Takaysu and Sato (1996) argued that the Internet itself was and always is 'noisy'. The point being that the idea of 'noise' on the Internet is not novel. But where Lundblad contributes differently is at the moment where the abundance of data produced as a consequence of the corporate pursuit of data recursively increases the costs of surveillance. He argues that the more data created and collected, the more technological imperatives are believed necessary in order to continue eroding layers of informational obfuscation around the lived experience of the Internet user.

Lundblad also points towards the transformation of noise into a collective agential capacity for all Internet users, dubbed the *noise effect*. The noise effect denotes how the collective expectation and experience of digital privacy increases due to the mounting, encumbering nature of Internet tracking. Lundblad is the first here to contribute to a way of thinking about the Internet that systemically identifies it as inherently noisy. How Internet users engage and experience the Internet is inescapably fraught with mechanisms that bind to the user and her technology, making digital privacy a competition with forces she cannot so obviously circumnavigate. The noise is here to stay, and it is a problem for digital privacy. The issue with Lundblad's work is that it raises the question, to what extent is noise agential? To what extents

can noise be harnessed beyond the noise effect? The implication with his notion of the noise effect is that it engenders a limitation on who and what creates digital privacy. In this case, noise encumbers trackers and their tracking technologies. The logic abandons, and quite explicitly, the capacity of Internet users to engage digital privacy for themselves. The issue is collective, but their involvement is reduced to an almost entirely docile ontology. Through Lundblad, noise as the outcome of social activities, expressions and interactions plays a fundamental role in the structuring of digital privacy. With the aid of Bolton, as well as Paddison, Philo, Routledge and Sharp, Serres' ideas about noise galvanize in a contemporary, digital context.

Bolton's (2013) work expands Serres' ideas into online considerations specifically by wedding Serres' social systems theory with Hayles' work on post-human⁴ subjectivity. The connection opens way to an ontological imagination where digital social systems maintain their existence through *parasitic autopoiesis*: a socio-technical process through which digital actors produce meaning, affect and agency through their actions and behaviour. The notion of the 'parasite' is drawn upon by Bolton through Serres' *Parasite* to emphasize how user behavior online 'infects' digital spaces and structures that corporations and governments maintain online – a way of demonstrating that user activity online is not merely a byproduct of corporate or governmental design, but rather that user activity itself indeed creates meaningful effect and change online. Bolton's ideas are dovetailed by Paddison, Philo, Routledge and Sharp (2000) in arguing that meaningful political change on the Internet happens as a digital noisemaking activity that is dependent entirely upon the co-production between users online. New conditions

⁴ 'Post-human' is used within various fields within the Humanities and Social Sciences in general, but within academic works that tend to identify and subscribe to postmodern logics and philosophies. 'Post-human' is an ontological category which questions the status, condition, embodiment and position of the 'human'. It imagines humans as existing beyond biological considerations, into technical, digital, literary, constructed, imaginative and conceptual considerations. It is important for the dissertation because it assists in theorizing how the capacity for human action exists beyond the physical location of a 'user', for example.

for change between actors tend to occur most acutely in the *gaps* between digital relationships. The power of the parasite (of users, coders and technologies themselves) online, so to speak, is the way their activities reverberate into uncharted spaces between actors and networks – a process that invariably creates new nodes, new channels and new relations. Internet users, coders and software technologies are indeed theorized throughout the dissertation akin to Serres’ parasites, but it is important to note that the dissertation’s brand of noise is a departure from Serres’ brand. This is because of the seemingly unavoidable normative trap *Parasite* tends to encounter. While Serres’ parasites indeed affect social structures, his parasites tend to collapse them or spell their demise.

Parasites are not merely destructive, as they are crucial to the functioning and health of the human body and living ecosystems. Without parasites, equilibrium is impossible; bodies cannot survive in completely sterile environments because the immune system will simply attack itself (Adler, F. R. & M. Kretschmar, 1991, 199). Users, coders and the software systems under consideration parasite existing Internet relations in order to provide digital privacy because digital privacy is not merely a law or policy. They do it because law and policy do not guarantee privacy. It needs to be played out by other actors and on different terms. We as analysts generally recognize that digital privacy is important to these actors, for it is an important dimension of modern Western lived experience. But the dissertation also acknowledges that the playing out of privacy – whether from a top-down or bottom-up perspective – is problematic. Privacy protects information, enables political expression and space for growth and self-reflection. But it also impedes corporate pursuits of profit and governmental pursuits of information via surveillance. The point is that actors, as noisemaking parasites, can make noise (for example, in the name of privacy) beyond merely negative means. Those means can also be

as productive as they are problematic.

Moreover, and as importantly, not all parasites are successful. Parasites can fail to infect a host, even once in the body (Johnson et al., 2003). At other times, parasites ‘stand down’ when they recognize that the probability of their infective capacity is diminished by the presence of other parasites (Hafer and Milinski, 2014). Noisemakers can be parasitic, but do not always become ‘parasites’. Serres recognizes that context – such as systems of constraint or the presence of competing social actors/parasites – is an important determinant as to whether or not a noise influences change on systemic levels (Serres, 1989, 83). Accordingly, and as we will see throughout the dissertation, users attempt to make noise so as to infect a system. The goal for these users is to influence change in a more favorable vision of privacy. We will also see that the coders and software of *WhatsApp* make noise that coalesce together. This coalescing drowns out the noise WhatsApp users make, effectively negating their own noisemaking/attempt to (re)claim privacy in their own vision. Noisemaking is indeed a social activity, with varying degrees of success, failure, change or otherwise. As such, noisemaking often relies upon cooperation and co-optation with other actors. These other actors may have more influence over one another in the context of noisemaking potentiality, but they nevertheless must be analyzed from the same ontological starting point. Accordingly, the last remaining component of the dissertation’s theoretical framework is Actor-Network Theory – a theory that flattens the existential between humans and things. A flattening that also equalizes the analytical starting point of how we as analysts categorize and thus understand the agency/capacity of actors.

The three core bodies of actors involved in making noise – Internet users, coders and the software technologies themselves – only functions logically through the assistance of Actor-Network Theory (specifically Latour, 2007) for its conceptual focus on the ontology of objects.

As the dissertation analyzes its three core groups of actors (users, coders, software), each is identified in a triangular relationship with one another. The goal is to identify and establish how each actor participates in, and has stakes in, protecting personal information by producing noise. Actor-Network Theory most appropriately facilitates the ability to achieve this goal because the relationship that each actor maintains with one another is treated with an even, flat ontological attitude and perspective. By moving away from anthropocentric impulses – particularly those that tend to dominate mainstream academic attitudes about ‘digital privacy’, impulses that tend to frame ‘digital privacy’ as the outcome of purely human intention, design and control – the dissertation theorizes that software mediates how Internet users and coders relate to one another. The software also governs how Internet user and coders relate back to the software, in turn.

To refer to the power of the software, so to speak, is to refer to its agency. The software, simply put, exists and behaves in social affairs. As the dissertation demonstrates through three case studies of three different anonymity software networks (*The Onion Router*, *WhatsApp* and *SpiderOak One*), each software system is generally attributed by its designers as playing a unique role in generating noise as a means of distracting hackers or detecting malicious information theft. However, the processes themselves depend upon decision-making that is co-opted by the ability for users to operate the software and navigate its limitations. For example, and as will be demonstrated through the case study on Tor, the software cannot sustain its noise production defense mechanisms as the user generates incidental noise, which in this particular case is referred to as a series of accidents users make – such as installing the *AdBlock Plus* plugin into the browser – which sends a series of indecipherable inputs to the software, making vulnerable its own noise production process, and thereby increasingly the likelihood that hackers can de-anonymize the destination and source of information. The point is that by framing the

intentional noise production by the software itself, and the incidental noise produced by the user, ‘digital privacy’ collapses. This is *not* a consequence merely of improper coding by human fingers, but by the relationship between machine and human temporarily rupturing. In other words, the rupture is a consequence of input and output exchanged between humans and machines. Indeed, this temporary rupture reveals how ‘noise’ cannot be understood without context for meaningfulness and understanding, and that in the very least, it is something acted out between machines and humans.

This is not to detract from the utility and importance of human actors in the dissertation’s analysis. Recalling earlier how a theoretical framework derived from Actor-Network Theory flattens the ontological horizon (so to speak), users and coders are analyzed in tandem with – not above or below – technologies, such as the software systems examined in the case studies. The same flat ontological attitude also applies to human actors. This is still a dimension of Actor Network Theory, which is explicated via Pinch and Oodshorn’s *How Users Matter: The Co-Construction of Users and Technology* (2005). Pinch and Oodshorn contribute ontological considerations of the role of the users of technology in terms of their role in shaping technology throughout all phases of its design, repair, modulation, implementation and usage. Of particular importance is their emphasis upon the ways in which resistance, tampering, altered usage and even non-usage (especially in terms of usage that deviates from a designer’s intended purpose) plays an intimate role in not only effecting change in the technology itself but also by effecting the kind of output the technology produces. For example, the case study on *SpiderOak One* demonstrates how some of the system’s most technologically literate users interrogated the software for flaws and found ways to share knowledge about their findings. Those findings mobilized across numerous technical communities online and eventually came to influence how

other users used different file hosting systems such as *DropBox*. The actions of these users are particularly important because they reveal the role of user action in effecting the outcome of digital privacy itself on *SpiderOak One* and even neighbouring software like *DropBox*.

As the dissertation traces out and identifies the noises each actor makes, they are compiled together as a system to allow for a systemic level of analysis. Noises reveal systems as much as they become parts of systems. They alter these systems as well, for these systems are as social as they are technical. They are socio-technical systems. The notion of the socio-technical system is a product of STS scholarship. As such, Pinch, Bijker and Hughes' (Eds.) *The Social Construction of Socio-Technical Systems: New Directions in the History and Sociology of Science and Technology* (1993) represent the final STS component of the dissertation's theoretical framework. Their work contributes a way of thinking about the inextricably mutual nature of influence between humans and technology. Moreover, they contribute a way of thinking about technological systems that compels consideration of how technology effects human desire, perception, direction and achievement as much as human beings effect technological design, function and purpose. Just like the way in which a large technological system such as a nuclear reactor is comprised of various component parts, such as cooling rods, uranium, pressure valves and a containment structure, specialized workers such as analysts, engineers and shift managers are as much component parts of the same system. After identifying each noise made by each actor, they are examined in relation to one another and in relation to neighboring actors. The purpose of doing so is to render these noises as crucial components in altering and even structuring new socio-technical systems. For example, we as analysts generally understand a technological system like *SpiderOak One* to provide privacy through its encryption protocols, server farms and software. The dissertation, via conceptualization afforded by the

logics of socio-technical systems, argues that user experimentation and interrogation as well as coders receptivity (or as we will see, that lack thereof) of such efforts play as big a role in determining the outcome of digital privacy.

As a final dimension of the theoretical framework, the dissertation's theory attends to the ways in which social relations and social actions thereof produce and engage in politics. Where social life exists and unfolds, so too do politics and political life. Accordingly, the dissertation makes a crucial distinction between capital "P" Politics (of legislation and policymaking or of state-corporate affairs) with 'small' 'p' politics (the politics of small scale interactions). This distinction is what Foucault (2000) identifies as the condition and process upon which "relationships of power" are negotiated. Foucault argues that these relations are vastly implicating, covering all dimensions and aspects of human relations. For example, Foucault draws attention to the way in which the act of writing or speaking reflects an effort to inform, persuade or entertain – just as the dissertation is doing in this very moment – in order to establish authority. This kind of politics is common, frequent and unavoidable but not inevitably unethical. Efforts to persuade become unethical and exceedingly problematic when galvanized to work one-way. When they become irreversible, they become oppressive and dominating (Porter, 1998, 155-6). But so long as they are contestable, so long as efforts and attempts to resist them play out – even in the most seemingly infinitesimal ways – 'small' 'p' politics exists. It is of the position of the dissertation that what Serres means by the transfer, movement and effect of noise between actors he means Foucault's notion of "relationships of power"; noisemaking is political and a site of politics as such.

Taken together, the seven parts comprising the theoretical framework indeed extend Serres' argument that noise and noisemaking is a meaningful social activity, but they are particularly important because they add context and conceptual clarity as to precisely how noise can be represented as a register of privacy itself. This is particularly important given that Serres' own approach to privacy itself does not relate to the contemporary and digital contexts of this project. For example, *Parasite* references 'noise' as a factor in the outcome of privacy by likening the privacy as the product of a 'parasite' 'passing gas' in a public place – a *private* act in the sense that the odor robs individuals of the capacity of enjoying public space on their own terms. This formulation of noise in relation to privacy is limited in the sense that it pits privacy as a meaningful social activity. Accordingly, the seven components of the theoretical framework allow the dissertation to explore noise in relation to privacy within a more socially and politically meaningful context. And from each of these seven components, the dissertation offers a distinct contribution in relation to them by explicating precisely where, when, how and why 'noise' and 'noisemaking' in the name of digital privacy.

Beginning with Lundblad, his work expands Serres' approach to noise and privacy beyond physical public spaces, and onto the digital realm. While Lundblad envisions the Internet as a noisy space – laden with confusion, distraction and misleading information and mechanisms as deployed and maintained by corporations and governments – the dissertation builds upon his emphasis and contributes differently by explicitly connecting the 'noisy-ness' of the Internet as an *enabler* of social action. For example, the first case study on *Tor* demonstrates that the incoherence of the system itself compels user action in the name of privacy.

Bolton's work similarly brings Serres' contributions a step further as well. Through his notion of parasitic autopoiesis, the dissertation points towards otherwise seemingly infinitesimal

actors as capable of producing noise (and as such, being ‘noisemakers’ themselves). In the context of his work, the meaning and value of ‘privacy’ is indeed derived from non-corporate and non-governmental action. The dissertation distinctly contributes distinctly from this concept by demonstrating that even the most unaware users – particularly those found in the first case study, those who do not tend to be aware of the forces of surveillance and criminality unfolding around them – engage in small-scale decision making that is akin to the kind of noisemaking that conditions large-scale outcomes for an alternative modality of digital privacy thereof.

Paddison, Philo, Routledge and Sharp extend Serres in direct succession by bringing Bolton and Lundblad one step further. What their work contributes is the specificity about precisely where noisemaking unfolds online – in the *gaps* between actors, relations and systems. The context through which meaningful social activity happens in digital gaps tends to be grounded in conceptual abstractions, through which the dissertation contributes by providing even more specificity as to what gaps noises and noisemaking fill. The third case study on *SpiderOak One*, for example, identifies a privacy gap for former *SpiderOak One* users as they return to mainstream profit-first products – a gap which is filled vis-à-vis the technical expertise of these users as they abridge digital privacy experiences through multiple platforms simultaneously.

Pinch, Bijker and Hughes’ work in the Social Construction of Technology subfield is a crucial connector for the theoretical framework because it links ‘the social’ with ‘the technical’ and inextricably so – a distinct contribution in the sense that it ports the social orientation of Serres’ work onto technical and digital matters of concern and interest. This is most noticeable through these authors’ emphasis on socio-technical systems. While their work enables a sense of conceptual structure about the shape, size and orientation of socio-technical systems, the

dissertation contributes uniquely by providing more concrete and tangible dimensions of these systems. Each case study, for example, points explicitly towards the kinds of encryption protocols, information flow processes, data capture mechanisms and spaces through which privacy is acted upon and within.

Latour's Actor Network-Theory relates along these lines, providing the ontological basis through these actors are situated in accordance to each socio-technical system. Through Latour, all actors are presumed to exist on an even horizon of existence, and as such all possess equal capacity to affect life, relations and systems. What Latour's work thus allows the dissertation's theoretical framework to achieve is a sense of scope in terms of uniting all actors together as potential noisemakers making sound in the name of privacy. While it is inferred that most any object is presumed an actor within the purview of Actor Network-Theory, these objects tend to manifest within the theory itself as tangible and concrete objects. A modest contribution indeed but one nevertheless, the dissertation contributes by identifying an abstract object concretely: software is an actor that creates noise on its own terms, which is explicated in detail throughout each chapter.

The final of the seven pieces comes from Pinch and Oodshorn, which plays a role in emphasizing the validity and agency of the human user. While Latour indeed evens the ontological horizon between all actors, Pinch and Oodshorn are used because they are – unto themselves – an avenue for intervention about extant digital privacy literature as it tends not to imagine the user as a relevant actor. Their work indeed points towards users on the Internet and in hacking cultures, while the dissertation contributes to them explicit accounts of not only user activity in three different kinds of encryption-enabled social media software system it also explicitly contributes various different kinds of users under the same rubric. As detailed in the

first case study, for example, there are three different kinds of user groups under the general rubric of ‘user’ who represent three different modalities of noise-oriented action – each of which has very specific outcomes upon digital privacy itself.

Overall, the dissertation extends and contributes uniquely to these seven theoretical informants by offering a balanced ontological framework that empirically accounts for the numerous ways in which actors compete and co-opt one another through noisemaking activities – activities that both clash *and* coalesce in a way that gives rise to and affects existing socio-technical systems. As such, the dissertation provides an empirically grounded conceptual framework and theoretical basis vis-à-vis a systemic level object of study; the socio-technical systems created by noisemakers is where the dissertation looks in order to generate novel and alternative ways of thinking about, with and through digital privacy – particularly as a matter of the *surrender* of control *beyond* the purview and practice of governments and corporations.

Methodological Framework

The dissertation approaches its case studies through a three-step process. The first, is an introduction to the case study. It is a general outline and background of each case study. This involves starting with accounts of the ownership, politics and size of the network under analysis. This section also familiarizes the reader with the ‘technical’ account of how the case study’s system works. It outlines how conventional thinking about digital privacy in the context of the case study generally unfolds. For example, the introduction to the case study on Tor reveals how ‘digital privacy tends to be a matter of onion-routing encryption carried out through a volunteer network of relays across the planet’. It is the ‘standard’ understanding of digital privacy, and as such, the understanding that the rest of the chapter will contest.

The second section, derived vis-à-vis Serres' *Parasite*, identifies each of the three actors in each case study: users, coders and software. Users refers to any individual or social group that downloads, engages and regularly interacts with a software interface – whether a downloadable software package like Tor or a website of the product itself. Coders refers specifically to the programmers, engineers and scientists involved in the creation, circulation and maintenance of any of the software users interact with. This category, more generally speaking, also includes individuals who work for the software company itself – including Web Masters, marketers and advertisers. As the case studies demonstrate, programmers also play a specific role in marketing and advertising the software and so this social actor should be treated widely in terms of its ontological categorization. The last actor, the software, refers to the networked, user interface itself. Whether the web browser or the technical systems powering and managing the software, this category generally refers to any product or interface the users and coders work with and towards. After identifying who constitutes each actor, the case study's first component then constellates precisely what each actor's noisemaking activity entails. For example, the way in which Tor's coders program send messages through the software, emitted towards users, instructing users to curtail their browsing behaviour in order to mitigate the any potential vulnerabilities that might arise in terms of how users interact with the software.

The third section stitches together these noises. It constellates them as socio-technical systems. This section demonstrates how noises affect neighbouring actors and neighbouring relations between actors. This section also identifies how and whether noises from different the actors clash or coalesce. Returning for a moment to the example of the Tor's coders making 'noise' that is directed towards their users – in a way that encourages them to browse cautiously – there is a clash with the noise the software emits. This clash has the effect of encouraging users

to browse liberally. The outcome of which being the emergence of a confused message exerted towards Tor's users. They become caught in-between coders telling them to browse conservatively, and software encouraging the opposite. The consequence of which is the splintering of user behaviour into various types – users who act upon the coders' noise, actors who act upon the software's noise, users who ignore both and so on. The effects of this noise clash between the coders and software on Tor also effects how the wider technical components of the network operate as well. As the case study demonstrates, this confusion of noises wreaks havoc on a very specific volunteer-relaying protocol that governs information transfer. As a result, the Tor system begins functioning in ways the software is not intended for. The point of the second section of each case study is to simply demonstrate that each system is indeed a socio-technical system – where social processes (such as noisemaking) directly implicate and alter technical processes and vice-versa.

The fourth and final component of each case study is the conclusion. The conclusion provides discussion on the nature and character of each constellating and intersecting noise. The goal is to provide the reader the alternative account of digital privacy – the one that contents purely technical accounts. This is achieved by providing a picture of how social and technical processes are constantly changing throughout the system, causing a kind of system-wide behavioural development. From the unique array of social and technical interactions presented in the previous section, the concluding section of each case study establishes how noises tell a different story about the how, what and why of 'digital privacy'.

Case Selection

The dissertation analyzes three separate Internet-related technologies: *The Onion Router*, *WhatsApp* and *SpiderOak One*. What all three of these case studies have in common is that they

contain an advanced form of encryption. Whether that encryption protects the location of the user or the content itself, the reason encryption-oriented technologies were chosen is because they embody and reflect the twenty-first century's most popular and conventional understanding of digital privacy. Encryption is almost universally perceived as *the* premiere cutting-edge modality through which digital privacy is guaranteed. Against the global proliferation of hacking, cyber warfare and Big Data developments, encryption is particularly sought after by designers of the Internet-oriented communications and browsing software most popularly used around the planet. And so, the second justification for this particular case selection is because each software system represents the most popular, globally-used system representing three distinct domains of Internet-related experience: Internet browsing, instant messaging and file hosting/cloud services.

The Onion Router

Tor is a PC and Mac-based web browser that allows users to allegedly browse the Internet as well as the 'deep web' – the largest domain of the Internet itself, which is not accessible nor regulated by corporate 'world wide web' protocols and destinations. Digital privacy is marketed to Internet users as a product of 'onion routing' encryption. 'Onion routing' is a process whereby the information leaving a user's computer is packaged into multiple layers of encryption, likened to the layers of an 'onion'. As the information is sent to its destination, such as a website, it first passes through a volunteer relay of computers across the planet. This relay or pathway is determined by the software and the larger Tor server. As the information passes through each relay, a 'layer of the onion' is peeled back, revealing information about the next destination in the volunteer relay that the information must be sent to. The process is carried

out until all ‘layers’ are peeled back, revealing the final destination or website for the information itself. This understanding is the conventional understanding of digital privacy on Tor. But as the dissertation demonstrates vis-à-vis the noisemaking capacities of its different actors, and of the socio-technical system they create as well, ‘digital privacy’ looks rather different on Tor.

What makes Tor such a fascinating case study is the way in which a three-way noisemaking process creates numerous conflicts in terms of messages, visions and ideas received between each actor. For example, Tor’s coders’ noise unfolds as a message they place on both their website and their browser for users to receive and act upon. It begins early in Tor’s emergence as merely a message, an encouragement to browse the Internet liberally. It is a reassurance to users that the technology works as designed. But this message eventually transforms into a noise, it becomes a demand of users to constrain their own behaviour. It aims to promote browsing behaviour in a uniform fashion because the coders realized that the software is being used in ways that it cannot handle. But this noise emission did not necessarily create conditions and expectations of digital privacy for users as the coders originally hoped.

Contrary to what coders sought to achieve with their noisemaking, many users started tweaking the software to make it more ‘reliable’ and ‘functional’ despite the coders’ desire. Some users flatly resented the demand and began using Tor in ways that undermined the software’s ability to provide privacy. Some users ignored the coders’ noises altogether and re-deployed Tor for illegal purposes. Regardless of which kind of user-oriented noisemaking takes place on Tor, all user noisemaking is mediated by the software’s noisemaking. This software’s noise works against the coder’s noise. The software’s noise emits from its aesthetic design, which is modelled after a blend of *Google Chrome* and *Mozilla Firefox*. The graphical mimicry

of popular browsers encourages liberal browsing usage. The software's noise is thus a visual 'knock' – a signal to users to 'browse as they please'.

The clash of noises throughout Tor's evolution yields interesting insight as to how Tor emerges and exists as a socio-technical system. Illegal browsing usage and behavioural trends started dominating the majority of the data flows across the Tor network over the past few years, which vastly implicated how coders attend to their own perception of the 'need' and 'utility' of digital privacy. This is particularly noticeable by looking at 'normal' web browsing behaviour on Tor. Conventional usage on Tor has become the most targeted stream of usage by external hacking attempts. And this targeting of normal web usage has compelled some user groups to blend-in with illegal streams so as to hide more effectively; some users learned to browse in unfamiliar spaces in unfamiliar ways and by doing so, make a different kind of noise that ultimately enhances their own and others' privacy. This change in behaviour is a socio-technical phenomenon, and it instructs us as analysts that digital privacy on Tor is not merely the guarantee of an encryption based upon an 'onion routing' encryption technique. Rather, digital privacy is the outcome of contingency on the one hand, and the wherewithal and adaptability of users on the other hand.

Another way of understanding this is that there is a degree of mutual adaptability taking place between different kinds of users. While some Tor users manipulate the software for illegal purposes, they have their own modalities of creating privacy. Other users, such as journalists, students and researchers, are becoming increasingly aware of these illegal flows, particularly because they have more novel and effective ways of utilizing Tor to provide a more reasonable and comfortable degree of protection through the software – more protection than the software tends to provide if used for legal activity. This is a primary example of what Pinch and Oodshorn

(2005) expressed earlier with regards to the importance of users in sociotechnical systems; resistance and even non-use of technologies plays a vital role in not only the eventual modification and improvement of technology, but it can also blur the line between who is responsible for the outcome of privacy itself.

WhatsApp

The most popular Internet-based communication system in the world is *WhatsApp* – a *Facebook* owned text message-oriented service that allows users worldwide to communicate with one another by bypassing cellular service providers’ networks (and fees) in order to ‘text’. Encryption on *WhatsApp* unfolds through what is called ‘End-to-End encryption’. As advertised to its users, once a message leaves a user’s phone it is encrypted. The message is only decrypted once it reaches its destination, which is another *WhatsApp* user’s device. What is particularly significant about this modality of encryption is that it comes with the guarantee to users that none of the content of their message can be read by anyone at *WhatsApp*, *Facebook* or any external company. *Facebook* uses this modality of encryption politically. They argue that they cannot data mine or out-source the content of their messages because it is impossible to access the information. And if it cannot be accessed by them, it cannot be accessed by external eyes such as hackers or government surveillance/security regimes. Alas, the information is indeed harvestable despite *Facebook*’s claim otherwise. Moreover, this case study is a particularly unique choice because of the way in which the noises made by the coders and the software itself coalesce. The coalescing engenders a social environment that demands re-assessment by privacy analysis, specifically because any noisemaking capacity by users is essentially precluded. And this has dramatic implications for how we as analysts understand ‘digital privacy’ on *WhatsApp* altogether.

The noise the coders make and emit into the network is a continuation of noises its original designers made. For example, the noise the software makes reifies the notion of protection from external gaze through certain aesthetic properties but also introduces a completely different and unfamiliar property to the gaze of the users themselves: meta-data about their interactions with other users. The noise the software emits towards the users is a message of confidence on the one hand, but of curiosity and inquiry on the other hand about the behaviour and nature of interactions between users on the other hand. The users, rather differently from any other any other case study, have very little option to make their own noise. At one point in time, they had a thirty-day window to opt-out of data mining. But this window was not well publicized. The noise the coders emit and the software emits is intended to ‘depoliticize’ the users’ experience – to create trust that they simply need to interact and not worry about digital privacy, and as well will see, this creates tremendous problems for ‘digital privacy’ itself.

As a socio-technical system, the coalescing of the coders’ and software’s noises handcuffs users. This is precisely what Grant and Bennet (1995) had since the onset of the Internet itself with regards to the capacity of corporate influence online to control not only the flow and access points of information but how that information is experienced as well. *Facebook* may not be reading users’ messages, but they are directly harvesting their meta-data: the math or the numbers of how they interact with one another. The system takes advantage of certain social assumptions and norms amongst users regarding their privacy in order to insulate the world’s largest instant messaging community from external harvesting by other companies on the one hand, while also encouraging users to interact on the other hand. But of most interest here is the way in which this meta-data is visualized for the users themselves. The software shows ‘time stamps’ about when users last read or received a message. At one point in time, the software

even provided users assessments about the average time it takes for certain users to respond. These indicators have crucial implications for how we as analysts understand digital privacy.

Digital privacy on *WhatsApp* is not merely an affordance of world leading End-to-End encryption. It is also a process of *manipulating* users into believing that *content data* is their primary matter of concern. *Facebook* uses the meta-data they collect to allow external parties to advertise directly to users in their inboxes on *WhatsApp*. Moreover, the visualization of some of these meta-data sets is, in turn, giving rise to a completely different domain of digital privacy altogether. This domain refers to the digital privacy between users. Since the introduction of these meta-data visualization technologies in the software itself, there has been an acute proliferation of bizarre and increasingly invasive behaviour between users themselves. Many users obsess over the amount of time it takes for other users to respond, which also reveals to us as analysts that with this new domain of digital privacy there is an equally large proliferation of digital privacy violations – which *Facebook* does *not* attend to nor express any concern regarding whatsoever.

SpiderOak One

The final case study examines one of the most popular security and privacy-first file hosting/cloud services: *SpiderOak One*. Digital privacy is said to unfold similarly to *WhatsApp*. End-to-End encryption is provided, whereby users' data is encrypted on their computer and on the *SpiderOak One* servers as well. The company also markets their product as impervious to gaze from its employees as well as from outside access as well. *SpiderOak One* is a particularly interesting case study because of its story as well. Its evolution and popularity is due not only to its early reviews and industry-wide recognition (perhaps most recently popularized by an endorsement from Edward Snowden in the wake of the 2016 election primary hacking scandals

between Russia and the Clinton campaign) as a privacy-first product, but also because of the way in which it gained much of its popularity because of the 2011 and 2012 security controversies surrounding the file hosting industry in general, as well as its primary competitor in particular: *DropBox*. In fact, these controversies played a crucial role in preconditioning the largest example of user-oriented noisemaking in terms of its effect on the socio-technical system itself on the one hand, and also in terms of an alternative understanding of the ‘how’ and ‘what’ of digital privacy on the other hand as well. In what Bolton (2013) theorized around noise and privacy online, it can indeed be exemplified rather clearly here that some of the most significantly progressive outcomes for the future of digital privacy depends upon the Internet’s users to find and construct their own meaning and value.

The noises the coders make and emit into the wider *SpiderOak One* network, specifically towards the users, which – like the other case studies – promises users that their product is safe and reliable, particularly more so than their rival’s products. Their noise is particularly powerful in the sense that this promise was marketed to users on platforms that are otherwise inaccessible to the other case studies. The coders designed the software to work on non-mainstream platforms, such as *Ubuntu* and *Linux*. The software however counteracts this noise with its own noisemaking, which unfolds in two ways – both of which have been consistently present since the release of *SpiderOak One*. First, the software system itself is embodied by a graphical user interface that is rather bizarre and unusual for a file hosting service competing with companies such as *DropBox*. Its aesthetic design is unfamiliar and difficult to navigate. For example, it is difficult for many users to know whether or not their files have successfully synced and stored. Secondly, the software has been plagued by numerous technical issues, specifically a frequency of disconnects from the *SpiderOak* servers and files not being stored properly as well. The noise

the coders make is a response to the clash between the noises from the coders and the software. These users took the onus of the protection of their files upon themselves and in two ways. First, they experimented with the design of *SpiderOak One* to make it stronger and routinely participated in an open-source dimension of the software's source code that allowed users to program and write the software. Secondly, they began critically investigating other technical issues that revealed that the encryption does not in fact protect certain locations and streams of interaction and file storage, which led many users to leave *SpiderOak One* and others to split where they stored their files between *SpiderOak One* and profit-first services like *DropBox*. Like the way in which John Cage swung the doors of the concert hall open to invite in the noise of the world via Attali's (1997) account, *SpiderOak One*'s users similarly brought in an array of noises that had dramatic implications for how *SpiderOak One* unfolded as a system.

As a socio-technical system, *SpiderOak One* is particularly unique because of the way in which its users' behaviour began influencing the way digital privacy is achieved in the file storage industry altogether. Because of the ways in which the noises of the users and software clashed, and because the noises initially attracted the Internet's most technologically literate and privacy-oriented user-ship (which is found on *Linux* and *Ubuntu*), users began playing a two-pronged role in how *SpiderOak One* grew and was used altogether, which has vast implications upon how we as analysts understand digital privacy on *SpiderOak One*.

Digital privacy on *SpiderOak One* is a reflection of a shift in social norm about the value and meaning of data itself. As users re-assessed and re-evaluated what information they deemed most worthy and most important of storage on *SpiderOak* not in terms of its content but in terms of its size – smaller sized files store more efficiently because they fit more comfortably in between the frequency of disconnects. Users also began going back to services like *DropBox*,

bringing with them their creativity and propensity to investigate and build their own solutions. This has dramatic implications for us analysts in terms of understanding digital privacy here as the users' experiences demonstrate that digital privacy is not merely a question of encryption protocols on the world's most secured file storage service. Rather, it is a reflection of two things. The first being the onus placed upon technologically literate users; the more awareness they have regarding the slippages and shortcomings of their technology, the more compelled they are to act upon those issues. Secondly, these users are thus also compelled to critically reflect upon how they value their own information, and which information they feel is most important.

Outline

The dissertation consists of seven chapters in total. The first is represented by the afore, while the second chapter follows closely with its literature review. Chapters three through five represent the case studies as discussed above. These chapters follow the same order accordingly: Tor, *WhatsApp* and *SpiderOak One*. The sixth chapter is a comparative analysis of the three case studies. The purpose of that chapter is to provide how and why each case study is different particularly in terms of how we as analysts locate alternative and new understandings of 'digital privacy'. The chapter provides key overarching themes of contrast and comparison as well, such as for example, the way in which coders across all case studies seem to emit a similar noise – one that compels users to simply trust the technology blindly. Moreover, we see that these noises always fail to deliver precisely what they promote otherwise. The chapter also revisits the theoretical territory of the dissertation itself to provide insight, for example, on how Paddison, Philo, Routledge and Sharp's (2000) theory about the way in which gaps between relations (i.e. between users and coders) preconditions different sets of outcomes for how noises constellate

together in turn producing different outcomes for each socio-technical system. The final chapter of the dissertation is the conclusion. The primary purpose of the chapter is to outline the contributions the dissertation makes to two fields of study: Communications Studies and Privacy Studies.

The former entails a re-invigoration for how we might approach the concept of ‘noise’ as a subject and object of analysis. The goal is to identify intellectual merit in abstaining from the field’s tendency to approach ‘noise’ from value-laden perspectives that tend to promote normative epistemological judgements upon the notion of ‘noise’ itself. By attending to noisemaking and the presence of noise in different socio-technical systems, we can advance the intellectual task of re-visiting our empirical studies of noise-in-systems to re-articulate how these systems behave, fluctuate, shrink, grow and alter themselves as well as splinter, rupture, depart and adapt as opposed to simply failing.

The latter entails the fundamentality of noise to privacy itself. The conclusion argues that the future of privacy studies ought to proceed by demonstrating the intimacy of the concept of noise to the very structure and outcome of privacy altogether. In doing so, the dissertation encourages existing and future Privacy Studies research to find methodological invigoration by attending to the unobvious and taken-for-granted ways in which even the most accidental actions, movements and diagnoses generate reverberation in networks – in a way that adds or detracts even marginally. These slight changes can dramatically amplify or dampen system changes in relations between actors and with the technical dimensions of the system itself. By zooming in and zooming out around sites of noise, we take stock of the complex array of colours produced by actors that we tend not to see when studying privacy altogether.

Chapter Two: Literature Review

The primary bodies of literature contributing to the dissertation either explicitly or implicitly engage the notions of digital privacy and noise. The chapter engages both of these notions in separate parts – part two and part three, respectively. Part one provides the chapter’s overarching argument. Part two engages historical works on public and private life as well as contemporary works that take up the notion of ‘digital’ privacy more directly. Part three engages fields that take up the notion of noise as their subject matter. Each part provides an overview of how they frame and approach digital privacy and noise, as well as an overview of what they contribute to the dissertation. Each part also identifies and discusses the limitations of each approach to the study of digital privacy and noise. Thereafter, part four of the chapter engages Michel Serres’ (1982) *Parasite*, for the ways in which it generally reconciles limitations and problems presented in parts two and three. Part five charts the limitations of the preceding three parts so as to identify gaps across both contemporary and historical literature dealing with digital privacy and noise altogether. These gaps are filled in the dissertation’s first chapter via the theoretical framework. Part six offers a brief conclusion to the chapter, which precedes the next chapter being the dissertation’s first case study.

Part One: Overarching Argument

Literature engaging digital privacy tends to emphasize and reify the role of governments and corporations in regulating and controlling digital privacy (Acquisti, 2007; Marcella, 2003; Bodó, 2014). However, the literature tends not to engage the ways in which individuals, social groups or even technologies themselves play a role in the ‘how’ and ‘what’ of digital privacy. The issue stems from a two-part problem. The first stems from an empirical preoccupation

whereby scholars trace privacy's threats. The second is the subsequent normative endeavour whereby that same scholarship prescribes solutions such as digital information protection and pre-emption protocols, laws, policies and technologies. The result is a perpetual academic cycle, a process of diagnosing and prescribing digital privacy. A particular issue with this tendency is how it reifies the notion that large-scale institutions are the sole purveyors of digital privacy. Social groups and individuals are increasingly removed from conceptual and empirical consideration as players in digital privacy. Social groups and individuals are simply ignored as actors in the outcome of privacy. This is a departure from historical scholarship, particularly from the fields of Political Philosophy (which is, on its own terms, a historical analysis of the emergence of privacy in and around tensions with the state), Social History, and the History of Science/Technology. These fields conversely engage privacy as a very individual and social group-based modality for the engagement of daily social, economic, cultural and political issues. The chapter thus identifies the gap between historical accounts of user and social group-based engagement with privacy with contemporary scholarship on digital privacy scholarship for the ways in which questions of individual and group based privacy-oriented practice are generally ignored.

A second significant issue with digital privacy scholarship is the way in which the literature idealizes digital privacy as a 'guarantee' through legislation and policy (Westby, 2004; Svantesson, 2015; Dowling, 2009). This idealization reifies privacy as a definition, which does not easily open up to alternative ontological considerations of who and what is involved in the outcome, design and maintenance of digital privacy itself. The dissertation argues otherwise, and this is precisely why the dissertation makes the conceptual move to noise, which is the next matter of discussion and analysis in the chapter.

Noise is not merely a technical phenomenon. It is also a social phenomenon, particularly in the sense that noise is a bi-product of social activity. As such, noise and noisemaking carries with it the power to create new, and alter existing, social systems. Noise-oriented scholarship attempts to address this, but fails to do so in ways needed by the dissertation. The noise-oriented scholarship the chapter discusses generally contributes how noise – whether conceptually, theoretically, phenomenologically, or technically – is indeed more than a technical phenomenon. It is a social activity, a social force, a social preoccupation. Like the way in which noise emitting weaponry deflects protest movements or the way construction noise caused social havoc in throughout the United States' metropolitan areas during the 'roaring twenties', noise ought to be taken up as more than reverberation and as a register of social action and social expression that achieves certain goals or outcomes.

The limitations of noise-oriented literature are three-fold. First, the literature assumes that noise is something that can be predicted in terms of its effect on social life. What the literature misses is that noise tends to animate in the mind's eye notions of slipperiness, confusion, distortion, interference but it is evident that intellectual engagements with noise in relation to social dynamics tend to organize, striate and even operationalize noise. Shannon argued that noise can be measured, and because it could be measured, noise could thusly be located in terms of its origin – so as to eliminate it. This framing of noise is a technical level, which is useful for the nature of Shannon's work and the field he was addressing at the time. However, this approach requires development through ideological, cognitive and affective registers. Secondly, noise tends to be treated – much like digital privacy literature – as a normative, social activity or preoccupation. The normative register through which noise is imagined as a social activity is problematic in particular because of the dichotomous epistemological nature of the register itself.

According to the noise-oriented scholarship reviewed below, noise tends to be imagined as a social force that either ‘builds up’ or ‘breaks down’ social relations. But never with the other, and most certainly never in-between. Thirdly, noise (with the exception of cryptography literature reviewed below) tends not be realized as a register of privacy itself. Like the ways in which sunglasses worn inside enclosed spaces deflect knowledge of the wearer’s gaze or how tinted windows similarly obfuscate sightlines into an automobile, this way of thinking about noise-as-a-social-activity does not lend itself self-evidently. Of the three issues with noise literature identified here, all of them are amended via Michel Serres.

Serres’ approach to noise, via *Parasite* (1982), renders it as something of a fundamental social activity – akin to the precursory nature of all social relations and social life itself. Noise, Serres argues, is what brings social life together, and makes it collapse. It is responsible for the growth and demise of entire social systems. But the fundamentality of his logic about noise also means that it should not be treated normatively, nor should it be conceptualized as something entirely harness-able, predictable or completely controllable. Serres argues that noise is variegated in nature, that noise affects social systems differently from context to context. Serres even argues that noise is indeed a register of privacy itself.

Part Two: Historical & Contemporary Privacy-Oriented Literature

To offer an overview of how various fields within the academy engage the notion of digital privacy, it is important to engage how the notion of ‘privacy’ takes root across different intellectual lineages. The primary reason for doing so is that what constitutes digital privacy today is taken for granted. The origins of the notion of privacy itself, what it is constituted by and by whom and how, are not self-evident across historical literature exploring privacy.

Accordingly, this section considers historical literature upon the notion of privacy, then follows with contemporary privacy works but those particularly oriented towards the subject matter of the dissertation itself: digital privacy. The overarching point to be taken from what follows in this next section is a specific *disconnect* between historical and contemporary privacy literature. This disconnect is caused by the disappearance of the actions and involvement of non-state and non-corporate actors in the unfolding of digital privacy. As historical works that engage the notion of privacy indicate otherwise, privacy is indeed a very social and often individualized set of practices founded upon sets of norms, rules, beliefs and ideas that are often founded and formulated in contrast or juxtaposition to the public sphere of government and corporate dominion.

Histories of Private and Public Life

Prior to engaging digital privacy literature, it is important to chart historical scholarship pertaining to the origin and tensions in/around privacy. And this is precisely what is meant here by ‘histories’ of privacy. The absence of a ‘history of privacy’ subfield of the Humanities or of the field of History writ large compels the dissertation to seek out multiple bodies of historical literature that oriented towards the explicit or implicit study of notions of ‘privacy’ or ‘private life’. This absence also compels the dissertation to engage historical literature that engages, whether explicitly or implicitly, notions of ‘public’ or ‘public life’ as well. The overarching goal of which being to demonstrate that historical research documents social evolutions of how different individuals, groups and societies created and responded to changes/fluctuations in the spaces around them. Spaces such as, for example, physical proximity between people as populations in cities change over time. Or as another example, the change in frequency of visits to the front door or calls over the phone by government agencies. Many historical studies reveal

that social, political, economic and cultural tensions and apprehensions arise when the space between individuals, groups and societies undergo change – a process that, in turn, has intimate effects upon the unfolding of social identity, affect and belonging.

Perhaps most importantly, historical research offers the notion of privacy as a social activity and social preoccupation – one distinct from the realm of governments and corporations. As will be discussed in greater detail later in the chapter, one of the largest issues with contemporary privacy literature is that the majority of it argues that privacy is a constitutional or legal right. For example, most contemporary literature engages privacy as a civil right or liberty as afforded to Americans by the Fourth Amendment, which protects against the unreasonable search and seizure by governmental officials (Amar, 1994). In Canada, there is no constitutional right to privacy but the *Charter of Rights and Freedoms* does contain a right similar to the American Fourth Amendment in the sense that the Canadian Supreme Court recognizes privacy as a fundamental pillar of any liberal democracy (Levin and Nicholson, 2005). The issue with resolving privacy to a matter of ‘right’ promised by a government is not only that it reifies the notion that government (and related institutional actors) are to take it upon themselves to protect privacy violations of its citizens; the focus of the dissertation’s empirical matter is to demonstrate that users and the software itself also plays an intimate role in the unfolding of privacy itself. The issue here also has to do with the fact, which will also be discussed later, that the many of the very privacy violations the dissertation is concerned with emanate from government preoccupations with Internet-oriented surveillance.

Accordingly, what follows is review of different historical subfields that all play a different role in demonstrating how privacy has been recognized as an activity and preoccupation that *also* depends upon the involvement of individuals and groups as their own actors of privacy

– where the onus of privacy in the name of protecting personal information, for example, is taken up beyond the mere ‘promise’ of constitutional rights and liberties. Three subfields of History are explored accordingly: the history of Political Philosophy; Social History; the History of Science and the History of Technology. The idea is to begin widely in abstraction and move into more particular realms. The former is selected because Western Political Philosophy, and political-historical literature thereof, represents some of the earliest academic engagement with the notions of privacy/private life and public/public life. They also play a central role in demonstrating that some of the earliest political thinkers – despite their influences on the role and outcome of government – advocate for the separation of state/society wherein the earliest notions of ‘privacy’ and ‘private life’ tend to reside as objects of study. The second and third fields are selected because they engage more specific social, cultural and political contexts grounded in primary historical texts. As such, they are more deliberate with their engagement of empirical matter, such as primary historical documents. One of the pieces of literature (Sennett, 1977) within social history, for example, how the notion of the ‘private’ home emerged during the socio-political turbulence against early Christianity during the height of the Roman Empire. The history of science and technology may initially seem an odd fit, but its study of the evolution of scientific and technological life levies the importance of individual actors – such as researchers, scientists, laboratory technicians and explorers – manipulating the proximity or distance between themselves and their employers, neighbours, media, scientific dynasties as well as religious and educational institutions in order to realize their goals.

John Locke’s *Second Treatise on Government* (1690) marks a distinct separation between public and private life, particularly as it pertains to the difference in how individuals and societies come to own personal property. The distinction thus derives is logic from Locke’s

interpretation of the Law of Nature. The State of Nature to Locke is characterized as a “state of perfect freedom to order [their] actions, and dispose of [their] possessions and persons as they see fit” (Chapter II, section 4). In Locke’s image of the State of Nature, no individual owns the planet. Rather, Nature itself and all things Nature produces are owned in a public common. Individuals however do possess the right to own property that they achieve through their labour. As that labour facilitates the creation of their property, that property becomes private as such – not part of the public common. Because their labour is also the principle driver of the social contract, they also have the means to set out the distinct realm of the ‘public’ itself within which the maintenance of civic order is established through governance. Moreover, Locke argues that the social contract is ordained specifically to assure private ends vis-à-vis the protection of life, liberty and property.

Rousseau’s famous treatise *The Social Contract* (1762) also delineates an important distinction between public and private life, but one which unfolds a bit differently than from Aristotle’s logic about nature. Unlike Locke, who argues that the social contract formulated the basis for agreement with government, Rousseau argues that the social contract established the basis for society itself. There is another crucial difference here between Locke and Rousseau, particularly in the sense that Rousseau did not believe humanity was born free. Rousseau believed that in order for a society to emerge and evolve, humanity must give up its ‘natural rights’ in exchange for civil rights and civil liberties (McWhirter and Bible, 1992, 49). Privacy and private property only become notions as such because society would allow it. The impetus being that society had the right to limit or control privacy, and from society came government. Government’s purpose is to determine ‘general will’, as Rousseau argued. But in his formulation, man is born ‘good’. In a perfect democratic system filled with ‘good’ humans, there would be no

concern or need for government surveillance. There would also be no need for something like the United States' Constitutional Amendments. The interests of small social groups would inevitably corrupt society, making privacy virtually impossible particularly in the contemporary placement of Rousseau's vision. Nevertheless, the point here is – rather simply – that Rousseau plays a fundamental role in delineating that there ought to be a distinct realm upon which privacy unravels and that even *if* it is a responsibility of government it is a vision of government that does not represent contemporary neoliberal models of democracy.

Aristotle offers one of the earliest political philosophies that engages the notion of privacy, which is conceptualized within his work *Politics* (350 B.C.E.). The work is divided into eight books, and within his first book he sets the conceptual territory upon which much of his analysis of political life unfolds. This territory is demarcated largely in part to his distinction of two realms of life. The *polis* includes the structure of the body politic itself and the sphere where the details of government unfolded itself, while *oikos* referred to the opposite – a private sphere attached to the home, particularly the private household (Decew, 1997, 10). This distinction is particularly important because *oikos* sets out precisely what social activities constitute the sphere, of which Aristotle thus identifies as outside the domain of concern of governance: life, reproduction, entertainment and death.

John Stuart Mill's *On liberty* (1859) asserts that the only justification for an individual to force another individual to do anything beyond their will is when they cannot protect their own interests or the interests of others. And so, the only condition upon which a government can intervene upon a person's life is when that individual cannot protect themselves from danger, such as self-harm. Otherwise, Mill's philosophy on the order and relationship of liberty and authority emphasizes the fundamental importance of individuality in liberal democracies.

Opinions, thoughts and discussions upon daily politics are to never be repressed by government (Ch. II), nor should they be interrupted in pursuing their own interests (Ch. IV). So long as individuals do not harm one another or themselves, their thoughts and actions are sanctioned 'private' from governmental repression and intervention.

Aside from Political Philosophy, Social History introduces more empirical specificity around not only the lines between public and private life, but of the role society plays in that line drawing between public and private life. The overarching contribution is thus that of the select works chosen here – From Orlin and Igo to Sennett – that social life and social bodies occupy a sphere upon which private affairs and privacy unfold. For example, Orlin's (1994) *Private Matters and Public Culture in Post-Reformation England*, argues that the birth of English privacy is a history of the obsession and subsequent mimicry of the public life of English aristocracy to own property and private spaces. Her argument delineates the structure of a public and private sphere that are less distinctly separated than what is offered through the Political Philosophical works reviewed above. In fact, her work infers a mirroring and drawing-in of private life towards the realm of government and the public. Nevertheless, the point here is that members of society *outside* of government cultivated the notion of privacy on their own terms, through their own labour and in their own image despite their referent inspiration coming from government and public institutions.

Sarah Igo's (2007) *The Averaged American: Surveys, Citizens, and the Making of a Mass Public* offers a different temporal perspective upon the separation of public and private life. Her work documents the ways in which mid-twentieth century social scientific public surveys created tremendous public backlash through the invention and circulation of surveys and opinion polls ranging in topics between daily politics and the sexual status of married couples behind closed

doors (Igo, 106-7; 139). What her work specifically introduces to the dissertation is that inquiry into the practices of the home delineates a distinct level and theme of societal intolerance and resistance. Upon knowledge of the public-ation of the information collected from the surveys and opinions polls – particularly once interviewees and participants began learning of the details of the affairs of their neighbours – Igo’s work demonstrates that the cultivation and ownership of the home embodies the distinct desire to control what information should and should not be made privacy to the public. The stake here is that the lack of control or direct access to that information, the removal of its circulation from the hands of the survey and poll subjects, makes legible a very discernible social apprehension about the removal of the management of one’s own personal life.

Richard Sennett’s (1994) seminal *Flesh and Stone: The Body and the City in Western Civilization* documents the emergence of the Christian home as an escape from Roman oppression as a means to privately worship and discuss the differences of Jesus and Paganism. At the height of the Roman Empire, the pursuit of the Christian ‘cult’ pressured Christians to find alternative means to practice their religion. They also required the means through which their community members could meet and discuss their religion as well. The emergence of the private home, to Sennett, is the result of such pressures against the early formation of Christianity.

The last body of historical literature contributing to the dissertation significant contribution derives from the History of Science and the History of Technology. The first piece of literature is Shapin’s (2010) *Never Pure: Historical Studies of Science as If It Was Produced by People with Bodies, Situated in Time, Space, Culture, and Society, and Struggling for Credibility and Authority*, which document the seventeenth-century professional scientific lives of Britons Robert Hooke and Robert Boyle during their creation of the air pump – an experiment

involving the creation of a device that the *Royal Society* – specifically outlines the tension between the politics of *Royal Society* in requiring the device to work in order to garner political legitimacy with the daily lives of Hooke and Boyle. Shapin’s historical account is one of the place-ness of science, an account of the movement of people into and out of the home/laboratory of the scientists. While Boyle identified his home/laboratory as an intensely private space, where he could escape the distractions of public life, Boyle treated it rather oppositely – as a stage for the public, a place where the lines between inside and outside life were considerably blurry. Privacy here is something that is cultivated by individuals fighting, closing doors and choosing not to invite people into their home/laboratory.

A similar tension is found nearly one-hundred years later in Deborah Coen’s (2007) account of the mid nineteenth-century Austria’s premiere scientific dynasty, the Exner family, who struggled in their quest to promote a liberal political climate with regards to the intellectual treatment of mathematics and philosophy by the monarchy. While chastised by the government for instructing university students that divinity interrupted the logics of uncertainty and probability in daily university instruction, the Exners brought their colleagues, students, neighbours and friends to their Alpine cottage, *Brunniwinkl* (Coen, 257), where both heuristic strategies and experiments could be conducted outside of the confines of the university laboratory and outside the gaze of monarchical parochialism. The return to life in Vienna meant transporting ideas created in the Alpine cottage, rendering *Brunniwinkl* as a tension-filled space where public discourse and private exploration clashed. The birth of Viennese liberalism itself is documented here as the way in which very public figures created, transported, engineered, deployed and circulated private ideas as a means of not political resistance. Ruskin’s (2004) *John Herschel’s Cape Voyage: Private Science, Public Imagination and the Ambitions of Empire* –

like the previous two examples – similarly documents the mid eighteenth-century private funding of a scientific excursion into the southern hemisphere to generate public celebration in scientific excellence. The history of privacy as both solution and problem to public issues, as well as the historical demonstration that privacy is indeed a matter of social expression, experience and opportunity is not confined to the history of science, it is also generally reflected in social history.

What these three bodies of historical scholarship generally contribute is a reminder for contemporary scholarship that there is that social groups imagine, construct and act upon images of privacy on their own terms – many of which are uniquely different epoch to epoch, space to space. The general limitation of historical orientations here is rather obviously that it is not contextualized within the contexts of contemporary, digital dynamics. And so, the next section of this literature review is thus contemporary digital privacy. It not only demonstrates the contributions of numerous fields of scholasticism invested in digital privacy research and diagnosis itself, but it follows rather naturally here because there is a rather discernible disconnection between individuals and social groups in relation to the ‘how’ ‘what’ and ‘why’ of *digital* privacy altogether – a significant difference from the lessons of the histories of privacy.

Contemporary Digital Privacy Literature

To think about, with and through digital privacy from a scholastic standpoint presents numerous logical and theoretical challenges because the concept of digital privacy itself is not the intellectual child of any single field. The literature reviewed here comes from numerous different fields and subfields of scholarship from both the social sciences and hard sciences. The fields, in many ways, engage with one another so as to enrich their own understanding of what

digital privacy looks like and of the different modalities through which digital privacy is implicated by the flows, interactions and events of daily lived experience both online and offline.

Communications Studies scholarship has been particularly interested in charting surveillance practices in and around the sites and methods upon which privacy is infringed, as the field is particularly well suited for intersecting mass, open and closed communications systems (for example, the relationship between police communications systems carried out over public Internet access points), interactive media, information studies and social inequality (Gates and Magnet, 2007). Along such lines, one of the most prominent contributors to studying privacy vis-à-vis surveillance is Greg Elmer's (2003) exposition on the various forces, institutions and processes through which information about Internet users (in general, and consumers in particular) is captured, analyzed and sold for profit purposes. While the bulk of the work is focused on the concept of surveillance as opposed to privacy explicitly, it is significant for privacy studies because it assists in formulating the basis through which diagnoses, arguments and prescriptions for and of privacy unfold.

More explicitly upon the matter of privacy, Communications Studies is also particularly commanding upon the subject matter of incursions, violations and threats to personal privacy. In fact, the field began charting privacy problems before the turn of Age of Information. Gumpert and Drucker (1998) delineate a general change in social issues (i.e. increasing intrapersonal community integration) and economic developments throughout the 1970s that precipitated and accelerated the incursion of privacy by telecommunications technologies entering the consumer marketplace throughout the 1980s. Communications Studies has also been particularly proactive in offering new theoretical models of anonymous communication to re-visit and re-articulate how we as scholars understand the extents and constitution of privacy altogether (Scott, 1998),

alternative theoretical explorations of the differences between private and public communications so as to generate new insights into the nature of digital privacy and threats therein (Rawlins, 1998). The field has also made notable contributions upon theorizing the nature of identity in the digital realm, particularly in and around notions of precisely what constitutes a digital identity (Hodkinson, 2017; Wessels, 2012) and how groups formulate their own identities (Livingstone, 2008; Agosto and Abbas, 17).

The field has also been actively involved in prescribing ways in which personal information ought to be protected at various levels of intervention. For example, through the cultivation of new analytical typologies to encourage progressive academic engagement with the nature of privacy threats (Crowley, 2017), as well as through the development of literature analyzing the varying degrees of success latent in popular privacy protection mechanisms on websites (LaRose and Rifon, 2006), Big Data analytics groups (Baruh and Popescu, 2017) and social media companies (Aroldi and Vittadini, 2017).

Communications Studies scholarship upon privacy studies tends not to articulate how the individual acts as an agent of her own digital privacy. As will be demonstrated below, there is a general issue throughout most interdisciplinary, social scientific and humanities research fields when studying privacy in the sense that large scale catalyzers of information violation tend to be treated throughout large scale intervention. The question of the role of the individual is not self-evident, nor is there much indication that individuals *can* play a role in their own privacy altogether. Communication Studies has significantly outlined the various processes of surveillance, a multitude of ways of theorizing the spaces and places of privacy and prescribed a wealth of different avenues through which personal information can be protected. Alas, the individual, smaller-scale efforts – from individuals such as users themselves, including coders –

generally escape analytical and conceptual consideration within the field.

Another widely recognized field upon privacy scholarship is International Law. Numerous guides have been produced in the past two decades by legal practitioners and philosophers so as to primarily assist different entities, whether corporations or governments, in identifying and overcoming the challenges that international law imposes upon the economic and political activity of each respective entity's civic, political, social, cultural, economic and diplomatic digital presence. A concentration of scholastic preoccupation within international law, for example, has a sustained call for greater co-operation between European member states and the European Union in adopting international privacy law frameworks into domestic legislation (Westby, 2004; Svantesson, 2015; Dowling, 2009). The general contribution the field makes to the dissertation is constellating the 'burden' of responsibility on the behalf of corporations and governments in attending to digital privacy infractions. While it is indeed the case that this body of scholarship is rather evidently designing policy and best-practice orientations for these entities, the scholarship makes quite legible an issue with relative scalability: as digital theft, terrorism and hacking violations continue to grow exponentially, so too does the perception that digital privacy *ought* to be handled by entities large enough to counter the size and frequency of privacy violations.

The limitation with this approach however is that it tremendously isolates individuals and social groups from the equation altogether. If digital privacy is a right in the case of a constitution or governmental law, or as a right in the case of a corporate customer or employee, the scalability has essentially removed individuals and social groups of their agency (let alone the relevance of their opinions or voices) from the protection process altogether. A noteworthy exception is found in Nissenbaum's recent (2009) work calling for all legal approaches to digital

privacy to maintain a contextual integrity when attempting to organize catalysts, stakes and prescriptions, which calls for the inclusion of the perspectives of social and cultural groups. Aside from the exception, a similar register of contributions and limitations arises from the social sciences as well.

The fields of Political Studies and Political Science, particularly the subfield of policy analysis, has been notable strides in the larger scholastic effort to constellate the burden of digital privacy protections as too in the effort to chart how digital privacy comes to be violated. And so their efforts mirror those of international law scholarship with a slight shift in normative orientation. While the constellating of protection processes continues to emphasize the responsibility of governments and corporations in protecting digital privacy, this body of scholarship differs in the sense that it identifies governments and corporations themselves as the culprits of privacy violations. For example, there is a noteworthy emphasis through the past two decades upon calling upon domestic government policy agendas to become more transparent in private sector personal data collection and treatment because the nature of how information tends to be handled by these entities leads to accidental loss from reckless transportation or storage practices as well as general issues associated with information access abuse, breaches of trust and a lack of oversight protocols (Alexander and Pal, 1998; Grant and Bennet, 1999; Leuz, 2006).

These fields contribute a different register of calls for protection that international law in the sense that the 'who' and 'what' of the burden of protection responsibilities rests not merely with governments and corporations but within university research centers as well. Since the late 1990s, there has been a string of political studies scholarship advocating for the development, adoption and usage of privacy enhancing technologies, for example, to aide corporations and

governments in protecting the digital privacy of not only themselves and their employees but of the general population to which they tend to engage on a daily basis (Cavoukian, 1998; Goldberg, 2002; Oliver, 2003).

More interdisciplinary approaches under the general rubric of Political Science and Political Studies, such as International Political Sociology and Surveillance Studies, tie together the technical, social and ethical implications of surveillance in the twenty-first century itself (Bauman and Lyon, 2014; Muller, 2010; Peoples and Vaughan-Williams, 2010). For example, numerous works contribute significantly to how social scientists come to understand precisely how the individual member of society is implicated by pervasive, globally-reaching hacking, surveillance and theft preoccupations (de Goede, 2014; Bellanova, 2014; Amore, 2014). What these fields and its literature generally demarcate is that individuals and social groups tend to be almost entirely divorced from the process of articulating how their security is provided to them. When it comes to the security of personal information, the protection process is formulated, negotiated, cultivated, executed, managed and maintained almost entirely within the realm of corporate and governmental regulation and control. As such, the protection process omits direct action – let alone influence – from the individuals and social groups upon which the process is otherwise designed to serve. There is an exception through the work of Colin Bennett (2008) for example, as his emphasis on the development, inclusion and co-operation between even the smallest privacy advocacy networks ought to bridge the gap between large-scale digital privacy entities and the common individual, alas the extent to which these connections incorporate individual voice tends to be marginalized by the narrative strategies of these networks as they engage politics and politicians on both domestic and international levels.

The hard sciences, particularly the Computer Sciences, have played both implicit and

explicit roles in mounting, clarifying and extending the arguments and orientations of all of the aforementioned literature. The subfield of Information-Technology Security has sustained inquiry into the practical and scientific nature of both privacy invasions and privacy protection from a computer programming and programming architectural perspective. From a programming language perspective, Marcella (2003) contributes significant legibility to how the social sciences in turn might frame precisely how malicious software accesses information, as well as how protection software can counter such incursions. Similar sentiments are forwarded by Acquisti (2007) but positioned in a different logical sequence in the equation of invasion-protection analysis, particularly by emphasizing that digital privacy begins through counter-surveillance and pre-emption/monitoring software technologies. The fields contributions are not restricted entirely to the empirics of programming as there are clear calls for a more comprehensive social adaptation of advanced cryptographic software (Dingledine et al., 2004) and for more ‘ethical’ hacking into digital network security mechanisms to create new data protection mechanisms (Bodó, 2014).

While the field generally advances how the social sciences imagine and articulate the technical nuances of protection and invasion, it is also generally limited in a similar sense to the aforementioned fields. Unless individuals and social groups access the technological literacy to mobilize this knowledge on their own, it tends to be accessible only to scholasticism with the resources to mobilize programming knowledges. It is important to note that despite strides taken by the computer sciences in making their works accessible, significant graduate level academic training in the social sciences seems a prerequisite from accessing the kinds of suggestions and contributions programming literature provide altogether. The next logical challenge in the genesis of the dissertation itself is connecting digital privacy to noise, which is the next body of

literature to be reviewed. As the thesis argues, noise is a specific modality through which privacy unfolds. This is particularly conceivable by abstaining from thinking about noise as merely unwanted sound, for it is also the presence of grey-ness, static and blurriness. As such, its deliberate and even accidental placement upon and around knowledge, objects and space creates obfuscation, confusion and misdirection. The section to follow demonstrates that noise is, like privacy, a very social preoccupation and one that can be re-deployed as an alternative theory for thinking about, with and through the ‘how’ and ‘what’ of digital privacy.

Part Three: Noise-oriented Literature

The absence of something akin to an inter or multidisciplinary ‘noise studies’ field compels the dissertation to engage ‘noise-oriented’ scholarship across both the social and hard sciences. What the collection of noise-oriented scholarship contributes is a logical and conceptual avenue through which noise can be articulated as a social activity. While one of the pieces of literature (cryptographic science) opens up noise as a social modality of privacy, they generally are explored because of the ways in which the set-up the conceptual space required to make the connection later (during the chapter’s theoretical framework). There are four different (and rather unrelated) fields of literature engaging noise under consideration, all of which demonstrate noise as a *direct* social activity – something akin to the conscious and deliberate act of being loud, interruptive, aggressive, or merely ‘noisy’ so as to produce certain goals or outcomes: Acoustic Ecology; Linguistics Studies; Communications Studies; Cryptographic Science.

Acoustic Ecology

The field of acoustic ecology is particularly important because it explores the negative effects of acoustic and physical noise upon the lived experience of the human biological body. In particular, it explores the effects of acoustic noise upon the human body. The central contribution the field makes to the dissertation is the way in which the scholarship correlates noise as a social process unto itself. From literature exploring the effects of human naval shipping traffic on ocean surfaces upon marine life (Clark et al., 2009; Hildebrand et al., 2009; Sousa-Lima and Clark, 2016) to the effects of human construction upon bird song alerting distances (Barber, Crooks and Fistrup, 2010) and windmills upon bird migration patterns (Devereaux, Denny and Wittingham, 2008), acoustic ecology invested considerable research energy in the late 2000s into the relationship between noise and human social activity, particularly as a force that mitigates the lived experience of both humans and animals in a wide range of contexts. But perhaps most significantly in terms of human noisemaking upon human experience within the field of acoustic ecology comes from Westerkamp's research on *Muzak Corporation*. Westerkamp argues that since the company's foundation in the 1930s, their efforts to transform existing libraries of musical recordings to play in the background of office places instantiated an industry-wide movement to socialize to become not only a tool to cultivate greater workplace efficiency, but also in catalyzing American society throughout the twentieth-century to 'need' to listen to music outside of the workplace (Westerkamp, 1988, 46-9).

To Westerkamp, popular music and the otherwise enjoyable pastime of 'listening' to music forever transformed into noise – a collective sanitization of music's artistic value, a technical persistence that reduced music to a reverberating energy (Westerkamp, 2002). Conversely (and although not fundamentally belonging to the field of acoustic ecology, but

dovetailing nevertheless due to the ecological tone of his analysis of noise) Attali's *Noise: The Political Economy of Music* (1997) contributes a way linking noise to social and political protest. Attali argues that music orders society, and as such, thus also channels political power itself – one modality through which channeling is realized is through music's opposite: noise. Attali argues that the North American mainstream media industry manipulates social ideals about 'good' music by essentially dictating what is 'bad' music, or 'noise' (Attali, 1997, 26). In his discussion of the controversial live performances of musical theorist and composer, John Cage, Attali discusses the ways in which Cage harnessed noise to protest against mainstream ideas of 'good' music, specifically by forcing his audience to wait for long periods of time in silence before the performance began, essentially encouraging the audience to become noise in their impatience. To exacerbate the situation further, Cage often opened the doors of his concert hall to the street outside, inviting the world's noise into a place that tends to otherwise be imagined as distinctly and purposely quieter than the world outside.

Attali exemplifies how noise is not only inherent in the social body as a means of expressing discomfort and resentment, but also how noise becomes a specific modality through which social and political arguments are, rather axiomatically, realized through the harnessing of acoustic interference. The limitation of scholarship in this area is the scale of its critique. Partial to sociological description, the field has a methodological tendency towards choosing objects-of-study in sizes between social groups and entire populations. The issue at hand is that there is little conceptual or theoretical space to articulate noise as a human process that can be individually associated. What is at stake for the dissertation here is the lack of a conceptual building block for exploring how individual noise making can affect social experience (and as will be discussed later, entire social systems). This issue is replicated elsewhere as well, but there

are fields – such as linguistics studies – that do assist the dissertation here by providing a crucial building block that begins at the level of analysis of the individual human being. Particularly, human vocal chords.

Linguistics Studies

The field of Linguistics Studies may seem at first glance a curious fit for review and contribution to the purposes of the dissertation. However, it is an important component for two reasons. The first is that the field of Linguistics Studies has a sustained and rigorous engagement with the notion of noise. Secondly, the field identifies that noise is not only a byproduct of human language, but a fundamental component to human linguistic communication (and thus human sociality) itself. And it is here that its primary contribution is made. The scholarship identifies, for example, how tongue and throat movements that produce sounds, such as the ‘clicks’ made by drawing the tongue away from the upper molars on one side of the mouth, are fundamental pillars of meaningful, linguistic sound structures (Katamba and Dobrovolsky, 2011, 16-20). In the subfield of Phonetics Studies, noise is being re-conceptualized as its own sound class, something that is not merely a fundamental acoustic phenomenon to be harnessed and controlled by the human herself, but also as an independent component with its own ontological significance within the field of study itself (Bloch-Rozmej, 2011, 13). What the literature contributes is thus a different epistemological posture on the concept of noise itself – at once a necessity and prerequisite to human social activity altogether. In order for humans to engage in social relations in the first place, ‘noise’ and the mutual management and reciprocation of systems of noise postures the notion itself as a precondition to all social relations and systems thereof. Simply put, this field of study posits very directly – and very similarly to Serres’ (1982),

which will be reviewed below as a crucial theoretical component to the dissertation – that noise makes possible social relations altogether.

The limitation of the literature however is that – conversely to acoustic ecology – there is little room for conceptualizing the relationship between human communication on an individual basis to human communication on a societal basis. Enter the field of communications studies which assists the dissertation just a bit more in locating the building blocks necessary for a more comprehensive theory.

Communications Studies

The field of Communications Studies launched into decades of research surrounding noise a social phenomenon, social consequence and particularly as a social detriment. This began through Shannon's (1949) "A Mathematical Problem of Communication". Shannon explores noise in electrical communications systems, referring to it as excess information that undermines the statistical certainty of receiving, interpreting and understanding a message. This notion of noise to Shannon is something disruptive to communication but also something inherent to communications systems – something that can be collected, analyzed and mounted upon for building more accurate and scientifically reliable models for human interaction (Wiener, 1965, 10). It is important to note that the basis for Shannon's work stylized noise as a technical issue, not a social issue. His research intended to increase the efficiency and reliability of telephone cables and radio transmissions. As such, his primary audience was engineers and computer scientists. By making information 'measurable' through his model, for example, he contributed to the hard sciences a mathematical study of information, which spawned further theorization about the technical nature of 'information' itself (Golomb, 2001).

Beyond the hard sciences, Shannon's work did make a significant impact upon the social sciences but one that was very limited through sustained social scientific critique. For example, Shannon's model of communication has been attributed as a foundational text behind the emergence of the field of Communications Studies (Fiske, 1982). This is because of the way in which his model became a metaphorical and heuristic device for studying social life around communications systems. For example, it has been used to build new historical arguments upon how nineteenth-century society believed information moved – a process that was, at the time, synonymous with the movement of goods and people, or 'communication' (Carey, 1989). It has also been used to describe the process of communication during the mid and later parts of the twentieth-century (Reddy, 1977). But as de Vries (2012) deftly describes in his account of the emergence and influence of Shannon's work, Communications Studies scholarship quickly recognized that the popular influence of his mathematical model of communication increasingly ignored the heavily quantification-oriented nature of the model itself. The model, rather inappropriately, became a "one-size-fits-all blueprint that seemed applicable to both quantitative *and* qualitative acts of communication, including the perfect transfer of thought and meaning" (de Vries, 2012, 63-4). The purpose of the inclusion of the model in the social sciences, as de Vries notes further, was not merely heuristic or metaphorical. Shannon's model founded a taken-for-granted belief in the social sciences that the concept of 'noise' – not merely technical, but semantic interference in the study of human language and signs – could be isolated and erased (de Vries, 2012, 64). De Vries argues that the obsession with Shannon signaled a common desire for many social scientists to banish obstacles in communication in hopes of creating error-free information transfer systems. De Vries argues this also created longstanding academic "aversions to noise" (de Vries, 64).

While contemporary Communications Studies scholarship has heavily criticized Shannon's model of communication heuristically, metaphorically and theoretically, de Vries' point about the field's "aversion to noise" remains today – at least in part. For example, noise has been utilized as a flag for semantic and discursive analyses of media organizations, signaling evidence of media bias (Nevitt, 1981), and even perceived as 'lag' itself that obfuscates the presence or possibility of 'meaning' in the information society (Klapp, 1982). Perhaps most interestingly for the purposes of the dissertation, Dolan (2008) identifies the soundscape of the public, particularly in urban city centers, as a key obstacle to the personal and governmental development of what he perceives to be a desperately needed strategy for individual privacy. Crowcroft (2007) identifies the range of existing arguments in Communications Studies over the discourse on net neutrality are producing 'noise', or an obstacle that impedes the ability to understand the 'best' way to provide net neutrality worldwide. Information theory scholars, dovetailing the aforementioned scholars within Communications Studies as a subfield unto itself, displays similar tendencies. Fulton (2009) refers to the notion of noise, conceptualizing it as semiotic interference between individuals attempting to understand one another as they communicate. Day (2009) targets noise as an obstacle to the development of semantic meaning that hinders the development of new theoretical models of present-day communications systems (Day, 2009). What these particular academics have in common is their mutual identification of noise on a specifically negative register. Noise, simply put, is a problem. Noise is a destructive social phenomenon, something to be eliminated and as such, something that requires 'fixing'. But this is not the only way the field of Communications Studies has interpreted noise.

Noise has also been identified as a 'positive' social phenomenon for some Communications Studies scholars as well, or at least as a social or conceptual phenomenon that

does not necessarily need to be resisted. For example, Hainge (2007) discusses that most communications systems theories within the field of Communications Studies fundamentally misunderstand the value of ‘noise’ in the function of human communication. He argues that on the one hand, noise cannot be eliminated. It must be identified and worked with as such. On the other hand, the presence of noise can be utilized technically so as to compress signals and make content more legible and discernible as such. St. Pierre (2015) argues that while the liberal humanist and late-capital models of communication attempt to remove noise in order to make communications systems more efficient, noise itself is a modality of critique and expression from disabled speakers and post-human bodies (St. Pierre, 2015, 330). Alongside a post-human perspective, similarly observing that the concept of noise itself is generally seen as a negative concept within Communications Studies due to the influence of Shannon’s model and Cybernetics theory (which popularized Shannon’s model, specifically vis-à-vis Weaver’s work on Cybernetic theory in the 1950s), Gunkel (2000) argues that an internal debate within Cybernetics theory scholarship created an opposing perspective that emphasized reflexivity (as opposed to the prevailing homeostatic attitude towards communications systems thought). The effect of such scholarship was a transformation in how noise was perceived: as something of a ‘virtue’ (Gunkel, 2000, 343). The idea of noise as a ‘virtue’ is derived from Mattelart and Mattelart’s (1992, 45) theorization of cyborg subjectivities – a humanities trend at the time, popularized by the third wave feminist scholastic movement beginning in the late 1980s, conceptualizing the state humanity as a hybrid of biological, technological and extra-corporeal lived experience – whereby there is no ‘goal’ of communication. Rather, indeterminate exchanges between people and information systems are meaningful on their own terms, thus positing that ‘noise’ itself is not merely ‘good’ nor ‘bad’, it just ‘is’.

Taken together, the field of Communications Studies' engagement with noise was birthed vis-à-vis Shannon through the popularization of his mathematical model of communication. Despite its serious limitations as a misplaced model for understanding communications due to its solely quantitative approach, it left a significant impact upon following scholarship with regards to understanding and approaching the concept of noise. Particularly in the sense that Communications Studies scholars began situating the concept of noise as a social activity and phenomenon and not merely a technical phenomenon or technical issue. However, a limitation of the field's engagement with noise comes from Shannon. As they mobilized the concept outside of technical studies and into study as a social phenomenon, they carried with them Shannon's tendency to 'judge' noise on purely normative terms – as something 'bad'. Departing from Shannon's influence, there is evidence in the field of scholarship approaching noise on a completely different normative register. As something 'good' for the post-human body and disabled speaker, for example.

Alas, the overarching limitation of the field upon the study of noise overall is its tendency to execute value-laden approaches to the concept of noise itself. What is required is something more along the lines of Gunkel's appraisal of noise as something simply 'present' and can be assessed on 'its own terms' without normative judgement. Gunkel's approach brings the dissertation the closest to an understanding of noise without normative bias, but it is only contextualized in post-human terms where the stakes for contemporary privacy are far less important. Noise still needs to be acknowledged as a purposeful social activity as opposed to a feature of indeterminate dialogue between cyborgs – as something that of a variegated phenomenon caused by actors in the name of privacy, effecting and influencing behavior upon social and technical systems. But always in 'good' and 'bad' effects taken together, never one

without the other. Or simply put, beyond a purely normative appraisal. But prior to doing so, the chapter now turns to cryptography as an example of noise-oriented literature that explores social processes through normative bias but on a very different value register altogether.

Cryptographic Sciences

Cryptography, or the study and practice of concealing messages, is the subject matter of the Cryptographic Sciences – a field that is more generally attributed as a subfield of Computer Science and Computer Engineering. The Cryptographic Sciences is a body of research that is particularly important to the dissertation not only for the ways in which it extends the connection between noise and the social into something of a unique register of human communication and expression, but also because of the increasingly prominent role it plays in contemporary digital privacy. The earliest historical examples of cryptography are found in the practice extend back to ancient Greece. In *Herodotus*, the early fifth century Milesian Histiaeus is described as needing to send secret word from his court to Darius, his son in law, the despot Aristagoras at Miletus. Secret word was sent by shaving the head of his most trusted slave, and tattooed a message on his head and waited for a new crop of hair to grow in before sending the slave to his son in law (Reinke, 1962, 114). After the slave arrived, Aristagoras shaved his head, revealing a message urging him to revolt against Persia. Similarly, when Xerxes planned his invasion of Greece, the Spartan Damartus - an exile at the court of the King at Susa - warned his country by sending a wooden tablet covered with wax, to be later melted off to reveal the message (Reinke, 1962, 113). These two examples contribute a general linkage between the process of deliberately creating noise – hair and wax – to hide information.

As a modern and more pertinent historical example to the purposes of the dissertation, the

second world war case of the *Enigma Machine* – an electro-mechanical rotary-operated cipher machine used to protect commercial, diplomatic and military communication – further demonstrates the usage of noise to conceal information. Invented by German engineer Arthur Scherbius at the end of world war one, the enigma machine became central to military communications for Nazi Germany throughout the 1940s (Christensen, 2007, 247). The machine itself functions through the combination of mechanical and electrical systems involving a keyboard, a set of rotating disks arranged horizontally along a spindle, and a variety of stepping components that turned one of the disks as keystrokes were depressed by the machine's user. The problem with the enigma to the Allied war efforts was in the inability to decrypt the enigma's messages. The problem was a political problem, one that required mathematical theory to address. Enter A. M. Turing's "Computing Machinery and Intelligence" (1950), which theorized whether machines can think, or what Turing proposed as a conceptual problem called *The Imitation Game*. The game is based upon a hypothetical scenario wherein a man or woman is being interrogated, and premised that the individual being interrogated will do everything s/he can to mislead the interrogator. The game involves a machine that plays a central role in calculating the game's outcome, so much so that it raises key questions about whether or not a machine can think or behave like a human – questions that have fundamentally impacted the ways cryptographic sciences contribute to the contemporary production of noise to conceal information. The limitation of the cryptography upon thinking about thinking noise as a social process is it tends to imagine noise as something completely discernible – like written human language. The notion is constraining because it fails to account for the unintentional and more political effect of the usage of noise upon social life.

Taken together, from Acoustic Ecology to Cryptography, noise-oriented scholarship

contributes a way of thinking about noise as a social process and activity. A social process and activity harnessed to achieve certain outcomes, politically, socially, economically, culturally or otherwise. The problem, however, with the scholarship is twofold. First, the literature assumes that noise is controllable. What all of the aforementioned literature implies, as it is certainly not explicated nor self-evident, is that noise produces generally negative results but in a way that is generally unpredictable. Noise is not simply a sharpened or well defined tool to be applied to a specific problem. Like the way in which Westerkamp's (1988) review of *Muzak*, for example, denotes the way in which noise dissolves one's relationship to music as something enjoyable, something like a pastime her account cannot take into consideration the range of effects as they are individualized. Noise in her study is a conceptual one. She offers an abstracted argument about the gradual transformation of music into noise vis-à-vis deliberately political processes, but one that unfolds over a long period of time. Her analysis does not take into account the context and variability upon which the degradation of an individual's relationship to music occurs. This is because of the nature of the relationship between the researcher and subject matter of noise itself.

Like the way in which the deliberate introduction of noise in cryptography-based anonymity systems assumes that a message will be perfectly concealed, the process of decryption and deciphering often fails under the weight of its own preoccupation; the Enigma coding machine was indeed deciphered but took tremendous human effort and virtually countless failures before a routine and protocol was established for deciphering messages. Moreover, the nature of digital cryptography today demonstrates – and as will be discussed in more detail in the coming chapters – that hacking attempts are becoming increasingly more sophisticated. So much so that many standards of noise-introducing encryption are rather easily 'cracked'. The point

from both examples is that most literature engaging noise tends to assume noise is well-controlled beyond the point of slippage, loss and risk.

Secondly, the literature assumes that noise almost always introduces a negative effect. Whether noise interrupts communications systems (Shannon, 1949) or conceals information (Turing, 1950), noise is almost always concealed as a deliberately antagonizing process upon social life around it, or as a force that prevents social life from engaging itself or neighboring social relations/actors. There is very little evidence or indication within the literature that noise might yield more ‘positive’ normative outcomes. But even if that were the case, it is not of concern to the dissertation here. What is at stake with the normative approach to noise is that it does not identify noise as a force that produces *variegated* results on social relations and systems of social relations thereof.

For example, consider the following questions: can the application of ‘annoying’ sounding music (or *Muzak*, for that matter) affect two neighbouring office spaces in the same way? Is it possible that some individuals may not experience, as Westerkamp argued, a degradation or loss in their relationship to the music they otherwise enjoy? Can noise be subjective in its outcomes, and perhaps more importantly, can noise affect and produce differentiated types of behavior and differentiated types of change in social relations and social systems? In order to answer these questions, and in order to amend the issues of the normative treatment of noise – along with the deterministically derived belief that noise can be completely harnessed and controlled – the chapter now turns to Serres’ (1982) *Parasite*. His work founds the core of the dissertation’s theoretical backbone precisely because his approach to noise not only identifies noise as a very particular social activity and preoccupation (and as we will see, one that can be deliberately oriented towards the process of privacy-making itself), but also because he

theorizes noise as a slippery, elusive object that produces often unpredictable outcomes – outcomes that spell tremendous change for the social relations and systems it latches onto.

Part Four: Michel Serres – Parasite

Serres' *Parasite* is introduced at this stage in the chapter (and is fundamental to the theory of the dissertation) because of the way in which he theorizes noise itself as the most essential characteristic of social life. Noise preconditions, creates, enlarges, mediates, diminishes and even destroys all social relations between living beings. He explains his theory through the analogy of a parasite, and his understanding of the parasite is derived from the French language. The French word *parasite* refers to three things simultaneously, and inextricably so: static; a biological parasite; a social parasite (Serres, 1982, vii). The first two understandings are familiar to the English language, but the last is absent from the English definition. To Serres, it refers to *social* infections, of the ways in which living beings infect one another's relations by producing *noise*. Prior to explaining precisely what Serres means by noise here, a brief outline of the nuances of his social theory are provided, which is followed by their contributions to the dissertation. The limitations of his theory will be exposed thereafter, but prior to wrapping up all of the aforementioned bodies of literature in terms of the gaps and theoretical implications they leave upon the dissertation itself.

The first contribution *Parasite* makes then is the way in which noise is articulated as an *implicating force derived from all social activity*. What Serres is essentially contributing is the idea that social actions – whether verbal as in speaking, literary as in writing or reading, discernibly interactive as in exchanging data on thumb drives or subconsciously implicating as in the effect of subtle body language between the brief moment of recognition between complete strangers in a city square – produce noise. Or simply speaking, all social actions and social

activity are distinguishable as *noisemaking*. The essence of Serres' conceptualization is the idea that prior to any two beings having a relation to one another, an otherwise excluded being (like a person) or phenomenon (like the effect of a car horn in an otherwise quiet park) can instantiate a relation between those two beings. Whether significant or casual, that noise can bring them together and formulate a relationship. That same being or phenomenon, or what Serres might otherwise simply refer to as a *parasite* (that makes noise), can affect previously existing relations between two or more beings by way of permanently affecting the relation itself. Serres demonstrates throughout the entirety of his book how relations affected by otherwise excluded social activity (or noise) can mediate relations. It can strain the relation, strengthen the relation, become a catalyst in instantiating a permanent metamorphosis by including new networks or destroying the relation altogether. This brings the chapter to the second contribution Serres makes to the dissertation – the way in which his social theory about noise is *also* a theory about the evolution, mediation and destruction of entire social systems as well.

The second contribution Serres makes can be most conveniently accessed via his first chapter discussion of Bourgault's *Fables d'Espose* – a story of a city rat that invites a country rat into the home of his master for dinner. The rats feast on leftover scraps of food that his master and his guests drop on the floor. The rats feast, and it costs them nothing. The master is not aware, nor are the guests. Through the story of the city rats, Serres constructs the basis of a social system – between rats, a homeowner, the guests and the home itself. The rats, are parasites – they embed themselves into relations between the home owner, his food, his labour, his material possessions and his social life. Where things become interesting is when a loud 'bang' at the front door occurs, a knock perhaps, that frightens the rats and grabs the attention of the diners. The country rat flees home to the countryside, while the city rat flees momentarily but returns on

his own later in the evening. This second event, of the sound interrupting the feasting of the rats, is a fundamental conceptual feature of Serres' account. It reveals how noises – made by social actors – enter into and effect social systems. The sound itself is unknown in the story and to the reader. It may have come from the door, but it may have also been a creak in the floorboards, or perhaps an angry neighbour. The unknown-ness of the sound is significant because it liberates the conceptual space for imagining how social systems evolve. This sound is essentially information itself – a mechanism that not only fundamentally interrupted the social system of rats, food, home and social life, but fundamentally re-deployed it as well. The noise is a message of panic, one that ruptures or departs other information from itself (Serres, 1983, 3) before new information can be made discernible, legible and useful with regards to understanding any semblance of sociality in the home altogether. The noise also temporarily rids of parasites, at least some. This benefits the home owner himself – who happens to be a parasite himself; the food the rats were feasting on was taken as tax from the home owner's neighbours, who are guests themselves at his dinner table. And so the noise is at once a social problem, social solution and conceptual ambiguity all at once – but *never* one without the other. Accordingly, noise is recognized as a phenomenon that affects the daily activities of social beings and social systems in a variety of *variegated* ways. And because of the way in which it can scare another actor or parasite away, the noise is even responsible for creating new social systems from old ones.

There are two limitations with Serres' *Parasite*. The first is Serres' noise and social systems theories are contextualized largely through literary examples. From Homer's *The Odyssey* and Plato's *Symposium* to Rousseau's *Les Confessions* to Xenophon's *The Art of Hunting*, Serres' methodology presumes at times that literary devices, imagery, metaphors and allegories – despite exhibiting radically different metaphysical presumptions of their own –

translate to ‘reality’; there is a significant absence of interpretative flexibility due to the textual tone around the narratives, metaphors, allegories, myths, and other literary devices that essentially composed Serres’ subjects of concern. And so the question is raised, in what ways can the logics underpinning Serres’ theory on noise and social systems be articulated outside of literary scholarship? And perhaps most importantly, how might these differences be reconciled in a digital context?

The second issue follows accordingly, in that Serres’ work is inescapably Nihilistic, which implicates his analysis privacy – which is *the* central object of study of the dissertation. A significant body of scholarship have made similar comments about the inherent pessimism of Serres’ theories. While they seem to accentuate how noise makes systems unique in terms of the variegated nature of change they experience by noisemaking, most of his examples tend to collapse to a defeatist, pessimistic critique (Enns, 2009, 170-1; Crocker, 2007; Gullestad, 2012). His theory of social life and social systems leaves little room for the imagination to think beyond dynamic themes of ‘infection’, ‘sickness’, ‘chaos’, and ‘disorder’. The popular image of the parasite itself, let alone phenomenon-laden noise, is hardly welcoming. The texts and imagery that Serres analyzes, which happens in no systematic order, compound the experience of darkness as well. The outlook is problematic for the purposes of the dissertation because of its negative tilt. Take, for example, Serres discussion of privacy itself. What may otherwise be a rather pertinent context through which his own theories of social noise and social systems intersect with the case studies of the dissertation, rather unfortunately, it collapses under the weight of his theory’s pessimism (Serres, 1982, 128-30).

To Serres, privacy is the product of social parasitism – of people taking what ought to be otherwise completely public space as afforded by Rousseau’s *Social Contract* (Serres, 1982,

144). Privacy is a closed thing, he writes. It is founded upon murder and war. To hold a thing in a bag is to take away from the public what should be a collective commodity or good. To conceal is to hide as personal property. Moreover, the chainsaw and bulldozers, piercing the air of public space, or the belching of social deviants in crowded corners, segregates space and makes it their own (Serres, 1982, 142). To hold bodies through stench, proclamation, and physical displacement is a story of noise - acoustic and otherwise - as an agent in the collapsing of shared areas. “Don’t bring your shit into my house anymore, a philosophical boss said to me recently when he thought I was an adult” (Serres, 1982, 144). The point being here is that Serres’ conceptualization of privacy is severely limiting. And so, the next section of the chapter will address all of the limitations in terms of the conceptual and theoretical gaps they leave open, which will be subsequently filled in the chapter’s concluding section.

Part Five: Gaps

The limitations of historical and contemporary privacy literature, noise-oriented literature and Serres taken collectively illuminates significant theoretical gaps that the end of this chapter will plug. But prior to doing so, this section outlines what those gaps are and explains why they are significant. Moving in order of the literature reviewed throughout the chapter, and then finishing with more general discussion of overarching issues with all of the literature collectively, the first significant issue derived is the tension between historical and contemporary privacy scholarship. The historical scholarship made rather legible that individuals and social groups indeed play an intimate role in playing out, structuring and acting upon their own spaces, places and contexts for privacy while contemporary scholarship demonstrates that governments, advocacy networks and corporations carry out privacy not only for themselves and their

employees/servants but for individuals and daily life as well. A gap thus exists between privacy-for-individuals-by-individuals and privacy-for-individuals-by-institutions; the former is accounted for historically but not contemporarily. A naturally following question asks, how might individuals play a role in structuring their own privacy today, particularly online?

A second significant gap found between historical and contemporary privacy literature is the absence of technology itself as an (f)actor in the equation. Indeed, technology – in the widest and most philosophically tolerant sense – factors into essentially every piece of literature reviewed regarding privacy, whether historically or contemporarily. Hooke and Boyle’s vacuum pump played an intimate role in the shifting degrees of privacy in their home/laboratory/apothecary. The personal diary and written astronomical observations themselves are as much scientific and personal technologies as they were political technologies in altering how and whether John Herschel revealed the details of his private life and experiences throughout his cape voyages. And from a more contemporary standpoint, Cavoukian’s discussion most accurately reflects the context of ‘technology’ in relation to digital privacy thus far. But the point however is that technology is only regarded as a factor in digital privacy, and not an *actor*. Technology is not discussed as having any capacity for political action/agency unto itself, in any way, shape or form in any of the literature reviewed. And so, the final section of the chapter addresses the significance of this logical and conceptual gap by inviting the logics of object-oriented ontology to the dissertation’s methodological considerations, specifically through Latour’s (2007) contributions to Actor-Network Theory.

As has been argued elsewhere (Cooke, 2015), the conceptual treatment of digital privacy by most scholarship today tends to overly victimize ‘digital privacy’. The subsequent issue is that ‘digital privacy’ has been arrested in the mind of most scholars’ and readers’. It has become

a static idea, something that everyone feels as though they are entitled to (whether via policy or law) and feel is important to their daily social life, but not as something like a modality for expression and engagement. For example, most contemporary digital privacy literature emphasizes the ‘invasion’ ‘theft’ and ‘violation’ of digital privacy. It is docile. It is fixed. It is the receiver of political agency, but never a giver of political agency. The point is that most digital privacy literature tends *not* to theorize, let alone often conceptualize, how digital privacy is *expressed* and how it is *acted* upon. If digital privacy were to have something of an agential dimension or capacity, a way in which individuals or social groups could *use* digital privacy as a tool for political purposes, the point is that the conceptual space through which this might otherwise be imagined has been robbed by a growing trend in intellectual insulation. Digital privacy today, unlike the historical investigations reviewed earlier, is not imagined as the culminating force (and as force unto itself) mounted by social interaction and social expression itself. And this is precisely what the chapter will address after the gaps in noise literature are addressed.

The first significant gap imposed by noise-oriented literature is that it assumes noise is something that is predictable. To Shannon, noise can be measured by electro-acoustical devices. It is something that can be anticipated, and so it is also something that can be managed by manipulating variables of existing electronic, or building new ones with the sole intention of mitigating noise. To Westerkamp and Attali, noise disrupts social spaces by opening doors, or turning on speakers in office buildings. Conversely, cryptography studies approach noise as inherently social - a practice of deliberately (mis)shaping and contouring otherwise discernible language, whereas the field of linguistics studies ventures far enough to argue that the acoustic resonances of the human physiology precede physical human communication itself. Noise, here,

is a matter of structuring the sounds of the human vocal chords into coherent systems. There is indeed something unsettling about the conceptual status of noise through these veins of literature. Noise infers messiness, discomfort and as such, relative degrees of unpredictability, all of which tends to disappear once ‘noise’ is taken up as an object of academic social description.

Regardless of whether noise is imagined as productive or destructive, the notion that noise does *not* escape the scope, means and measure of human control divorces the grey-ness of noise from itself.

Secondly, the literature dichotomizes noise on a normative (or ‘good’ versus ‘bad’) basis. For example, while noise is conceptualized as a force that encourages workplace productivity, its logical consequence according to Westerkamp is the divorcing of meaning and pleasure from music – a divorcing that cannot be reclaimed, reversed or reimagined. Conversely, noise is also said to be a deliberate activity of concealing meaning with precise calculation, in deliberately predictable (and as such, controllable) fashions. No matter the manner of process, ‘precision’, ‘accuracy’ and ‘clear legibility’ are understood to be inherent characteristics of encryption. To encryption theorists, noise tends not to be identified as something that might blur, obfuscate, interrupt, preclude or impede communication. Noise *is* productive, and if it is not, noise is no longer noise. Noise does ‘good’ by concealing information or rendering itself as the building block to human speech altogether. Or noise does ‘bad’ by engineering productivity and by upsetting audience members in a concert hall in order to make a point about the prevailing constraints of the institution of popular music. Noise – much like the dichotomous nature of normative intellectual treatment – falls prey to further dichotomous treatment. Noise enables, or it disables. It opens, or it closes. But it tends not to be identified as opening *and* closing simultaneously. As such, noise tends not to be recognized as a variegated or variegating

phenomenon. An ontological consequence of the academic preoccupations with noise death with thus far, is that noise loses its grey-ness, its inherent uneven-ness, its unpredictability. And so, if noise is indeed variegated, it needs to be rediscovered and that is precisely what the dissertation intends to do by outlining its theoretical framework in the final section of this chapter below.

The final gap, and a rather modest one at that, is that which remains after Serres' contributions. The majority of the analytical and prescriptive values remaining after the application of his social relations and social systems theories to his case studies are largely pessimistic. And those case studies also tend to be about literary, fictitious contexts. How these theories might be applicable in everyday 'real' contexts is one challenge, but their applicability upon the intersection of social life, the digital realm and technological actors is quite another. While it is indeed the case that Serres' work intimately founded and inspired the work of John Law and Bruno Latour – major contributors to Actor-Network Theory – an even more significant gap is levied by attempting to intersect Serres' logics about social life and social systems upon *digital privacy, particularly as a product of noisemaking.*

Part Six: Conclusion

To summarize, there are three primary gaps left open by the literature reviewed thus far: individuals do not seem to be equated in the unfolding of digital privacy today, nor are technologies treated as actors themselves; noise tends to be well received as either a direct social activity or a byproduct of social activity, but one that also tends to be treated on a purely normative basis; Serres' theories about the fundamentality of noise in all social relations and social systems is applied in literary frameworks, and therefore is not well charted into the daily, lived experience of digital privacy. Taken together, these gaps constitute a larger issue: there is a

general absence of scholarship that frames noise as socially productive *and* destructive simultaneously, and how the socially productive and destructive dimension of noise factors into digital privacy as well. The dissertation addressed these gaps vis-à-vis the first chapter's theoretical framework. It generally outlined that digital privacy is the product of Internet users, software coders and software systems themselves through *noisemaking*: social activities, expressions and interactions – from written communication, web browsing behaviour to software intervening upon how human users and coders provide software systems input – that produce a byproduct (noise) that either creates or enters into social relations online, which in turn produces a wide range of variegated changes that may mediate digital privacy systems as much as they might devastate them. The next three chapters to follow specifically highlight this argument, and beginning with the dissertation's first case study: Tor.

Chapter Three: Case Study One – *The Onion Router* (Tor)

The first case study examines an anonymity network comprised of users, coders and software intersecting with one another throughout an onion routing encrypted communications network. The network, or *The Onion Router* (Tor) is referred to throughout the dissertation as both the software that users use to browse the Internet as well as the network of users, coders and software as a larger, abstracted embodiment as well. Tor, as software, is a free Internet browser whose acronym is derived from a data encryption technique called ‘onion routing’. The software has been publicly available since 2002 (Leigh and Harding, 2011), making it not only the most familiar modality of anonymity-based Internet browsing across the planet, it is also one of the most controversial in terms of the kind of users and activity the network attracts. Its popularity and controversies facilitate a wide range of interpretative flexibilities as an object of analysis. This is primarily due to an abundance of gaps between the relations of different types of users across Tor, which is spawned through a number of social and technical problematics emanating from coders’ and the software’s noisemaking. As we will see, the noise the software and the coders create coalesce in a way that facilitates a proliferation of different types of browsing behaviour – types of behaviour that are not only initially distinct and isolated from one another, but ones that come to influence the behaviour of Tor’s more ‘legal’ user behaviour.

The chapter begins by briefly introducing Tor. The second section of the chapter makes legible who and what constitutes ‘users’, ‘coders’ and ‘software’. It identifies and constellates the dissertation’s theoretical perspective upon how each actor makes noise: coders sending a message to users promoting the technology itself but, after time, transformed into a noise – one that demanded users to dramatically alter their behaviour so as to protect their privacy as it became evident that software was failing to provide privacy on its own; users making three

different kinds of distinct noise on their own terms (users who attempt to make Tor stronger by tweaking/amending its functionality, users who simply use Tor ‘incorrectly’ and users who manipulate Tor for nefarious purposes); the software itself creating noise through the aesthetic properties of its interface, which creates a distance not only between users and the software, but also distance between users and coders. The third section of the chapter brings together the noises each actor makes and paints them together as a socio-technical system, which provides a systemic basis for locating the dimensions, shape and forces behind digital privacy itself. The final section of the chapter thus explicates precisely what that digital privacy looks like. As we will see, digital privacy on Tor is not merely a reflection of onion routing encryption protocols hiding users’ location and content data. It is, rather conversely, a matter of users navigating friction between the coders and the software, in such a way that compels many users to hide in nefarious data streams so as to promote their own privacy when it clearly cannot be provided by the software and coders on their own terms.

Part One: Tor, at a glance

Throughout its development and usage, Tor (as software) existed in three variations, the first of which is the only variation currently used. The first variant is a standalone software package, much like one would identify with *Google Chrome*, *Apple Safari* or *Mozilla’s Firefox*. The second is a ‘plug-in’ for the aforementioned standalone web browsers. Simply speaking, the Tor *plug-in* is a script of coding that can be installed inside of a standalone web browser that enables onion routing function – an option that might seem more involved and complicated than traditional browsers, but offers the familiarity and comfort of traditional browsers. Lastly, and for a short period of time, Tor was a mobile application on smartphones and tablets. And so, the

conventional understanding thus far with regards to ‘users’ using Tor to enhance their privacy vis-à-vis anonymity enabling software begins with the belief that Tor will encrypt any and all packets of information leaving a computer as users continue about in their daily browsing activities.

The primary mechanism central to Tor is ‘onion routing’, purposed to hide the identity and location of a user communicating through a digital network. Onion routing refers to the technical process of redirecting the flow of packets (data such as web browser search queries, pictures and emails that are broken down into smaller bits of information for ease of transport) through a volunteer network of computers serving as relays across the planet. As the packets leave their source computer, they are encoded or encrypted with multiple layers of coding that protects the content of the packets. As the packets are sent to each relay in the volunteer network, each relay/computer ‘peels’ back a small portion of the encoding to reveal an instruction. The instruction is merely information about what relay/computer the packets should be sent next. By the time the packets finish their journey throughout potentially thousands of volunteer relay/computers, the final computer ‘peels’ back the final layer of encryption and thus reveals the actual hidden content of the packets themselves as they are pieced back together for the intended receiver. The goal is to make it exceptionally difficult for the content and origin/destination of the information flow to be detected. It is, simply put, an anti-surveillance technology.

Given the size and popularity of the software, Tor is globally recognized as a user-friendly web browser that guides users as to how to install and use the software, including a simplified explanation of its technical function, limitations and benefits. Tor is also widely discussed in ‘how to’ video blogs on *YouTube*, in numerous user and coder-oriented explanation components of digital privacy advocacy websites as well as computer programming open-source

networks (such as *GitHub*) and on various institutional websites that encourage its usage for clients, customers and employees like citizen journalists in China and activists/whistleblowers with *Amnesty International*.

Although there are contexts in which government employees are encouraged to use Tor software, as in the case of workers within the *US International Broadcasting Bureau*, Tor tends not to be endorsed formally by government. Curiously enough, Tor itself was created by *The United States Naval Research Laboratory* in the mid 1990s (Fagoyinbo, 2013), and further assisted by the United States' *Defense Advanced Research Projects Agency* (DARPA) in 1997 (Levine, 2014). The two labs desired a software system to protect communications throughout the United States military. More specifically, the goal was to use the software to hide the identity of government agents and informants in the field while they collected intelligence and established sting operations. Tor was developed by mathematician Paul Syverson and computer scientists Michael G. Reed and David Goldschlag, but a key player in the public release was former NSA employee Roger Dingledine who is accredited with bringing Tor to life – naming the technology and releasing it to the public as *The Onion Router* – under the supervision and investments of military and federal government contracts (Levine, 2014). Although the NSA, the Department of Defense, the United States Navy and local law enforcement in the United States continue to use and fund Tor, it was released for public use in 2003.

By the time the Internet proliferates in the mid 1990s, the United States government realized that Tor was too susceptible to network analysis attacks and other forms of monitoring by other governments; prior to Tor's public release, Tor existed as a hidden intranet – its own network that existed independently of the Internet itself. To counter the risk associated with Tor's exposure as a separate network, the United States government decided to hire Dingledine

and his colleagues to build Tor into the Internet itself – a move that would give field operatives the ability to ‘hide’ in plain sight under the guise of routine, daily public Internet traffic. It is important to recognize this move politically, a manipulation of an otherwise ‘open’ communications network that would enable government agents the benefits of ease-of-access through the Internet without being constrained to exclusively governmental networks of communication (Levine, 2014). Dingedine realized that by encouraging non-governmental people to use Tor, particularly by appealing to individuals who might feel the necessity or benefit from hiding on the Internet as they communicate – such as activists, students, researchers, journalists, drug dealers, hackers, terrorists – the diversity and expansion of user-ship would further expand the ability for government operatives to ‘hide’ in plain sight.

The usage of Tor to enhance the public’s privacy on the one hand, in tandem with Tor being used to ‘hide’ government field operatives *inside* the public’s usage of Tor (and as such, the public’s ‘privacy’ so to speak), raises an interesting question about the difference between ‘secrecy’ and ‘privacy’. The notions overlap one another in the sense that they both refer to the status of information by means of awareness, knowledge and access. If privacy can be understood as the prevention or interruption of access to information by introducing obfuscation techniques, privacy thus refers to the status of information itself. For example, an outsider might be aware that there is information or practices taking place behind closed doors that are purposely made private. Secrecy, on the other hand, refers to the removal of awareness of any such practice altogether (Johnson, 2003). It is the intentional removal of information, practices and objects from the ability for any outsider from ‘knowing’ about both the removal and content of removal altogether. This difference between secrecy and privacy is interesting when analyzing Tor because it illuminates the nature of the double-standard of the United States government’s

position on Tor. In turn, such awareness animates rather saliently the stakes in developing a comprehensive, alternative understanding of digital privacy via Tor therein. As argued by Johnson (2003), Western governments are purveyors of secrets. They keep secrets in the name of maintaining national security and protecting popular interest. Alas, they are the same entity that is fearful of secrets as well. The United States *National Security Agency* (NSA), for example, stipulates that they actively respect and do not interfere with civil liberties, freedoms and privacy rights (NSA-CSS, 2016). Alas, they are the same agency that revealed during the first Snowden leaks that Tor is a priority target for surveillance – so much so that Tor users are disproportionately scrutinized in terms of precisely ‘what’ they are attempting to make private. In the Age of Information, the United States government – via the military doctrine of network-centric warfare (which dominates the governance mentalities of many of the United States’ government agencies including the NSA) (Stienen, 2014) – obsesses with information collection and analysis in order to predict and prevent security threats. When information cannot be made legible, its source is often presumed to be threatening in nature. Unknown information is thus also often presumed to be tacitly hidden – not in the name of privacy, but in the name of ‘keeping secrets’ whether those secrets are originating from hackers, cyber terrorists or other states.

Tor grounds the conceptual tension between secrecy and privacy as a practical problematic. Tor is used to make and keep secrets by the United States government, secrets that could allegedly harm national security and national interest if leaked. But at the same time, the usage of Tor itself indicates the potential existence of secrets that must be exposed. This tension thus, in part, explains why the stakes over Tor’s existence and usage are so high. The United States government funds the development of Tor, but also openly criticizes its usage by the

public for the ways in which it could be used to hide nefarious secrets used against the country. Curiously enough, the United States government needs Tor to continue to enlarge in its size, grasp and usage worldwide in order to continue protecting its own secrets that are created and mobilized by field operatives around the world. Moreover, the more the NSA learns about it, the more they work towards ‘cracking’ and ‘reverse-engineering’ the technology so as to locate and identify foreign threats (Koebler, 2014). The point is that Tor is not merely a technology of privacy, but also a technology of secrecy – one that encourages surveillance as much as it detects and prevents surveillance.

Accordingly, and by 2004, Tor’s designers stopped essentializing the technology’s usage and development with the United States government and marketed Tor as a tool for the masses. By February 2017, 2.2 million unique individuals use Tor on a daily basis with approximately 6500 individuals, agencies and institutions volunteering their computers as relays in the onion routing network. Approximately 200 gigabytes worth of data is exchanged across this onion routing network on a daily basis, with the majority of the data being sent between the United States, Russia, Turkey, Brazil, Iran, the United Kingdom, Germany, Belarus, Saudi Arabia and France. Today, Tor has grown exponentially since its release. That growth is reflected in a number of complicated ways that cannot be reduced to purely technical considerations simply because there are numerous social and political dimensions surrounding Tor’s proliferation, limitations and daily usage. Understanding how Tor works from a technical perspective is certainly one challenge, but understanding its function and dynamics from a social perspective is another. The next part of the chapter thus analyzes the ‘who’ ‘what’ and ‘how’ of Tor in terms of the noises coders, users and the software itself emits into the wider Tor network all on their own terms but all equally in the name of privacy.

Part Two: Users, Coders, Software Making Noise

Understanding the ‘how’ and ‘what’ of onion routing benefits from a sociological description. Purely technical explanations (followed by the subsequent production and circulation of ‘simplified operations’ analogies on websites, as another example) tend to be devoid of crucial information about the behavior, preferences, orientations, conditions, catalysts and implications of decisions and exchanges made by the actors comprising these technical systems. This section thus provides an alternative explanatory framework of the functioning of Tor – an approach that incorporates and respects technical explanations by also including social dynamics so as to animate social life in and around the network itself. The goal is to *enable* thinking about the shifting *conditions* and *status* of digital privacy via Tor so as to *avoid* thinking about digital privacy as merely a reflection of encryption and coding. Tor is technical, but it is also exceptionally social. And as we will see, the wedding of ‘the social’ with ‘the technical’ constellates an entirely different realm through which digital privacy unfolds on Tor.

Coders

The example of coder noisemaking, of those noises’ effects upon the wider Tor network, aligns most closely with what Serres’ referred to as the ‘bang’ or ‘knock’ at the door of the home of the tax farmer. Noise, as Serres argues, is information. But that information is significant for two reasons. First, its frequency and timing is inconsistent. It changes over time. Secondly, that information is not self-evidently heard, internalized and acted upon in the same way. The noise frightens the city rat away and incites cautious, docile behaviour upon the next visit. But the noise does not frighten the country rat. The country rat stays and can adjust its behaviour depending upon the nature of the noises, making decisions about what can be learned or ignored

from the noise itself. In the case of Tor, the noise these coders emit are the first noise rats (or users) encounter. And that noise changes, rather significantly, over time. And this has dramatic effects upon its users.

In the second year of Tor's public release, its creators discussed that the future success of Tor depended upon their ability to successfully promote an otherwise unknown technology from an unknown source for purposes that many users around the world would not self-evidently come to realize (let alone understand) as necessary; an anonymity network, to enhance privacy, was relatively novel in the early 2000s. And so, enlarging the technology's adoption by the public depended upon a successful marketing strategy. The strategy the coders chose was to appeal to users' social values – marketing the idea that privacy via anonymity was not only important in the Age of Information, but that it was also a fast and easy way to browse the Internet. The coders promoted Tor through a single message, distributed towards users via the start page of the browser itself. The message was that Tor was fast and provided users a reliable modality of digital privacy through its encryption methods. But as we will see, that message came to adopt a different tone and intention over time. The message eventually transformed into a noise, spawned through the coders' realization of acute technical issues in Tor's design.

Tor's initial design was discussed and promoted through Dingledine, Mathewson and Syverson in "Tor: *The Second-Generation Onion Router*". Published in May of 2004, the paper indicates that the entire Tor volunteer relay network consisted of 32 nodes (24 in the United States, 3 in Europe). The paper generally outlines the design of Tor, its goals, operating assumptions at different scales of usage, threat models, congestion control, integrity checks, attacks, defenses and observations about how Tor was experienced 'in the wild' as well as its future directions. In this first, seminal paper, Tor's designers marketed Tor rather aggressively.

Their strategy was to market Tor to align with what these designers perceived to be Internet users' social values: a technology that was not only secure and reliable, but fast. But therein lay the issue. Speed and security tend not to go hand-in-hand in the worlds of encryption and computation. By advertising Tor as speedy and safe, the coders hoped to enlarge the Tor network and its popularity across the globe. In order to bring in more users and make Tor larger, it needs to be fast. Tor's programmers envisioned a network accessed by a browser-like software that showcased their coding values.

To assist their users in understanding their design principle of fast but safe browsing, Tor's creators began doing a number of things in terms of sending messages to their users. The first was a stream of direct messages that came in the form of website notices, browser labels and community bulletins that advertised Tor was fast and reliable. For example, at no point during the release of any three of the variations of Tor could a user load the software without being exposed to one of these messages. The second, came in the form of visual aide that highlighted the bandwidth levels (DSL, T1, T3) of each volunteer computer (or 'node') in the Tor network inside the browser itself. The creators figured this would allow users to purposely avoid nodes that had low bandwidth (which equates to a slow information transfer and ultimately slower browsing experience). During Tor's early testing, users generally but happily adjusted to a relatively slow network speed. And so, the creators associated Tor's early success in terms of its growth, particularly in terms of the tremendous scalability of Tor to include more users and nodes simultaneously; as implied in the title of their first research paper, their guarantee of 'low latency anonymity' resembles an imagination of Tor as a network that worked quickly for the user despite its growing size.

However, a considerable technical hurdle accompanied the coders' desire and communication of Tor as fast and safe. As Tor became more popular, it accrued new users. And as it accrued new users, an uncertainty surrounded whether or not the network would slow down; if there are considerably more users, there would need to be considerably more volunteers worldwide giving up their computers and bandwidth to support the growth. Moreover, the network's growth also made it a more attractive target to the curiosity of hackers. At the time, and as continues today, there are two general fields of attack that are most risky to Tor – active attacks and passive attacks. 'Active attacks' refer to the direct attempts at compromising encryption keys, or by nefariously hiding in the network as a casual user so as to move from node to node and compromise their integrity, or by replacing the contents of nodes that were not yet authenticated during an information transfer process (Dingledine, Mathewson and Syverson, 2004, 13). 'Passive attacks' refer to observing user content by monitoring the intake of information from a user sending data through the network once it arrives at its destination, by watching traffic patterns to deduce the location of a user or website fingerprinting that involves finding patterns of website behaviour such as file sizes and access patterns. When it comes to ensuring speed in the Tor network, without compromising security, a balance must be realized in terms of being able to actively monitor for threats before they happen – and monitoring tends to create higher latency (slower experiences).

Three years later, the authors released their second research paper, entitled "Challenges in deploying low-latency anonymity." The paper identified that one of Tor's largest threats emanated through hackers cataloguing the latency (speed) of packet flows through volunteer nodes. While the nature of this attack does not compromise the beginning or end point of the Tor network's information flow, it can clog the network so as to enable other versions of attack. The

point here is the tension in maintain a low-latency browsing experience that does not compromise the integrity of the onion routing process. One of the ways in which the authors decided to address the issue was by coding a way that would make users ‘feel’ safe without feeling ‘slow’ while using Tor:

“From here we can better understand the effects of publicity on security: the more convincing your advertising, the more likely people will believe you have users, and thus the more users you will attract... So it follows that we accurately communicate the available security levels to the user... [we] aim(s) to do this by including a comforting ‘anonymity meter’ dial in the software’s graphical interface, giving the user the impression of the level of protection for her current traffic” (Dingledine, Mathewson and Syverson, 2007, 5).

As the programmers continue to market Tor so as to bring in new users, and as they aim to promote Tor as fast and safe, they realized that the increased traffic on Tor must be balanced. This meant that in order for the Tor network to provide consistent anonymity for all of its users, users “need to act like each other... end-to-end traffic correlation attacks allow an attacker who can observe both ends of a communication to correlate packet timing and volume, quickly linking the initiator to her destination” (Dingledine, Mathewson and Syverson, 2004, 5). The point the authors are making is that when users do not browse the same way across the Tor network, and as the Tor network continues to grow, a new issue arises between speed, comfort, trust and security: uniformity. To ensure a balance in speed and safety, network data flow must appear the same – in size, scale and frequency. In order to achieve this appearance in technical terms, users’ browsing behaviour needs to be regulated.

The implication here is that the design principle behind Tor, of safe but speedy browsing, began constraining how users would (and still do today) use Tor. The subsequent issue that is brewing thus far however is the way in which the design principle of safe speed rather ironically constrained how users ought to browse the Internet itself, which in turn also affects how they

experience digital privacy; if users do *not* browse the same, their privacy would be tremendously compromised. It is here that we see the original message – to browse liberally on a fast and reliable network – transform into a noise. It is a noise in the sense that the original message promoting Tor changed into a request that co-opted users into the outcome of digital privacy itself. If users do not browse in the way the coders came to require, the software would not be able to provide them digital privacy in a ‘fast and reliable’ way.

By 2015, Tor supported over two million unique users worldwide. The number of volunteer nodes in the network, however, did not grow as significantly (Koebler, 2015). The subsequent effect is that Tor did not successfully strike a balance in terms of its latency distribution, meaning that Tor is generally recognized as a slow privacy solution. To compound the issue further, the nature of attacks against Tor and the ubiquity/frequency of these attacks have exploded exponentially. Well after the Snowden revelations, it has been well documented by technology bloggers, journalists and news sources that Tor has been an active target of the United States’ *National Security Agency* (NSA). From leveraging exploits in existing web browsers like *Mozilla’s Firefox* (Makrushin and Garnaeva, 2015) to the FBI taking over entire hidden service sites to further exploit Tor (Lee, 2013), Tor has indeed been widely criticized for not being able to provide a reliable anonymity solution to its users not only because it is slow but also because it is routinely attacked and prodded for vulnerabilities. To save Tor’s position in the anonymity marketplace, its programmers designed a solution that encouraged users to do a number of things to speed up Tor or to at least enable users to speed up their own experience. The former comes in the form of a request for users to free up their Internet connections so as to allow other users worldwide to transfer information more quickly. The former also manifested as a request to corporate and governmental agencies to ask their employees to volunteer their

bandwidth in order to increase the network's speed. Regarding the latter, users are also encouraged to engineer Tor browsers to only connect to the fastest nodes available⁵. Keeping in mind here that speed was perceived as a highly sought after social value of its users, the push to keep Tor fast so as to prevent users from stopping its usage continued to be a top priority for Tor's creators well into the 2010's.

Since it was first mentioned in their very first publication about Tor in the early 2000s, Tor's coders have actively maintained reminders and tips throughout the host website [Appendix A], as well as in the browser itself [Appendix B], arguing to users that in order for anonymity to be 'truly' experienced users must change their browsing behaviour. These sorts of reminders are not limited to the Tor website or browser as they are proliferous throughout programming communities online (see footnote 1). The reminders demand of users that they refrain from a wide variety of activity that generally makes up the majority of Internet traffic: to not torrent over Tor; to not enable plugins or install browser add-ons; to visit HTTPS enabled websites exclusively⁶; to not download documents or PDFs in the browser and to avoid using personal credentials when logging into social media sites. The former-most suggestion is treated as a piece of common sense, but is exceptionally constraining upon users' activities because social media websites – like the majority of websites used daily across the Internet – depend upon the ability to log in to services in order to use them (Tor, 2017). One of the more curiously limiting

⁵ Numerous blogging communities, such as those on *StackExchange's* *Torbeta* thread designed for researchers, developers and users of Tor (<http://tor.stackexchange.com/questions/217/how-can-one-make-tor-faster-when-willing-to-sacrifice-anonymity>) and *Quora* – a social media platform that is premised upon community members asking questions and providing answers to everyday things (<https://www.quora.com/How-can-I-make-TOR-faster>) to the Tor website's *Relay Configuration* page (<https://www.torproject.org/docs/tor-doc-relay.html>) all provide instructions to users and programmers about how to engineer the Tor network to privilege faster nodes.

⁶ The majority of websites online do not currently use HTTPS which is a corporately encrypted connection service between users and websites. The problem with HTTPS from a social perspective is that only the most profitable websites can afford HTTPS coverage. This issue is further compounding the latency issue with Tor as HTTPS has contributed globally to longer loading and waiting times while browsing the Internet.

requests is that users refrain from visiting websites that have *Javascript* and disabling the usage of *Javascript* altogether (Kirk, 2013) – a damning limitation upon Tor users considering that, as of January 2017, upwards of 94.4% of all websites use *Javascript* (W3Techs Web Technology Surveys, 2017).

In summary, programmers have attempted to create and promote an anonymity-based privacy experience for users worldwide by emitting their own noise into the network, a message that demanded users to trust their technology, but also to – rather ironically – regulate their behaviour by ‘browsing like everyone else’. This request from the coders formulated and continues to formulate a tension with the reality of how its users expect and subsequently experience digital privacy via Tor; the social value of fast Internet browsing is a global expectation amongst users of virtually any browsing software available, but it is at odds with the request that *how* users browse quickly ought to be changed so as to be more similar to one another. The heart of the tension is the loss of speed at the expectation of a kind of social retraining of how Tor users might otherwise browse and thusly experience the Internet because for users using Tor for the first time, they are *not* expecting to have to change their behavior in order to have privacy. Digital privacy, from the perspective of the coders, is at odds with the perspective of new users, a first glimpse into the very social nature of digital privacy itself not merely in the sense that the software is not the sole guarantor of digital privacy but also that the outcome of digital privacy is also dictated by the users themselves.

Users

‘Users’ in the Tor network are identified as virtually anyone that uses the software for professional or personal purposes. They can, however, be generalized in terms of their browsing preoccupations and why those preoccupations are independently deemed necessary for usage on an anonymity network. The range of users is thus quite wide, including activists, students, researchers, journalists and drug dealers to hackers, terrorists, pornographers and human traffickers. Again, what is key here is not so much who they are as much as it is what they are doing. The following section identifies three general noisemaking trends amongst users’ behaviour on Tor. The first is a reflection of users’ attempts to make their privacy stronger in Tor by tweaking, manipulating and adjusting the software and/or their own browsing behaviour – a reflecting of the growing awareness of Tor’s security vulnerabilities. The second and third encompass a very different body of user-ship on Tor. The vast majority of Tor’s users evidently do not use Tor as it is intended and are a tremendously higher risk in terms of security vulnerability than the aforementioned group. The second trend is that Tor users using the Tor plugin for *Firefox* have not been using the plugin properly. Finally, the third noisemaking trend finds that a significant portion of Tor users are manipulating certain dimensions of the Tor network itself to enable media pirating.

The first noisemaking trend is found in users’ attempts to ‘add’ more anonymity and security to Tor. This example aligns rather self-evidently with Serres’ (1982) initial observation about how social behaviour creates social systems via the parasitic nature of an excluded third social actor who enters into an existing relationship and radically alters it. Like the example of the city rat who is scared off by the bang at the door after feasting on table scraps in the country home, the city rat returns to feast after having learned from the experience. The noise at the door

becomes information parasitically – it becomes a lesson that establishes expectations, norms, limitations and even provides a little insight as to the timing and frequency of interruptions. Just like the way in which the relation between the rats and the food is permanently altered by the noise from the door, there are users on Tor who attempted and continue to browse only after having heeded the noise emitted by the coders – their noise being the suggestions, tips and advice to browse in a uniform way. There are thousands of cases where Tor users are taking an extra step towards owning their own digital privacy through Tor, specifically by adding plugins or ‘tweaking’ the software itself.

Curiously enough, most of these efforts towards greater anonymity (or at the very least, more reliable digital privacy) conversely restricted Tor’s usage, speed and accessibility. Over the past two years for example, there has been a marked growth in technology blog posts, reviews and instructional websites across the Internet⁷ explaining to users the security vulnerabilities of Tor and what they can do on their own to enhance their privacy. As difficult as it may seem here to correlate ‘enhancement’ with ‘restraint’ when it comes to the intersection of communications and information technology (in an age of machine-learning algorithms) with ‘digital privacy’, users advanced their privacy through themes of deduction, reduction and minimization around their actions. For example, users were encouraged to stop using hard drives that are unencrypted, to use laptops that can be quickly destroyed, to use light and portable browsing devices so that different Internet networks can be accessed throughout the day to generate the appearance of random Internet access behaviours, to not use the *Google* search engine whatsoever, to never use

⁷ *Google* search results populate approximately 8,050,000 results worldwide for “how to make Tor more secure”, with correlating related search terms resulting as “how to stay safe using Tor”, “how to be completely anonymous on Tor”, “how to use Tor browser to access the deep web” and “how secure is Tor for 2016”. Results available: <https://www.google.ca/search?q=google+search+result+graphs&oq=google+search+result+graphs&aqs=chrome..69i57j69i64.3970j0j8&sourceid=chrome&ie=UTF-8#safe=off&q=how+to+make+tor+more+secure>

Tor from work or home and to never leave your cell phone on while using Tor (Skufca, 2016). The recommended changes were not merely oriented towards users' behaviour, but also to their demeanour about browsing as well. From a psychological point of view, users were asked to "try to think of your Tor activity as pseudonymous, and create in your mind a virtual identity to correspond with the activity. The virtual person does not know you and will never meet you, and wouldn't even like you if he knew you. He must be kept strictly mentally separated" (Ibid). The idea that one must refrain from visiting websites like *Facebook* – the most routinely used social media networks worldwide – because the website reveals one's physical identity, or the idea that one must never make or receive *Voice over Internet Protocol* (VoIP – like *Skype*) while using Tor, has been embraced by some of Tor's users. Alas, these calls to adjust or tweak the software or one's behaviour tends to fall upon deaf ears. Behavioural trends across Tor paint quite a different story about the kinds of noise Tor users emit into the Tor network.

And so the second trend of users emitting noise into Tor is illuminated via research conducted at the *Vienna University of Technology* by Markus Huber, Martin Mulazanni and Edgar Weippel. Their work demonstrates that Tor users have been playing their own roles in compromising their own privacy due to the ways in which they have been using Tor itself. This example exhibits the behaviour of the country rat as opposed to the city rat from the previous discussion on user behaviour. Unlike the city rat who flees, the country rat stays. The country rat is more familiar with the environment and as such the nature of noises and interruptions. On the one hand, the experience allows the rat to engage the space and feasts more frequently. On the other hand, however, this rat is increasingly exposed to more danger – more guests, more presence of the home owner, and as such, comes with higher risk. To a certain extent, a combination of experience and naivety coalesce here.

This literary example as taken from Serres' text is limited in the sense that it speculates as to the risk factor for the rat. But returning to the example of this body of user-ship on Tor, the study documents that upwards of 78% of Tor users do not use Tor properly. They are, rather, using Tor in ways that directly compromises what the technology is otherwise designed to prevent. Motivated by a substantial lack of research and subsequent information into the nature of Tor's users' behaviour (with the exception of research conducted on the role of Tor in the aftermath of the most recent Iranian national election⁸), the researchers ran Tor network tests and logged over 9 million HTTP requests (or the requests by users to visit certain websites) over the period of several weeks between December 2009 and January 2010 resulting in a log file approximately 2.5 gigabytes in size. Social networking sites, particularly *Facebook* (which accounted for nearly 5% of all HTTP requests), *Google*, *BlackPlanet* (a social network site for peoples of African origin/descent), *Yandex.ru* (Russia's largest search engine), *btmon.com* (a torrent site that enables the downloading of pirated media), *craigslist.org*, *torrentbox.com*, *ameba.jp* (a popular Japanese social media site) and *Google Maps* (curiously enough, which often depends upon users disclosing their location in order to use effectively). While 54% of the HTTP requests were simply to visit the websites themselves, 32% of the requests were used to download images in .jpeg and .gif format. The majority of the HTTP requests were not however sent through the Tor browser itself, but rather via the Tor plugin for *Firefox*. The primary contention for the researchers was that the nature of these HTTP requests tend to leak personal information. For example, search queries about diseases give hints about a user's location, identity, nationality, language, browser preferences, operating systems – variables that can be

⁸ See "Tor Project. Measuring Tor and Iran, 2009" Available: <https://blog.torproject.org/blog/measuring-tor-and-iran> and "Forbes. PluggedIn: Web tools help protect human rights activists, 2009" Available: <http://www.forbes.com/feeds/afx/2009/08/19/afx6794971.html>.

used to disassemble a user's anonymity. Visiting (let alone signing in to) social networks is counter-intuitive to using Tor altogether. The researchers also noted that the Tor plugin tends to hide users' locations through coding that normalizes the usage of the "en-us" (English, United States) variable when any Tor user browses on a social media platform – so long as they actually reside in the United States; people around the world who visited *Google* in terms of their respective national *Google* pages (i.e. *Google.dk* or *Google.ca* as opposed to *Google.com*) were no longer protected by Tor's location normalization protocol. The conclusion is that while 78% of users were using the Tor plugin (which was most strongly encouraged by the Tor website at the time of the study) they were not using it as suggested by the coders.

The third noise users make is documented through research conducted by Abdelberi Chaabane, Pere Manils and Mohamed Ali Kaafar at *The French Institute for Computer Science and Applied Mathematics*. Where their research differs from the previous study is in the behavioural trend findings, specifically in the sense that they argue that the majority of users seem to be using Tor to torrent pirated media. Their research cites that previous studies on Tor missed this trend because it did not account for the extra layers of encryption in torrenting traffic. Moreover, and perhaps most importantly, the research reveals that a significant portion of Tor traffic is actually manipulating the final relay/node in Tor volunteer chains for nefarious purposes. This example most closely relates to the theoretical perspective offered by Serres' notion of 'parasiting' in the sense that the country and city, regardless of what they have or have not learned in terms of noises-as-information that may or may not affect their behaviour and relation to the room, they matter-of-factly engage and ignore such noises as much as possible. They are simply there to be parasitic, regardless of the potential dangers or risks inherent in their presence and decisions.

As opposed to the previous study that monitored one exit node, this study monitored six over a twenty-three day period on controlled servers in the United States, Japan, France, Germany and Taiwan. Each node was measured carrying approximately 20 gigabytes of bandwidth per day, yielding a dataset of 1.6 terabytes in size in total. From this dataset, the researchers used a technique called *deep packet inspection*, a process that involves digging inside of the information packets being sent along the Tor volunteer relay network to collect data. Otherwise considered hacking itself, the researchers chose this method to ensure a higher level of legibility and understanding about the origin and destination of traffic in relation to precisely what was being sent/collected. The findings reveal that just under 50% of Tor users were indeed browsing the Internet (searching/downloading images, using search engines and loading websites), but that this share of traffic was embodied in compressed files (.rar and .zip). The researchers note that 6% of the traffic carrying compressed files were routinely switching between peer-to-peer sharing services (P2P) for torrenting purposes, and then switching to Direct Download Links (DDL) – a trend they argue is an attempt by Tor users to *avoid* detection. A second significant observation from the research reveals that of the 4 million domain names (unique websites) users visited, only a fraction of users used Tor for nefarious/illegal purposes.

MOST VISITED WEB-SITES ACCORDING TO THEIR CATEGORIES

Rank	Category	Percentage
1	Search Engines/Portals	14.45%
2	Pornography	11.50%
3	Computers/Internet	11.45%
4	Social Networking	9.52%
11	Blogs/Web Communications	2.26%
13	StreamingMedia/MP3	1.82%
14	Software Downloads	1.66%
36	Hacking	0.3%
40	Political	0.18%
42	Illegal/Questionable	0.15%
52	IllegalDrugs	0.06%

Table One: Most Visited Websites on Tor

The website visit findings should not be confused with how Tor was being used outside of websites. The research also finds that the majority (>50%) of Tor users were using *BitTorrent* or some other form of torrenting software to pirate media thus implicating that the majority of non-website browsing activity was not only using Tor to hide their activity, but they were supplanting Tor's anonymity processes with their own practices to further enhance their privacy; despite the fact that these practices violate Tor's usage policy, the majority of these users were manipulating the Tor relay to transform the exit node into a 'tunnel' (a SOCKS or single-hop proxy).

APPLICATION USAGE (DATASET 1)

Protocol	Packets (Millions)	Size	Flows (Thousand)
HTTP	185.7 (34.31%)	136 GB (36.44%)	4735 (68.57%)
BitTorrent (clear)	136.8 (25.27%)	93 GB (24.92%)	320.5 (4.64%)
SSL	28.5 (5.26%)	20 GB (5.37%)	126 (1.83%)
Others P2P/ file sharing	5.7 (1.07%)	4.4 GB (1.17%)	15 (0.22%)
Insecure (ftp, telnet, email, etc.)	1.3 (0.26%)	1.2 GB (0.32%)	6 (0.09%)
Instant Messaging	6.5 (1.22%)	972 MB (0.26%)	119 (1.72%)
Well-known (other recognized protocols)	18.2 (3.37%)	22.6 GB (6.04%)	1173 (16.99%)
"Unknown"	158 (29.21%)	95 GB (25.47%)	410 (5.94%)
Total	541.5	373.6 GB	6905

Table Two: Application Usage on Tor

Simply speaking, these users are forcing Tor to skip as many volunteer nodes as possible so that they can directly connect to the exit node in the network – a way to decrease latency as much as possible at the risk of lowered privacy but at the benefit of bypassing corporate firewalls as well as receiving an extra layer of encryption while pirating media.

In summary, Tor users can generally be categorized as making their own noise inside of the Tor network in three ways. Like the sustained presence of the country rat and the returning of the city rat, who are both affected by the production of noises themselves, they in turn produce noises as well. The relation of the home owner to the table, to the food, to its neighbours are invariably affected by the different kinds of behaviour and engagement emitted into the space by the rats. In terms of the noises the different user groups create on Tor, these three different

expressions of noisemaking trends indicate the diversity of the social group of the ‘user’ itself. This in turn formulates another tension with coders’ expectations.

Tor’s users are not only browsing differently than requested, their social makeup and complexion is more highly differentiated than Tor embraces let alone openly admits. Despite recent discovery that upwards of 81% of *all* Tor traffic across the globe has been compromised for some time (Koebler, 2014; Paganini, 2014; Tung, 2017), there are indications that users are refraining from behaving in a certain way in order to enhance their privacy while using Tor. Alas, the abundance of noise being made by users and emitted into the Tor network present themselves either in terms of users manipulating certain dimensions of Tor to avoid government and corporate detection mechanisms for pirating purposes or that the majority of Tor users are simply using the software in such a way the inadvertently ruins their own digital privacy. The combined significance of these noisemaking trends from the ‘user’ social group is found in the observation that Tor users’ vision or expectation for digital privacy – regardless of which noisemaking trend they contribute to – is completely at odds with the coders’ vision. While some users want digital privacy for politically ‘correct’ purposes, the vast majority want digital privacy to hide nefariousness; the idea that any browsing behaviour could be akin to ‘uniform’ is essentially moot because different users do not and cannot use Tor the same way. The stakes of an enforced or even imagined uniform network flow and/or or uniform browsing behaviours are simply too high.

Software

An inherent challenge in studying Tor as software is that the software is not merely the inevitable outcome of the hands of coders through a meticulous preoccupation with

computational language. Such explanations tend to dominate the vast majority of both popular and academic descriptions/prescriptions of software, the likes of which are found on Tor's website, or privacy advocacy organizations like *The Electronic Frontier Foundation*:

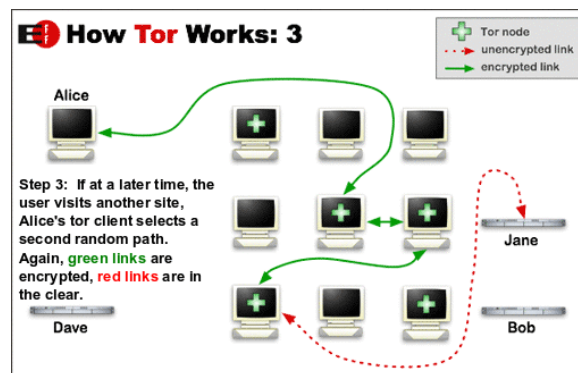


Illustration One: How Tor Works

“Tor works by” machines collecting information and routing that information between computers somewhere in the world that encrypt and decrypt your information to provide you privacy, as it were, or is. The workings of Tor are not self-evidently technical for its workings are also social. As stipulated by Actor-Network Theory (Latour, 2007), actors in a social network are not merely limited to anthropocentric logics. ‘Things’ like Tor may be a reflection of the technical know-how and expertise of human intention and design, but Tor also intimately affects how users and coders behave, perceive and relate to information and their digital environment. Tor has agency, and that agency is realized via its noisemaking capacity. The noise Tor makes is a visual ‘knock’, an impression made upon the user through her gaze. Prior to browsing the Internet, there is a crucial moment where the user meets the graphical interface of Tor itself. That interface is not unique. That interface is an impression, a simulation of *Google Chrome* and other mainstream browsers. This impression carries with it a familiarity about ‘how’ to browse the Internet. This memory is characterized by ‘usual’ browsing – the routine, daily task of visiting

websites and accessing information. Using Tor is not as simply as loading the software and browsing. Tor interrupts that process by pretending to look and feel like something it is not. And with that simulation comes important consequences. This is precisely where we trace Tor's noisemaking capacity.

Tor encourages users to use the software just as they would whilst browsing any other mainstream browser. Most traffic is PC or Mac based via the Tor browser⁹, which has been and currently is – curiously enough – released to look and feel anything other than something uniquely itself. Tor is not a unique web browsing interface. In fact, it is designed to mimic *Firefox* entirely. Consider the following examples. Turning to appendix C, note the “File”, “Edit”, “View”, “History”, “Bookmarks”, “Tools”, “Window” and “Help” drop-down menus populating the menu-bar atop the browser screen. They are consistent with what is found in *Firefox* as well as *Google's Chrome* and *Apple's Safari*. The “Forward” and “Back” buttons embodied by circles containing arrows corresponding to the browsing directions implied found at the sides of the URL/search bar are identical to the design of *Firefox* as well. Access to the browser's settings are represented by the exact same three horizontal lines found atop of the browser to the left, just as one would find with *Firefox*. The “Bookmarks” and “Favourite Pages” toolbars are located in the same position as they would in *Firefox*, and the plug-in tray is positioned and scaled in the same way as well.

As another example, and as consequence of its mimicry of popular browsing solutions, Tor is as equally to the security flaws of popular browsers. As argued elsewhere (Cooke, 2016), HTTP cookies are fundamental to very operation and exchange of websites with users. These

⁹ Extensive research into breakdowns of Tor network traffic in terms of device used is not published publicly. Speculation derived from the number of worldwide users as of 1 February 2017 (~2 million unique users worldwide) against the number of *Android Marketplace* mobile downloads (between 10 and 50 million downloads) raises questions about whether or not a discernible distinction can even be made.

technologies are also fundamental to web analytics, data mining and the reverse engineering of geolocations by hackers and surveillance regimes across the planet. The point being is that whether or not Tor's designers want users to be anonymous, the priority of a pleasing and familiar aesthetics invites a dangerous politics of exposure and insecurity – not only in terms of its design principles (which encourages the kind of reckless browsing behaviours and monitoring-oriented practices that an anonymity network might otherwise aim to avoid) but also in terms of incorporating technologies like HTTP cookies that are (arguably) the first and most fundamental technologies enabling Internet tracking. Simply put, users on Tor bring with them a behaviour that is socialized in products that Tor is attempting to amend. Curiously enough, its design is encouraging the opposite.

As a final example, consider appendices D, E and F, which represent a window made accessible in Tor by clicking a 'green onion' icon located to the left of the search bar. When pressed, users are presented three security level options. Each level has a different set of implications and constraints upon how the user will browse/experience the Internet. The highest security settings disabled upwards of 95% of the crucial features that 90% of the world's top websites use (flash, javascript, HTTP cookies) thus making the majority of the Internet's websites completely inaccessible. The lowest setting, which is also the default setting, indicates to the user that it is the most "usable experience". 'Usability' is equated rather curiously here to browse-ability, inferring simultaneously that in order to have a stronger guarantee of privacy, Tor might not even be a wise choice whatsoever.

The familiarity of Tor, its HTTP cookie security vulnerability and its green onion slider, all taken together drive distances between Tor and the user, as well as driving distances between certain users from other kinds of users. Tor's URL address bar default loads HTTP addresses,

when most HTTP sites use technologies that render Tor inept. Tor has a drop down window that provides options for bookmarks, plugins and browsing histories – options that also tend to render the software inept. Tor has a ‘green onion’ slider that allegedly allows the user to control her privacy level despite the fact that Tor is marketed to control privacy *for* the user, *without* her input. The slider thus sends an ironic message to the user about what to expect of their privacy when they use Tor. And so, it is not merely the case that the slider simply distances the user from the software. It also distances users from one another, specifically by disproportionately affecting the browsing experience of legal users who have higher stakes in their search habits. For example, users who have an unusually high stake in requiring the highest amount of security – such as targets of political oppression and journalists – cannot afford to use Tor on the lowest security setting. The green onion slider is simply useless to them as such. If they choose to leave the security setting at its default setting, thereby making Tor the most useable, these types of users are susceptible to having their browsing activity stand out rather acutely from the majority of the illegal traffic that tends *not* to visit HTTP sites; most illegal activity, over 57% as of 2016 (Nelsen, 2017), is carried out on the deep web across ‘.onion’ websites – those created specifically for Tor, that cannot be accessed by any other standard, commercial Internet browser.

This kind of distancing power latent in the software’s visual design begs simple questions that further animate the role Tor as software plays in emitting its own noise into the network-at-large: why should a user need to adjust a security slider on a technology that is supposed to hide their activity as opposed to require further activity? Perhaps most significantly, why is the user herself being asked whether or not she wants to blend in, and with what register of ethical traffic is she being blended in with once she has released herself the expectation that the majority of the websites she would normally visit are no longer available to her within reason? Tor affects many

of its human users by affecting how they ‘feel’ whether or not they have privacy. This happens because of the fact that the ‘how’ of digital privacy is not self-evident to the user – it is, rather, a matter of their input and control. What is more evident, however, is that the software is placing the onus of digital privacy upon the user herself. Curiously enough, the user-ship of Tor is so diverse that the majority of its traffic cannot exist if the slider is actually used whereas, and on the other hand, the slider *is* used to provide reliable privacy for the smallest minority of its traffic (journalists, academics, targets of political oppression). For many Tor users who have the highest socio-political stakes in how and why they use Tor itself, they have a different vision of digital privacy and different rationale for its necessity. However, that vision and rationale is drowned out by the majority of the traffic that identify and engage the ‘green onion slider’ as an impediment as opposed to a benefit to their browsing experience. Users that play an active role in manipulating the ‘green onion slider’ are the most disadvantaged because they are specifically seeking an Internet browsing experience that is *not* reminiscent of *Firefox*. The goal is to avoid casual everyday browsing as much as possible.

And so to summarize the affective power of Tor – as they are found in the visual elements Tor’s design itself – Tor makes its own noise by sending a visual message to users that reliable digital privacy is not the priority of your experience – access and usability are the priorities. From the perspective of object-oriented ontology, this clash of values and priorities regarding privacy is a reflection of how the software mediates the affairs of its human users and coders by manipulating distance between itself and between them as humans. The software is effectively creating a tension between itself and its users, and users from themselves. It also drives a wedge between Tor’s coders and Tor’s users by re-casting who the responsibility of information protection rests upon. Downloading and using free, open-source software infers that

it is upon the shoulders of coders. However, we see here that much of that onus rests upon users. Tor's agency as an actor on its own terms is an ontological matter, a question of 'how' it exists. The notion that software can 'exist' is not novel to the academy. Brian Cantwell Smith's *On the Origins of Objects*, for example, explores the capacity for computation and computational software to have metaphysical properties. Another way of understanding this is that machines exist in a distance from humans. They 'do' things that humans 'do' but in a very different way. Their existence as such maintains a difference from humans in terms of the spaces they occupy, intersect and influence. When human and software spaces intersect, the 'how' and 'what' of the control, passage and access of digital information cannot be so easily presumed a matter of regulation and control by the software's coders. When these spaces intersect in the case of Tor, we learn that if users desire reliable privacy, they are expected to hold at least one of the reins.

Part Three: Tor as a Socio-Technical System

Digital privacy via Tor is indeed a reflection of technical processes, but it is also a reflection of social processes – ones delineated by a series of intersecting noises made by users, coders and the software itself. As a sociotechnical system, Tor never occupies a static, uniform and concrete architecture – whether material, ideological or otherwise. To access this way of conceptualizing digital privacy, this section charts out the noise emissions from each actor and discusses how they enter into and affect neighbouring, pre-existing relations. It also identifies how these noises create new relations across Tor as a sociotechnical system. The aim here is to setup the final section of theorization of the chapter, which outlines precisely how this sociotechnical system challenges conventional understandings of the 'how' and 'what' of digital privacy as afforded by Tor.

The first, crucial implication of any noise emitted into the Tor system starts with the coders and how it affects users' behaviour. Recalling Serres' emphasis upon the ways in which noisemaking infects relations of neighbouring actors, Tor's coders play a particularly intimate role in establishing a connection with its users and then shifting the nature of their noise emission, which catalyzes very different dimensions for Tor as a socio-technical system. The coders' message – which initially emphasized speed and safety – was not sustainable on its own terms. The message must change over time. This is because 'speed' and 'safety' tend not to be synonymous with one another in virtually any context – particularly cybersecurity. Just as one might imagine the risk of barrelling down a highway at 100 kilometres an hour or tucking down a ski slope, the propensity for injury and other associated problems/risks for by-standers increase – especially when seatbelts and helmets tend not to be worn.

Although a crude set of analogies, they embody the kinds of tensions at the heart of the idea of promoting security with large numbers of subjects under haste. In his *Security, Territory, Population* lecture series at the *College de France* during the 1977-78 academic year, Foucault displayed a map of a mid-century French town to his audience. He pointed out the obvious. Here are streets. Here are lamps that illuminate the streets and the people walking down them. Here are sidewalks. They indicate where foot traffic flows. These buildings are destinations of that foot traffic. These canals are limits of the streets and buildings and foot traffic. And this wall is the limit of the town. Foucault twisted the perspective to demonstrate that the map itself was also a political technology. It made legible the flow of life, which enabled degrees of predictability for policing purposes. It levied strategies about where criminals might run and where they might be most illuminated or most obstructed as they flee capture. Much like an airport's security inspection area, where the ongoing proliferation of new-age and 'high-tech' scanning and 'truth-

telling tech' (Muller, 2016) is routinely implemented, we see Foucault's tension between security and mobility intersect with the necessity for speed in contemporary ways. Social life and social bodies flow freely, which is a problem for security. In order to prevent security issues, social flow and bodily flow must be made legible, monitored, striated, organized, and inspected. The process is counter-intuitive to the economic principle and value of speed. The point is simply, in order to have reliable security, care and time are necessary investments.

It is indeed the case that government-controlled and corporate-controlled spaces are managed to balance economic and social flow in relation to perceived risks and security issues associated with said flows. But it is also the case that spatial management interferes with social flows. This interference often invites response and resistance by the bodies making up these flows. And this is precisely what happens within Tor. The noise the coders make is an attempt to heavily manage the spaces and nature through which users move, so much so that where they can go online and what they can access and send is heavily restricted. Users push-back accordingly. This kind of resistance is taken up in Latham's *The Politics of Evasion: A Post-Globalization Dialogue Along the Edge of the State* (2016).

Latham theorizes the consequence of digital systems upon users' security, specifically by highlighting the taken-for-granted nature of the notion of 'open circulation'. To Latham, the ability – let alone the intention – to move openly or freely on a digital network formulates a tension with security. In the case of *Anonymous* (the hacktivist collective), for example, Latham denotes the way in which part of their effort for social and political outreach demands that they create webpages, social media groups and correlated content on mainstream, corporate social media websites like *Facebook*. While mainstream media generally attributes characteristics of camouflage, subversion and clandestine-ness to the group, it appears rather trivial if not also

ironic and counterintuitive that *Anonymous* would reveal itself ‘in the open’ – on social media networks that are generally characterized as possessing contrary characteristics: openness, accessibility, and free movement. An anonymous organization on an ‘open’ social media platform is, at first glance, a rather obvious security problem. But Latham’s point, however, is that the notion that social media companies in particular (and the Internet in general) are ‘open’ is misleading. They are, as Latham argues, inherently closed and as such inherently insecure. This is caused by what Latham identifies as a coalescing of interests between government surveillance and corporate data mining. For example, Snowden’s revelations highlighted the way in which agencies like the NSA piggyback corporate tracking efforts in order to analyze the flow of bodies and information online. Like the way in which Internet Service Providers (ISPs) like *AT&T* were compromised by NSA backdoor tracking techniques, other companies like *Google* and *Twitter* are similarly and/or subsequently compromised as the data they create, collect and circulate is subject to scrutiny by the United States government for risk management, threat assessment and attack prevention purposes.

The point Latham is making is that networks that seem to be open, free and easily accessible are in fact the most compromised. The subsequent issue being, and further to Foucault’s point, is that social life online adapts. The threat to open networks, as Latham sees it, is the way circulating bodies and information divert and create alternative pathways and avenues around and through open networks in response to the Snowden revelations. For the coders of Tor, this is precisely what they were trying to avoid – users adapting to the knowledge of surveillance regimes and surveillance systems monitoring even the most highly adapted technologies (like Tor) will find a way to further protect themselves. In the case of the values of speed and safety being emitted upon Tor, particularly as a noise emission by the coders

themselves, it is crucial to recognize how it attempts to similarly striate and organize the shape and systematic behavioural quality of future users on Tor.

As the size of the Tor network increased (and it increased rather quickly, into the millions of users less than a decade after its release), its coders hoped that the number of users would increase proportionately to the number of volunteer nodes. This was *not* the case and it remains this way today. There have been and are considerably fewer volunteer relays in relation to the number of users. From a design point of view then, the issue then became a question of how to ensure low latency (high speed) given a small backbone network infrastructure without compromising safety. The result was a push early on to ensure that users would use relays in a balanced way, and would behave in a uniformed way so as to ensure that the most common passive and active attacks would be mitigated. The message the coders sent – to enjoy guaranteed speed and safety – transformed into a demand, to browse uniformly. The demand became a ‘noise’, a knock at the door that would forever change the users’ relationship to the software. Just like in Serres’ review of Bourgoing’s *Fables d’Espose*, the knock at the door interrupted consistency and expectation in the room. It established new expectations, new excitement and new constraints. Users are startled by the strange request to browse against their intuition; it is revealed to the users for the first time that the system cannot provide privacy through its encryption. Users must change their behavior, they must adapt to the noise or they risk having no privacy protection whatsoever.

This noise the coders make affect how users socialize into Tor. These noises also directly affect how they related to the software itself. The relation between users and the software-side of Tor was offset in one significant way. A dependency developed for users as they socialized into an aesthetics in Tor’s browser, a process that engendered a trust that the technology would

simply work and be flexible as it become more and more streamlined and access-enabling. And so as the nature and frequency of attacks against Tor normalized over the years, coupled with the issue of the number of relays capping as the number of users gradually increased, users depended upon an aesthetics that conveyed mixed messages about ease and speed on the one hand with ‘due diligence’ and ‘self-care’ on the other.

Users, conversely, have been pushing back upon their relation with coders via their own noise productions. And it is here that we see a resistance to the implications of the noise itself. The knock at the door, so to speak, is not only dismissed as irrelevant, it is recognized as a nuisance. Like the way in which Lundblad (2004) theorized how noise productions (exactly like the kind that Tor’s coders have been emitting) precondition resistance and adaptation, the various noisemaking examples emanating from Tor’s users display numerous examples through which noises are emitted upon the Tor network that counteracts the noise coders emitted. While it was indeed the case that some users simply heeded the coders’ wishes, the vast majority worked directly against those wishes. For example, 21-year-old Eldo Kim – a political science student at Harvard University – used Tor to login to an encrypted email service. Hoping that the extra layering would provide greater anonymity, the bomb-threat he sent to the university was deduced rather easily because he did not use Tor according to the coders’ precautions and soon found himself in jail (Brandom, 2013). Some users have been interrupting the relationship between actual user behaviour and the usage reports generated by Tor for its coders. Most Tor users do not use Tor properly. Many other users the Tor volunteer relay network, specifically by ‘tinkering’ with the exit node of each network in order to cover up illegal activity. Between improper usage and manipulated usage, we see that different users are trying to use the software, for privacy purposes, on their own terms. On their own accord. In their own imagination of ‘what

works best'. This is what Bolton (2013) refers to as *parasitic autopoiesis*, wherein a different value and meaning of privacy begins to emerge around the site of the user's experience and awareness of the inefficiency of the software itself.

This user-oriented noise is not the only 'knock' entering into and disrupting the social system. As Tor's aesthetics invites users to behave liberally, a tension emerges between the kind of anonymity that Tor allegedly provides with the rules of browsing behaviour required in order to produce anonymity and freedom. The noise the coders are emitting upon the network, for users to behave uniformly and take extra precautions, is undermined by Tor's aesthetic and affective power. For example, reconsider the position, accessibility and consequences of the 'green onion' security slider. If Tor's default setting is the most flexible and provides the fastest browsing experience, reliable and standardized digital privacy is not realistic. Moreover, it is a subsidiary priority to access and usability. If Tor's highest security setting is used, casual Tor users are prevented from visiting nearly 95% of the Internet's most common websites (which are HTTP based), which leaves said users stranded and most susceptible to surveillance upon the Tor network simply because they are *not* constituting traffic carried out and through ".onion" domains.

Part Four: Conclusion

As the array of noises triangulate into the wider Tor network, a very different story and image emerges about digital privacy on Tor. Digital privacy via Tor is not merely a software technology coded to reroute, encrypt and randomize packet flows. Privacy is, as Nissenbaum so deftly identifies, a product of social, political and economic contexts. And her observation about the privacy needing to be grounded in specific contexts so as to provide more robust,

comprehensive understandings of privacy could not apply more. To extend her argument, however, is to recognize the manner in which those contexts are given structure and as such, meaning. Digital privacy in Tor is constituted by the social actions and behaviour in the network itself, largely as a by-product of the kinds of constraints the system places upon its users on the one hand, and how they respond to such constraints on the other. The constraint/response nature of Tor, as engendered by its coders and maintained by the software conditions a specific context for digital privacy where a one-size-fits-all notion does not compellingly apply, particularly for the ways in which the system categorizes its users into different categories of identity. Not only did the essentialization of Tor into an exclusively standalone pc/mac based product alienate different kinds of users and accessibility, it also essentialized browsing behaviour in terms of the kinds of behaviour most amenable to a *Firefox* styled product. What is particularly significant about the essentialization process is how it forces users to make decisions about the kind of browsing experience they desire, which has two significant implications upon the context and subsequent understanding of digital privacy here.

First, digital privacy is not a priority of the network. It is subsidiary to values of access and usability – a contradiction of the core value of onion routing anonymity altogether. For those browsing legally (those browsing casually), the most amount of protection is absolutely necessary. A similar argument could be put forth for illegal activity, but as research demonstrates, the majority of illegal browsing activity does *not* visit HTTP sites as a researcher or activist might. Most of that browsing is conducted on different websites called *onion* websites (which do not end in *‘.com’* or *‘.ca’* but in *‘.onion’*) on the deep web, and the majority of illegal traffic that browses the Internet casually tends to be more reckless about with their *‘green onion’* security slider settings; the stakes between each group of Tor users is significantly different. The

minority of users who depend upon Tor for legitimately anonymized communication purposes are caught in a fray where complete privacy means using Tor in a way that renders most of the Internet essentially useless. It also means that *if* they visit the sites they desire, they are taking a massive risk over whether or not the Tor network will protect them. As coders continue to re-assess how to deliver meaningful and reliable options, flexibility and efficiency for its user-ship, the push to attract new users by making the product as user-friendly as possible continues to alienate legitimate browsing behaviour.

Secondly, and accordingly, digital privacy is not a one-size-fits-all guarantee afforded by the Tor network and marketing value of speedy, reliable anonymity at all. Digital privacy privileges certain kinds of usage and behaviour. Ironically, that usage and behaviour is illegal activity. The majority of its users benefit by blending into traffic flows across non-HTTP/HTTPS based web destinations, which leaves legitimate users susceptible to passive network analysis attacks. In Tor, we need to understand that digital privacy is an entirely variegated experience. A gamble of sorts. Perhaps most confusingly then, is that from a design and coding perspective, Tor promotes a vision of ‘digital privacy’ that is almost too reminiscent of the convention that ‘digital privacy’ is a matter of regulation and control. Onset as a military technology, it is imbued with an essence of predictable and reliable privacy as if digital privacy existed as a law or policy statement. But the network itself does not reflect the behaviour of its user-ship. Whether nefarious, unusual or otherwise, there is a substantial disconnect between the message coders are sending to its user and the users’ behavior. Tor itself is caught somewhere in between, mediating and making legible for one another the stakes and perils of that digital privacy.

The most significant conceptual feature and logical lesson derived from this case study is that the notion of ‘digital privacy’ Tor broadcasts on its website and in its product is in direct

tension with the realities of users' information protection needs and browsing experiences. The case study demonstrates that by attending to the various noisemaking activities across Tor – and the subsequent social system that emerges as a result – the conventional understanding of digital privacy as found on Tor's website and on its product is turned on its head. A different understanding emerges in its place, one that instructs us that Tor is laden with politics. This politics is revealed to us as analysts due to the constant changes around the conditions of users' privacy from one release of the software to the next. And as Tor continues to grow as a system, this politics will continue to take on and further embody the inability of the network itself to sustain its users' privacy requirements.

Chapter Four: Case Study Two – *WhatsApp*

The second case study explores the world's most popular mobile texting software, *WhatsApp*. *WhatsApp* uses an End-to-End encryption system. The system works by protecting the connection between users so as to deflect external traffic monitoring attacks. *WhatsApp* is the world's most popular social media-based instant messaging software. It functions much in the same way as 'texting' does on smartphones, but without being constrained to domestic texting charges and as such allowing users to text internationally for free. *WhatsApp* is also recognized as the most secured popular instant messaging application in the world; as of 2017, one in three Canadians use the application regularly. What follows is an analysis of the coders, users and the software *WhatsApp* itself. The story of *WhatsApp* is similar to the story of Tor in the sense that *WhatsApp* was similarly marketed to users as a fast and secure technology. The attempt to push both products as something that can be trusted gained users' attention very quickly. Like Tor, that push had significant social consequences. The consequence for Tor was that it constrained how users browsed the Internet. For *WhatsApp*, the consequences are as significant but with very different implications: that users themselves would come to infringe upon one another's' privacy due to the way in which the marketing of enhanced digital privacy via new encryption conditioned a false security.

The situation for users on *WhatsApp* perhaps reflects the inescapably darker overtones found throughout Serres' perspective on noise in the social realm, particularly in the sense that a concentration of coalescing noises (between the coders and the software itself) has essentially negated users altogether from emitting noise on their own terms. As the chapter will demonstrate, *WhatsApp* may preclude external and even internal eyes from reading content data,

but it does not prevent internal mining of meta data nor the introduction of advertising from third party organizations vis-à-vis *Facebook*'s partnerships.

Accordingly, the chapter is structured into four parts. The chapter begins by briefly introducing *WhatsApp*, which includes a technical overview of how the End-to-End encryption service operates. Secondly, the chapter identifies the coders, software and users so as to constellate the noise each actor emits into what the chapter identifies as the *WhatsApp* network – the socio-technical system of users, coders and software interacting with one another in terms of information creation, exchange and subsequent circulations. The section identifies the kinds of noise each actor emits: coders marketing *WhatsApp* as secure and reliable but programming *WhatsApp* to harvest users' data (despite the fact that doing so undermines the privacy statement they produce on the app and on their website); the software's aesthetics closing any sense of distance between itself and its users so as to manipulate an even closer proximity between users themselves; some users increasingly checking *WhatsApp* to inquire into the status of relation with other users. The third part constellates the noises made by each actor, painting the socialness of the *WhatsApp* system to reveal how each noise affects neighbouring relations in the system. The significance of understanding *WhatsApp* as a socio-technical system as opposed to merely a technical system is acknowledging how digital privacy plays out as a network of social interactions that includes the technology itself but expands towards the actions and intentions of the technology's programmers and the users of the technology as well. In comprehending *WhatsApp* as a socio-technical, we make a crucial theoretical move towards understanding digital privacy rather differently. And so, the final and concluding section of the chapter identifies digital privacy as indeed the protection of the information flows from external analysis on the one hand, but *at the cost* of generating a social insecurity amongst users that, rather

ironically, *encourages them to violate one another's own privacy* in the name of data mining. Simply put, the encryption system isolates interactions across *WhatsApp* so much so that it engenders privacy violations between users. Our understanding of digital privacy on *WhatsApp* thus undergoes a refocusing, one that reveals that digital privacy has much higher stakes and implications than thinking about digital privacy as merely an encryption process.

Part One: WhatsApp, at a glance

WhatsApp was originally designed and based out of Mountain View, California in 2009. The product was incorporated by Brian Acton and Jan Koum who are former employees of *Yahoo!*, two software designers who sought to produce an instant messaging based 'app' for the *iPhone* marketplace with one particular aesthetic feature in mind – a text based messaging service that placed 'statuses' of users next to their name on *WhatsApp*'s contact list. By June of that year, *Apple* released the 'push notification' feature that allows different apps to post a message on a user's smartphone screen to provide updates on a variety of app-related information ranging from notices of app updates to global news events. The push notification feature compelled the designers to begin marketing *WhatsApp* to work with push notifications; any time a *WhatsApp* user changed their status, it would send a corresponding notification to other *WhatsApp* users' phones. *WhatsApp* quickly gained a user-ship of approximately 250,000 users worldwide, and accelerated in its popularity thereafter (Olson, 2014), with marketing towards the push notifications feature being attributed as gaining popularity amongst users. By this point, *WhatsApp* was available as a beta-stage product on the *Apple* marketplace. *WhatsApp* was released in November 2009. The app grew so fast at the time that the designers decided to change the service from free to a cost-based service, charging users one American dollar to

continue using after a calendar year as the quick expansion in user-ship over encumbered the product's servers (Olson, 2014). By December 2009, the ability to send photos was introduced and by 2011, *WhatsApp* was one of the top twenty apps available in the *Apple* marketplace. By February 2013, *WhatsApp* had over 200 million active users and carried a staff of approximately fifty. Within a calendar year, the app supported over 500 million users worldwide who sent 700 million photos, 100 million videos along with 10 billion messages sent between users everyday (Chowdry, 2014). By mid 2014, *WhatsApp* received over 25 million new users every month, for a total of 65 million users worldwide by the end of the year. By December 2016, *WhatsApp* was populated by 950 million unique users engaging the device every day per month (Cochin, 2016). *WhatsApp* currently supports 1.2 billion users worldwide, 35% of which represented by the millennial age group (Cohen, 2015).

In February 2014, *Facebook* acquired *WhatsApp* for \$19 billion USD. Curiously enough, the number one competitor to *WhatsApp*, called *Telegram*, saw an instant worldwide download of 8 million on the same day that the new ownership acquisition took place (Tsotsis, 2014). Journalists argue that one of the major reasons behind *Telegram*'s popularity is that users feared for their privacy on *WhatsApp*; *Telegram* was globally recognized at the time as one of the few encryption-based instant messaging software systems that could not be infiltrated by Russian surveillance agencies (Tsotsis, 2014). But *WhatsApp* retained its market share regardless of *Telegram*'s boost, which is in part due to both a push in marketing by *Facebook*'s owner Mark Zuckerberg as well eventual promises to improve user privacy. Shortly after *Telegram*'s surge, Zuckerberg announced at the *Mobile World Congress* held in Barcelona held in late February 2014 that the idea to acquire *WhatsApp* was to develop more 'free' communications products for the world that would be linked to other products, like *Facebook* – the value in mind was to

prevent users from having to pay for communications technologies (like texting) that they may otherwise soon come to believe was not worth paying for. As of January 2016, the dollar charge was lifted following one of *Facebook*'s marketing campaigns designed to reach out to potential customers who did not have a credit card to pay for the service. The move to overcome barriers facing numerous users worldwide was also extended by the declaration that *Facebook* would not place advertisements in the app.

The previous two points about marketing avenues are particularly noteworthy because they dovetail *Facebook*'s overall vision for *WhatsApp*. *Facebook* acknowledged from the onset *WhatsApp*'s worldwide popularity. The move to purchase *WhatsApp* secured tremendous revenue for *Facebook*, but the initial purchase raised numerous concerns about privacy violations. *Facebook* is known as one of the most aggressive data harvesting social media companies across the planet, and so the aforementioned marketing mechanisms designed to overcome stigmas about social barriers and remove advertisements is a move that *Facebook* hoped (as Zuckerberg articulated in the February 2014 exposition) would (re)build trust with existing and new users. Moreover, prior to *Facebook*'s purchase of *WhatsApp*, the app never had encryption. End-to-end encryption was introduced in November 2014 after *Open Whisper Systems* announced a partnership with *WhatsApp* (via *Facebook*) (Evans, 2014).

Open Whisper Systems is one of the world's leading encryption solutions firms, who has gained worldwide notoriety in the Information Technology security industry for its services to *Google*'s *Android* products. The introduction of the encryption service was not announced publicly; German security magazine *Heise Security* used a software spoofing method (ARP spoofing, which involves sending numerous fake messages across a network to cross reference MAC addresses with IP addresses) to reveal that *WhatsApp* was indeed using encryption but only

on *Android* devices. In April 2015, *WhatsApp* announced that encryption was added to every form of *WhatsApp* software. Moreover, and for the first time, users were provided with their own verification mechanism inside of *WhatsApp* that would indicate whether a secure connection existed between users. This kind of end-to-end encryption is a variant called *Signal Protocol*, a technique that incorporates Double Ratchet Algorithm, prekeys, and triple Diffie-Hellman handshake methods (Frosch et al., 2016) – a long, roundabout way of saying that it was and remains impossible for outsiders (including *WhatsApp* and *Facebook*) to read the content of users' messages (Scherschel, 2015).

But as the chapter demonstrates, the introduction of encryption to provide existing and new users a sense of trust in a verifiable encryption process – with a company that is known for harvesting data – needs careful re-examination. A re-examination is crucial because of the constraint the development of *WhatsApp* – particularly in terms of its push for more enhanced encryption via *Open Whisper Systems* – places upon user privacy. From a purely technical perspective, the move towards End-to-End encryption represents an enhancement for user privacy. But this is merely a technical projection, and one that tends to be void of socio-political ramifications of *Facebook's* move towards encryption. While the introduction of the new encryption mechanism may enhance users' trust that the content of their messages is un-see-able – by outsiders and *Facebook* itself – the meta data of their messages is not. The math of their communications, such as the logged data pertaining to the number of messages users send and receive, how long it takes them to communicate, whether or not users check the 'last seen' status of a contact on their list and or whether a contact actually reads messages they receive, consists of a massive wealth of information that is aggressively harvested by *Facebook*. The point, rather simply, is that the encryption mechanism misdirects users as to what information is most

important to protect, and from who: hackers or *Facebook*? As the next section demonstrates, particularly under the ‘coders’ subsection, there is an abundance of noise emitted into the *WhatsApp* network by its programmers that serves to directly undermine users’ privacy, not enhance it.

Part Two: Coders, Users and Software Making Noise

Shannon argued (1965) that noise is inherent in every electrical communications system. But that noise is not merely a reflection of the arrangement of technical components on circuit boards carrying electrical signals. System noise also emanates from social activity, and that social activity intimately effects technical processes. Noisemaking is not necessarily to the detriment of social and technical systems either. As the dissertation has argued thus far, noisemaking is a unique and important register through which digital privacy unfolds – as is reflected in what follows in this section. But what makes this account of noisemaking different, from actor to actor, are the odds against user-oriented noisemaking – they are disproportionately higher than in any other case study. What follows is an account of those odds, beginning with coder noisemaking that is designed, from the onset, to serve digital privacy as it fits a corporate agenda – not the user agenda.

Coders

Coder noisemaking began taking shape in August 2016. It happened after *Facebook* purchased *WhatsApp*, and shortly after *Facebook* reneged on its promise to not advertise on *WhatsApp*. *WhatsApp*’s Terms of Use Agreement outlines that users agree to allow third party organizations that are partnered with *Facebook* to directly text/instant message them on

WhatsApp (Burrell, 2017). The agreement also indicates that *Facebook* will be sharing users' phone numbers with advertisers to place targeted advertisements on users' corresponding *Facebook* pages. In a clear move that directly conflicts with *Facebook*'s previous commitment to protecting users' privacy, the first instance of noise coders emit upon the wider *WhatsApp* network is thus similar to the previous case study on Tor: coding parameters that harvest users' data, which directly undermines *WhatsApp*'s official security declaration [Appendix G].

In a similar fashion to Tor's coders' priorities (which were to market their software as widely as possible), the systemic coding of values to market a privacy-oriented product was determined most effective if done in a way that is accessible, comprehensible and attractive to users. As noted in Appendix G, the language used is particularly interesting in the sense that privacy on *WhatsApp* is 'fundamental' 'reliable' and 'straight-forward'. End-to-End encryption on *WhatsApp* is 'so powerful' and 'so reliable' that 'the designers of the encryption themselves cannot crack the code'. Marketing that communications systems are reliable and trustworthy was not a common occurrence in Silicon Valley until the global hard-encryption discourse began circulating after the initial Snowden leaks; the controversy of *Facebook*'s purchase of *WhatsApp*, being the largest social media buyout in history at the time, was one of the original lynchpins for perpetuating further development of the discourse on privacy and hard-encryption. By virtue of connecting coders' values about an unprecedented level of reliable security directly to the user as they are learning about *WhatsApp*, an equally unprecedented level of 'trust' is thus imparted upon a user-ship that is just beginning to learn about the necessity of privacy in an age where the largest social media data miner is routinely criticized for data harvesting.

The screenshot depicted in Appendix A is taken from the *WhatsApp* website, a message that has been displayed since the buyout in 2014. But the noise about trust began well before the

buyout itself. The emphasis on building trust with users is a particularly important dimension of *WhatsApp*'s coders emitting noise because of its two-pronged nature. It is 'noise' in the sense that it encourages users to engage one another feeling assured that their communications would be protected. The double-sided nature of this noise however is the politics of the noise itself: users came to trust the idea that *WhatsApp* was safe and encrypted, while all along it was anything but safe and encrypted.

Koum, *WhatsApp*'s first designer and primary coder, openly marketed *WhatsApp* along similar lines regarding trust but with a much more sociopolitical orientation. "*WhatsApp* may have grown in Silicon Valley, but its roots are in Eastern Europe" wrote Reuters (McBride, 2014). *Wired UK Magazine* interviewed Koum in 2014, a story that connected Koum's Ukrainian origin with his vision of privacy:

"I grew up in a society where everything you did was eavesdropped on, recorded, snitched on. I had friends when we were kids getting into trouble for telling anecdotes about Communist leaders. I remember hearing stories from my parents of dissidents like Andrei Sakharov, sentenced to exile because of his political views, like Solzhenitsyn, even local dissidents who got fed up with the constant bullshit. Nobody should have the right to eavesdrop, or you become a totalitarian state -- the kind of state I escaped as a kid to come to this country where you have democracy and freedom of speech. Our goal is to protect it. We have encryption between our client and our server. We don't save any messages on our servers, we don't store your chat history. They're all on your phone."

Reminiscent of Serres' tax farmer, who invites his neighbours to his dinner table only to feed them their own produce for which they are also taxed, the message Koum sends his users and the media 'sets the table' so to speak about origin, anticipation and purpose of his venture. The point being to rather, and as aforementioned, hold attention and keep the belief that the relationship is meaningful and trustworthy. And so, and as Serres infers, this kind of noise organized in this kind of space facilitates a modality of striation and control that amplifies the tax farmer's own

noise. So much so that despite the emergence of a social system around the dinner table, its capacity for an otherwise more liberal exchange and encounter is virtually precluded.

What Koum declared was simply not the case. Since the *WhatsApp*'s beta release in 2009, the company had been widely criticized for being careless, even reckless, with users' data. The criticism was grounded in the observation that *WhatsApp* never had encryption or specific security measures until 2012. All user content was transmitted openly across the Internet in simple text, essentially allowing any hacker with the simplest of traffic analysis or sniffing tools to intercept and read the traffic (Levine, 2014). In fact, *WhatsApp* users created a free app for the *Android* marketplace called *WhatsAppSniffer*, that allowed anyone to grab videos, pictures or texts over any Wi-Fi network instantly. The problem was made public in 2011, to which *WhatsApp* offered no formal response. Many critics attribute the introduction of encryption to *WhatsApp* nearly a year later partly in response to pressure exerted by the Dutch and Canadian governments who were threatening investigation into *WhatsApp*'s privacy and data practices (Office of the Privacy Commissioner of Canada, 2014).

The problem was further compounded by the kind of encryption the coders implemented. In 2013, the *PC World* launched an investigation into the 'End-to-End encryption' method Koum implemented. They argued that Koum's team was using one public key to decrypt all of the messages being sent. The implication being that once the key is compromised, any messages intercepted can be decoded rather quickly. To most computer scientists, this method of encryption was foolish. It was the most unreliable, but most efficient option available to *WhatsApp* – a decision that only further contradicted the noise Koum's coders emitted. "Reusing the key in this manner is a basic crypto implementation error that the *WhatsApp* developers should have been aware of... It's a mistake made by the Soviets in the 1950s and by Microsoft in

its VPN software in 1995 (Levine, 2014)”. Koum dismissed the argument as ‘theoretical in nature’ but the privacy issues kept unrolling throughout 2013. The Canadian government released the results of their investigation, demonstrating that *WhatsApp* was uploading users’ contact lists and phone numbers, without their knowledge, to unsecured servers. But as Koum argued, “people need to differentiate us from companies like *Yahoo!* and *Facebook* that collect your data and have it sitting on their servers. We want to know as little about our users as possible. We don’t know your name, your gender. We designed our system to be as anonymous as possible” (Rowan, 2014). Alas, one need not look further than *WhatsApp*’s Terms of Use Agreement to find further evidence of contradiction:

“We may use both your Personally Identifiable Information and certain non-personally-identifiable information (such as anonymous user usage data, cookies, IP addresses, browser type, clickstream data, etc.) to improve the quality and design of the WhatsApp Site and WhatsApp Service and to create new features, promotions, functionality, and services by storing, tracking, and analyzing user preferences and trends. Hopefully we improve the WhatsApp Site and Service and don't make it suck worse. We may use cookies and log file information to: (a) remember information so that you will not have to re-enter it during your visit or the next time you use the WhatsApp Service or WhatsApp Site; (b) provide custom, personalized content and information; (c) monitor individual and aggregate metrics such as total number of visitors, pages viewed, etc.; and (d) track your entries, submissions, views and such” (WhatsApp, July 2012).

Ironically, it was *Facebook* that Koum teamed up with for the sale of his product. At the time of the sale, Koum stated: “here is what will change for you, our users: nothing. *WhatsApp* will remain autonomous and operate independently... And you can still absolutely count on no ads interrupting your communication... There would have been no partnership between our two companies if we had to compromise on the core principles that will always define our company, our vision and our product” (Panzarino, 2014).

Koum’s commitment was extended by his priority for the company moving forward after the purchase. To keep *WhatsApp* running, and to prevent users from leaving the product after

Facebook finalized their purchase (Olson, 2014): “Fundamentally what we care about is building a product and a great user experience. Mark [Zuckerberg] understands the network effect and he always talked about making the world more open and more connected. Connected is where we come in” (Olson, 2014). Zuckerberg was less than forthcoming about his commitment to connection at the *Mobile World Congress*. At the same time that Koum is being interviewed about the sale, Zuckerberg was encouraging investors that the *WhatsApp* sale would continue to enlarge *Facebook*’s coffers because its products are ‘gateway drugs’ to users’ worldwide addiction to popular social media products like *WhatsApp* (Knibbs, 2014). As Zuckerberg infamously stated in 2007, “there is no opting out of advertising” (Gustin, 2016). The noise Koum’s coders began emitting changes here. What once was a message about guaranteed privacy via encryption which was ultimately a lie assumed even less substantive ethical meaning as rhetorical value furthered propelled the coders’ noise into new political territory amongst users and marketplace critics. The point being rather simply that the noise continued. ‘Use our product, it is trustworthy.’

But this team brought a new voice that was even less trustworthy amongst privacy-oriented communities. This new voice became the vehicle through which coders’ noise was projected. This is particularly due to *Facebook*’s terrible track record with privacy, for *Facebook* has been the leading social media company worldwide in habitually pushing the limits of online privacy. Since the onset of the Internet itself, this kind of manipulation of ideas into opportunities to build trust upon a lack of transparency and honesty over personal information protection (Grant and Bennett, 1995) has been a persistent problem. But what makes this case particularly noteworthy in terms of deceit is the unprecedented extent to which *Facebook*

manipulated not only users' personal information and trust but also their lack of awareness over precisely *what* was being manipulated.

For example, in 2010 a Harvard Business professor caught *Facebook* sending personal information to online advertisers without user consent (Gustin, 2016). As another example, *Facebook* hired academic researchers in 2012 to assist in manipulating the newsfeeds of 700,000 users to test whether emotional responses could be cued so as to encourage users to alter their posting behaviours (Merchant, 2014). Despite *Facebook*'s routine of addressing public backlash and media inquiry into privacy concerns, Zuckerberg has (since the initial release of *Facebook*) been known to be intolerant to user privacy; referring to *Facebook*'s first users as 'dumb fucks' for having shared 4,000 emails, pictures and addresses with him simply because 'they trust me' (Carlson, 2010), not to mention a longstanding legacy built by tech journalists critiquing Zuckerberg's leadership with regards to anyone's privacy (Yarrow, 2010; Warman, 2011; Johnson, 2010; Michallon, 2017). Under such leadership, and exacerbated by contradictions between marketing and programming values existing in *WhatsApp* long before *Facebook*'s purchase, *Facebook* continues to emit noise in *WhatsApp* in ways that sends one message about privacy protections to users but clearly contradicts their privacy in practice. In 2016, *Facebook* reneged on its promise to not harvest *WhatsApp* users' data. In August of that year, *Facebook* changed the Terms of Use Agreement indicating that users' phone numbers would be used to cross-reference data with their corresponding *Facebook* profile (Lomas, 2016). "By coordinating with *Facebook*, we'll be able to do things like track basic metrics about how often people use our services and better fight spam on *WhatsApp*... *Facebook* can offer better friends suggestions and show you more relevant ads" (WhatsApp, 2016). In particular, *Facebook* recoded *WhatsApp* to

track relative usage against activity on *Facebook*, using *WhatsApp*'s activity logs to feed data mining practices marked by *WhatsApp*'s 'last used' indicator (Lomas, 2016).

Tracing the noise *Facebook*'s coders emit into the *WhatsApp* network makes legible the contradiction between the privacy-bonus of their new end-to-end encryption feature and their message about respecting users' privacy in a way that is unrivaled by other social media products. Referring back to the language in Appendix G, note that *Facebook* alleges it cannot read users' message content. The language is mirrored elsewhere. In *WhatsApp*'s public update blog, for example: "Your messages are encrypted by default, which means you're the only one who can read them. Even as we coordinate more with *Facebook* in the months ahead, your encrypted messages stay private and no one else can read them. Not *WhatsApp*, not *Facebook*, nor anyone else" (WhatsApp, 2014). The noise is loud, because content data is not the primary interest for *Facebook*. *Facebook* is manipulating *WhatsApp* users into contextualizing their privacy with the affordances of end-to-end encryption. End-to-end encryption protects message content data. The content of texts are words, pictures and videos. This category of data is generally referred to as 'content data', which tends not to be of any interest to most social media data mining divisions at all – especially *Facebook* (cite). But what *Facebook* is harvesting is meta-data – the numbers or math between content itself. The point is that there has indeed been a longstanding legacy of noisemaking that began with Koum's coders, rearticulated as they came from Zuckerberg's coders, transformed in the sense that the source was different but the message remained the same: 'our product is trustworthy'. The noise has been the persistent maintenance of rhetoric and lies to encourage users to trust a product that provided encryption in a way that only shielded from *some* privacy violations while it in fact made other privacy issues much worse, part of which is articulated by the noise the software emits itself.

Software

The noise the software emits further reflects Serres' darker fears about his own theory of social noisemaking. Imagining that the tax farmer controls the stages of the meal and the stages of the conversation, so much so that the very guests he entertains are fearful to speak up about their discomfort with their business arrangement, so much so that their capacity to have any conversation that does not entertain the interests of the tax farmer, the guests return to their homes and work as usual. The point here is the extent to which the tax farmer controls his guests and their experience, and this is precisely the issue with the nature of noise that the software emits. What follows here is an account of the extents of the influence and control the coders possess over the noisemaking capacity of *WhatsApp*. This example is particularly unique amongst the other software-oriented noisemaking throughout the dissertation's case studies because it is the strongest example of how coders' noisemaking empower the software's noisemaking – a phenomenon that unfolds around a dual capacity surrounding the software's aesthetic properties.

The noise the software emits is derived from the same vein of information collection that Zuckerberg tapped into, as discussed in the previous section: meta data. The software aggressively captures meta data, but also makes some of that data visually available to its users. This section identifies how this data is visualized and how this visualization represents the noise the software emits into the wider *WhatsApp* community of users and coders. To account for this noisemaking, the chapter now provides a brief history of the relationship between Zuckerberg, *Facebook* and meta data.

At the time of Zuckerberg's launch of *Facebook*'s IPO, meta data was not self-evidently useful to marketers. As discussed elsewhere (Cooke, 2016), the decision by Zuckerberg to

establish *Facebook*'s initial public offering (IPO) was fraught with hesitation, concern and skepticism. Although the IPO is now recognized as a 'cultural touchstone', citing one of the most successful IPO's in Internet history, *Facebook* struggled to convince investors for nearly half a year prior to *Facebook*'s stock rising to unprecedented levels; negative memory bias in the public's imagination tends to forget that Zuckerberg needed tremendous help in order to help potential investors understand why *Facebook* users' data was worth pursuing. In the early Fall of 2012, *Facebook* attempted to prove to investors that users' data was indeed worth the investment, and the attempt resulted in the release of *Facebook Exchange* – an automated *eBay*-esque bidding system for advertisers that would allow investors to place targeted ads on users' newsfeeds (LeJaq, 2012). The attempt was one to make legible the correlation between users' behaviour – as embodied by the aesthetics of the bidding system itself – and consumer purchasing power. It did not catch. Zuckerberg then decided to enlist the assistance of *DataLogix*, a Denver-based independently-owned data mining organization that accumulated physical purchasing data (such as receipts and consumer questionnaires) from over 1,000 American retailers based upon 10 billion purchase records reflecting over \$1 trillion USD in consumer spending (Bea, 2012).

What *DataLogix* did for *Facebook* was cross-reference any physical purchasing data they could find from *Facebook Exchange*'s own data collection and analysis technology, which is based upon HTTP cookie tracking. HTTP cookies are small data files installed onto every smartphone and computer every time a user visits a website. Cookies have been a fundamental component of the Internet's infrastructure since their inception in 1997, which was originally purposed to assist websites in managing increasingly cumbersome data loads on their servers specifically by dumping information about search preferences, image history and favourite pages

on users' devices (Cooke, 2016). It was the NSA that discovered, by accident, that HTTP cookies can be reverse-engineered to build profiles about user behaviour. And this is precisely how *Facebook Exchange* utilizes these cookies – by installing their own cookies onto users' devices that record what websites users visit and how they interact with the site, which most data miners today have come to identify as information that reflects consumption behaviour (Cooke, 2016). Once *DataLogix* began connecting the cookie contents with the same users' physical consumption behaviour, *Facebook's* stocks exploded to the level public memory tends to most recall (as aforementioned) the most successful IPO in the Internet's history (Macke, 2013). *DataLogix* too tripled its staff size within a calendar year of their coordination with *Facebook*. The point here is the power of meta data.

Meta data 'says' more to advertisers and miners than content data because it allegedly animates the 'how' as much as the 'why' when it comes to consumption – so much so that *any* and *all* meta data collected is increasingly treated as an untapped or unrealized treasure trove for marketing potential. And it is here that the power and significance of *WhatsApp's* software's noisemaking unfolds. *WhatsApp* embodies precisely this marketing orientation towards meta-data. With over 1.2 billion unique users on *WhatsApp* every month, *Facebook* is literally swimming in data. The 2016 decision, then, to open up *WhatsApp's* data to *Facebook's* investors needs to be acknowledged because *WhatsApp's* original aesthetic design (and as it persists as such today) offered *Facebook* a very specific way to organize, mobilize and correlate the meta data *WhatsApp* produces and collects.

Appendices H, I and J, document *WhatsApp's* meta data indicators for users. These indicators allow users to let one another know how they are feeling, whether they feel like talking or if they are available. Moreover, *WhatsApp* documents the last time a user was seen

online, whether they have received a message versus when they read the message. As significantly, *WhatsApp* also lets users know the average response times for certain users and whether or not a user has been blocked. To give an example as to precisely what these aesthetics intimate, *WhatsApp* allows the user to correlate that ‘Suzie’ ‘is online and has received your message but has not yet responded’ or that ‘Joanne’ ‘is always online and gives instant responses’. This also intimates that the instant messaging service here is far removed from the tradition of instant messaging, which did not visualize or indicate for a user when a message was received or how the receiver is feeling. By virtue of *WhatsApp* introducing meta data to the exchange experience, they are also attempting to colour content data. As inferred earlier by how Big Data paradigms rationalize the ‘math’ between communications content, the idea here is that meta data is animating potential emotional and affective ideas and imaginations about the communication process. The stakes of this introduction are rather high here for the user, and inquiring into those stakes further animates the power of the noise the *WhatsApp* software emits into the wider network.

Most *WhatsApp* users are *Facebook* users. On *Facebook*, users have an instant messaging service – *Facebook Messenger*. They also have group communication on *Facebook Messenger*, just as *WhatsApp* offers as well. But the fundamental difference is that *Facebook* is generally a tool for public engagement and public communication. It is a medium that allows users to publicly share their feelings, ideas and photos/videos with one another. *WhatsApp* is more personal, or more ‘private’ (Chakraberty, 2014). It is designed to privilege *direct* communication, communication that is privileged *because it is encrypted – so much so that nobody else can read it*. It is also privileged because it is the ‘most’ private experience available to them across two of the world’s largest social media platforms. When users feel the need to

engage publicly, they use *Facebook*. They also know that *Facebook Messenger* is harvested and not protected by encryption. And so, the attraction to *WhatsApp* is characterized by its ability to protect communication in a way that *Facebook Messenger* cannot provide. What truly makes *WhatsApp*'s noise generating capacity so powerful is how it draws users in to escape any sense of public-ness, but in a way that still provides the unprecedented intimacy of communication animated by affective meta data and meta logic. As we will now see, the aesthetic power of *WhatsApp* indeed has intimate effects on users' behaviour, so much so that some of correlating consequences are producing affects that undermine most ideals of privacy itself.

Users

Returning to Serres' depiction of the dinner table, the tax farmer controls the meal and the conversation. He controls the flow and structure of the dining experience. In Serres' depiction, there were numerous diners at the table. The most disadvantaged, most manipulated and most repressed are the farmers. It is, after all, the farmers' food that the master, the farmers themselves and the other guests are feasting upon. The farmers, in a sense, pay to be guests. There is a clear power structure in the arrangement of the food and the experience. Moreover, the other diners – the master's acquaintances, neighbours and friends – reify this power structure in two ways. First, their orderliness and docility amplifies the noise the master makes. When he laughs, they laugh. When he changes conversation topics, they change conversation topics. When it is time to move onto the next course in the meal, they move on as well. Secondly, their orderliness and docility also signals the capacity for the continuation of the power of this noise outside of the tax farmer's home. The tax farmer's home is not merely a home. It is also a place where politics are organized. A place where political power can be striated so as to continue their

power-effect upon the guests well after they leave the house. The point, very simply, is that farmers' thoughts, reactions and attitudes are cultivated and disciplined during the meal to unfold in ways preferable to the master's interests even after they leave the house. The horizon of possibility for engaging and experiencing the master's space and even the farmer's own space is heavily controlled. Substitute master with *Facebook*, farmer with users, and the guests and the dining room itself with the software, and we begin to appreciate how challenging it is for users to make noise on their own terms.

Unlike the previous case study where users could manipulate the software itself, there is very little that can be done in terms of directly interacting with the software. That being said, there are some steps that users can take to aide in their own production and control of digital privacy. Just like the way in which 'the noise at the front door' startles the city rat to flee, users are equally startled into action to protect themselves; the noise that users are emitting here are three-fold: opt-ing out of data collection; disabling 'last seen', 'profile photo' and 'read receipts' meta data indicators and/or limiting others uses' access to the 'status' display. Although the lattermost seems most unrelated to the content of privacy vis-à-vis data collection and data mining, it is exceptionally important in terms of understanding how the coders and the software have raised the stakes in terms of encouraging privacy violations *between users*.

Prior to discussing, it is worth noting in Appendix H the 'security' and 'two step verification' features. They are not discussed here because they do not significantly implicate, effect or even remotely embody the kinds of user-oriented noisemaking that the 'privacy' features offer. The former-most allows users to receive notifications if another user deletes/reinstalls *WhatsApp*. The reason this is offered is to re-assure users that the encryption process is still working, as the encryption process establishes a specific encryption key on each device at

the beginning of the installation process. The lattermost two step verification allows users to establish a passcode when they transfer *WhatsApp* to a different device. As such, it represents a security feature that prevents unauthorized access to the app. These two features therefore do not significantly factor in to the dissertation's considerations nearly as much as what follows below here regarding the 'opt out' and 'privacy' subpage features.

The first modality of noisemaking for users exists within a very short window of time, which was the only opportunity for users to opt-out of data collection. For precisely 30 days after *Facebook* announced that it would be harvesting *WhatsApp* users' data in August 2016, users could opt-out of the data collection process (Mehta, 2016). This was the single most effective counter-measure users could have acted upon and as such represents the single most salient example of noisemaking into the *WhatsApp* network. Unfortunately, the 30-day window closed rather quickly thus leaving users to find different ways to emit their own noise into the network – noise via modalities that are almost entirely constrained to the options afforded by *WhatsApp* altogether.

The second modality of noisemaking for users involves changing security settings in the app itself. Appendix H represents the 'settings' page of the *WhatsApp* mobile software, which is the same on the computer-based software as well. The screenshot in this appendix reveals five subpages that allow users to adjust certain settings in *WhatsApp*. The first three, being 'privacy', 'security' and 'two-step verification' are the most significant at the moment. Turning to appendix I, take note of the five options presented to the user. The first two options of the five, 'last seen' and 'profile photo', provide the same options to the user. Each allows the user to restrict who on *WhatsApp* can see their 'last seen' status or 'profile photo', respectively, in terms of 'everyone', 'my contacts' or 'nobody'. The third option, 'status' allows users restrict access to only users in

their contact list, or to only share with certain users. The fourth option, ‘blocked’ allows users to block certain individuals from contacting/seeing them altogether. The fifth option, ‘read receipts’ allows the user the option to disable the ability for others be notified when the messages they send are received and subsequently read. The indicators for received messages are reflected by a single blue check mark, and the indicator for a message that is read is followed-up by a second blue check mark (as depicted in Appendix J).

In as far as noisemaking is concerned for users, these options to change or prevent status of *how* users use *WhatsApp* are their limits. Unless the opt-out feature was initiated, the point is that the noisemaking capacity for users has been engineered to be very constraining – the most constraining of the three case studies. As the next section will discuss, this places users at the mercy of the noisemaking by coders and the mercy of noisemaking by the software itself. These noises, taken together, have tremendous implications upon how we understand digital privacy itself across *WhatsApp*.

Part Three: WhatsApp as a Socio-Technical System

It is important to recount that since the onset of *WhatsApp*, well prior to *Facebook*’s buyout, the original coders designed *WhatsApp* to appeal to existing and potential users by emphasizing the security and privacy features of the product. Once it was proven that encryption was not actually provided, *Facebook* capitalized by promising said users a reliable encryption protocol via a reputable encryption solutions firm and went to great lengths to visualize the encryption mechanism for its users. As noted in the last section, the ‘settings’ component of *WhatsApp* allows users to be notified of interruptions in the encryption process and to re-establish connections when users change/delete software. The significance of this shift in

ownership and the subsequent deployment of encryption visualization mechanisms is the way in which *Facebook*'s coding preoccupations navigated users through the politics of *Facebook*'s buyout and the pre-existing controversies regarding the lies about *WhatsApp*'s security issues. The point is that users were conditioned into a certain rhythm, comfort and expectation since 2014 whereby *Facebook* further promised that *no one* can read users' messages – not even themselves. And so the first significant component documenting *WhatsApp* as a socio-technical system is the system production of docility as executed by both old and new coders, vis-à-vis a software whose aesthetics were designed to *make* users accountable to one another.

The onset of security concerns was a particularly interesting moment for *WhatsApp*'s development as a socio-technical system. This is because it signalled the first point of rupture and intervention by users concerned over the allegations of lying and deceit on behalf of both ownership groups. Akin to members of the dining room experience in Bourgault's *Fables d'Esposé* engineering the knock at the door themselves, we see here the first signs of purposeful parasitism upon the established system. The first signs of purposeful noisemaking intended to re-organize the system in the name of their own vision of privacy – a sign of protest, even if only briefly and rather ineffectively. The development of the *WhatsAppSniffer*, for example, did not merely demonstrate that the technology did not protect user information in the way its owners declared. The example highlights a gap between user experience and expectation on the one hand, and the ulterior motivation of the ownership group over personal information and privacy on the other hand. Recalling Paddion, Philo, Routledge and Sharp's (2000) argument that meaningful political change occurs at the moment of realization of disconnection between relations, the *WhatsAppSniffer* ought to be recognized as some users' attempt to emit their own noise into the wider socio-technical system. While there is indeed ethical merit to observation of

this gap still remaining open, the point is that the development of the *WhatsApp* socio-technical system maintained a trajectory largely favouring the noisemaking of its owners.

Once any concerns about security (via encryption) and data sharing (via the initial 2014 promise *not* to data mine *WhatsApp* users' data) were addressed, *WhatsApp* as a socio-technical system experienced approximately a year and a half of tremendous growth in terms of the number of downloads and unique users per month. This period of time is also a time of normalization, a time where user experience galvanized into a status quo. Once *Facebook* announced that it would harvest users' data by August 2016, the software's aesthetics assumed new functionality and importance for *Facebook*. The time stamps, status indicators, message/received read mechanisms have been in motion and play since well before *Facebook's* buyout. They are rather familiar to *WhatsApp* users as such. But that does not mean that they have not been newly invigorated with different purpose for Facebook. These features heavily draw the attention of users, so much so that there has been an explosion of discussion since 2015 about how *WhatsApp* is making many of its users behave in intrusive ways upon one another via the app itself.

In April 2015, a Big Data biomedical research team published findings on the relationship between conscientiousness and personality types with the frequency of usage on *WhatsApp*, concluding that of the average of 160 minutes spent on smartphones daily for males of the millennial age group over 30% of that time was used on *WhatsApp* (Montag et al., 2015). Moreover, the findings argued that personality types that were more extraverted used *WhatsApp* more often while introverted users engaged *WhatsApp* less. At first glance, the finding seems rather self-evident. Social media is increasingly generating a type of self-consciousness in terms of privacy; citing earlier that there is a marked increase (>70%) in *Facebook* users deleting their

posts before sending them for publication on their newsfeed. Users indeed are becoming more and more aware of potential privacy violations due to aggressive data mining cultures within *Facebook* in particular, and so the correlation with reserved engagement on *WhatsApp* is not a surprise. The most interesting point to be taken from the study then is how it dovetails other academic work from neighbouring fields that are drawing increasingly more significance from behavioural trends on *WhatsApp*, particularly with regards to corresponding implications of those trends on digital privacy.

Research conducted elsewhere reveals similar insights into how the aesthetics of *WhatsApp* engenders bizarre behaviour between users. A research team at the University of Wurzburg conducted an intensive study on user behaviour on *WhatsApp*. The research was conducted through a survey administered across 250 *WhatsApp* users in Germany during November 2014. One of the most significant pieces of information the research team identified was that of 86% of all *WhatsApp* users used *WhatsApp* daily, and only 6% of those users used regular texting or SMS on their phone by comparison (Cochin et al., 2016). Of the 250 users surveyed, 96% of them answered that they prioritized *WhatsApp* as a privacy *solution* when it comes to digital communication between themselves and their family, friends, coworkers and partners. The point here is that in terms of behavioural tendencies, the research reveals that privacy-oriented communication underpins many of the causes and catalysts behind shifts in behaviour on *WhatsApp*.

As a final example of research exploring the nature of relations between users on *WhatsApp*, the *Cyber Psychology Institute* published that the potential for instant gratification via the meta data mechanisms on *WhatsApp* (time stamps, last read, status and so on) engenders users to what to ‘get what they want’ from their communication as soon as possible

(CyberPsychology Institute, 2016). Moreover, it further engenders the reciprocal feeling that all communication *requires* an immediate response particularly in the sense that there is a socialization effect across *WhatsApp* that produces a norm whereby it would be considered rude to prolong responses. What makes this norm particularly lethal in terms of social etiquette is that it makes users emotionally dependent upon positive reinforcements created by accountability to time stamps and ‘message read’ signals. The more messages are responded to quickly, the more users feel appreciated and this in turn makes users addicted to knowing what is going on with who they are communicating with at increasingly alarming rates. The subsequent issue here for privacy is that when the record of transaction is interrupted or lagged by a lack of response (which translate into negative reinforcements) users may begin hypothesizing issues in the relationship and may also react emotionally in a way that encroaches upon the other users’ space and experience.

These observations are not limited to academics. For example, there has been notable growth of user-generated blog content dissecting the addictive nature of *WhatsApp*, particularly from the point of view of how it is creating depression, dependency and various other manners of correlating emotional and social insecurity – so much so that there is a correlating observation about the kinds of user behaviours that are deemed invasive. Appendix J represents a ‘wikihow’ page that teaches users how to independently measure and evaluate whether or not another user has blocked someone. It was the case at a point in time that *WhatsApp* simply told a user if another user had blocked them. Since a change to the software in 2016, users must do some investigating to find out whether or not another user had blocked them. Interestingly enough, the blog post starts from the rhetorical position that the user seeking help on the page has a ‘suspicion’ worth pursuing. The tone of the language on the top of the page also infers that the

steps required to discover whether or not the user was blocked *is* counter intuitive to digital privacy between users and actually violated *WhatsApp*'s Terms of Use Agreement. As another example of the kinds of user generated content about *WhatsApp* user behavior, an *OpinionPanel* social media site is a satirical account of the kinds of user behavior types that are most suspicious and concerning amongst users. For example, account two identifies the 'nagging Nora' who constantly asks why a user is ignoring her messages, while account three is the 'blue tick Brush off' who reads your messages but never replies (OPC Team, 2016). Blogger Asharful Ayan goes as far as to discuss that of all the blogs and social commentary about addiction because of the meta data mechanisms, that they only way to cure the addiction is to take a two-to-three-month hiatus from the application altogether – it was the way this blogger overcame his addiction (Ayan, 2012).

Caroline Brealey, founder of the UK's *Matchmaker Academy*, recently reflected on the effect of *WhatsApp* on relationships: "Not only do we know they've got our message but we can also see when they were last seen online, which adds serious salt to the wound when you've been waiting for a reply to a message you carefully crafted 24 hours ago. When were they last online? An hour ago. Ouch" (Thompson, 2016). University undergraduates at Sultan Qaboos University recently published a qualitative study in the *International Journal of Psychology and Behavior Analysis*, which examined their own peers' addiction to *WhatsApp* given its prevalence in Oman (AlBarashdi et al., 2016). Professionals from various walks of analysis are concluding, rather simply, that *WhatsApp* is not only addictive but that the addiction is a breeding ground for engendering privacy problems.

The Italian Association of Matrimonial Lawyers say that *WhatsApp* plays an integral role in unearthing evidence of adultery in 40% of all divorce cases in the country (Hanson, 2014). As

an inverse example, but nonetheless salient, the association cites that if a spouse wants to uncover whether or not their partner is having an affair, *WhatsApp* is the preferred method of communication for detecting dishonest communication. The point is that the social media service has at least amalgamated a specific kind of notoriety amongst certain social and political circles due to the kind deviance it attracts; messages containing child pornography, for example, are allegedly ‘secure’ because of the encryption mechanism afforded by *WhatsApp*.

The point is that both within and outside the academy there has been an explosion of observation about the correlation between users experience and the meta-data indicators on *WhatsApp*. The interactions between users do not merely exist in a vacuum. They are, rather, influenced by how users and their behaviours are visualized to one another. The correlation is significant for understanding *WhatsApp* as a socio-technical system because of the triangulation between *WhatsApp*’s owners’ promise for a secured communication experience, the software that provides encryption and displays meta-data and the constraint upon users to make digital privacy decisions for themselves. Users feel protected from hackers and intrusion into the content of their interactions, but their meta-data is not protected whatsoever. Curiously enough, some of the meta-data that is collected is visualized for users, which engenders a very unusual norm amongst significant numbers of *WhatsApp* users.

As a socio-technical system, there is tremendous interplay between the coders from two ownership groups and the software. There are a few noteworthy trends that delineate *WhatsApp* as a socio-technical system. The first trend is documented earlier by means of the introduction of a ‘reliable’ encryption protocol, precisely for the ways in which it engendered a social trust in the technology. Despite their announcements otherwise, coders prior to the *Facebook* buyout promised privacy that was not provided through encryption. Users’ disappointment was further

fueled at the time of the *Facebook* transition as media coverage about *WhatsApp*'s encryption failures and privacy violations, which *Facebook* sought to address by introducing *Open Whisper Systems*' encryption protocol: *nobody* can read your messages, not even us. Users acclimated quickly, and media speculation died off until *Facebook* announced that it would introduce data mining in August 2016. The introduction of this data mining emitted different meaning into the time stamps, last read and status meta data mechanisms on *WhatsApp*, in a way that signifies the dual purposes of said indicators: they not only made users accountable to one another, they symbolically embody the kinds of mining capacities latent in *WhatsApp* itself. And this lattermost point is particularly important here with regards to understanding *WhatsApp* as a sociotechnical system: *Facebook* crafted political positions in and around controversies and worked deliberately to quell them while seeking new ways to harvest data all along, despite their announcements and commitments otherwise. *Facebook* has been actively cultivating a specific idea about digital privacy for the media and its users, the idea that the most serious information violations happen from outside *Facebook*.

The tension between external hacking violations upon users' privacy with criticism of *Facebook*'s internal mining demonstrates rather clearly the evolution of ideas and values between two ownership groups for the ways in which they attempt to disseminate visions about what kind of digital privacy is the most important for not just themselves, but everyone. Users' have thus adapted to how these political and economic processes constituting *WhatsApp*, as documented by the gradual change of the aesthetics of the software altogether. The coders have manipulated the software in ways that keep users docile, committed and engaged to one another not merely because of Zuckerberg's public decree that a connected world is a universal goal for all humans in the twenty-first century, or that users should simply 'enjoy' connectivity in a way

that allows them to speak openly and fluidly without interruption or fear. Rather, users' docility, commitment and engagement also reflects coders' efforts to expand a user base as aggressively as possible in a way that will facilitate data mining. Simply put, the growth of *WhatsApp* as a sociotechnical system is actively animated by ongoing attempts to keep users' and attract users to the software by quelling concern and criticism. The coders worked hard across two ownership groups to maintain and promote users' relation to the software.

But perhaps as importantly as this development is how the software has, on its own terms, dramatically altered how users relate not only to the coders, but to one another. In a move that coalesces rather conveniently for *Facebook* and its coders, the software's meta-data visualization mechanisms engendered a plethora of unusual behavioral patterns amongst users that are not so easily accounted for empirically when analyzing the growth of *WhatsApp* not only from its onset but particularly since *Facebook*'s acquisition. Some speculation here might suggest that given Zuckerberg's previous initiative to manipulate *Facebook* users' emotions, it should not be a surprise that users on *WhatsApp* are experiencing tremendous change in how they relate to one another on affective terms and that *Facebook* certainly knows about it (whether announced publicly or not). The fact that the user basis is *not* simply 'interacting' with one another – the fact that they are interacting with one another in ways that encourages accountability, efficiency and a misplaced sense of intra-relational surveillance – indicates that the software is an extension of the coders' data harvesting desires. So much so that changes in the emotional and affective nature of communication across *WhatsApp* maintains an economic capacity for *Facebook* to continue profiting by harvesting 'unusual' user behavior.

It is as if the initial noisemaking conducted by users in an effort to push-back against the collapse of their privacy is misplaced due to the fact that not all noisemaking produces an effect.

Like the city rat of Bourgault's *Fables d'Espose*, who does not flee at the bang emanating from the front door, the coders and the software of *WhatsApp* have long since conditioned the socio-technical system to collapse upon users' privacy through the time stamp and message-read indicators. The original parasite prevails in its noisemaking, effectively squashing the noises made by users. In doing so, the coalescing of these noises engender an entirely different privacy system. A system of privacy that is completely separate from the 'official' system maintained by *Facebook*. A system of privacy that is not challenged by external violations and gaze, but from gaze within its own ranks and wall – a system wrought with violations that are almost completely unknown to most contemporary privacy scholarship.

Part Four: Conclusion

WhatsApp embodies a significant point of departure from the historical privacy-oriented literature reviewed earlier; the coalescing of noises emitted from coders and the software precludes influence from any noise made by users. While the Exner family, their friends, neighbours and colleagues literally smashed down the walls of *Brunniwinkl* to bring the natural environment into their cottage so as to invigorate private affairs in the name of public politics (Coen, 2007), the noises *WhatsApp*'s coders and software emits similarly broke down walls. A process that also invigorated the emergence of a different plain of privacy, but with a much more implicating horizon of privacy violations. The walls these coders and programmers dismantled were the walls of personal boundaries between users, which comes with tremendous cause for further scholastic attention. A completely different understanding of not only digital privacy but of its implications emerges through the dissertation's study of *WhatsApp*. Digital privacy to *Facebook* is defined by the inability for outsiders (not just hackers, but other marketers as well)

from seeing the content users exchange from one another. Their declaration about digital privacy is one that says, rather deliberately to users, your messages are your business. It is not our right to read them. But what they are saying is that your digital privacy *is* not important enough to preclude us from studying you and selling what we find.

There are thus two ways in which we can understand digital privacy on *WhatsApp*. Digital privacy as ‘the prevention of access to content data’ and digital privacy as ‘the freedom to mine meta-data’. The former is *Facebook*’s explicit declaration of what users most desire, while the latter is *Facebook*’s implicit declaration that users do not know enough or care enough about meta data. The latter is a form of privacy in the sense that the encryption process *precludes* other social media companies from accessing and harvesting the meta data created/found throughout the *WhatsApp* network. Another way of understanding the former is that it is a kind of digital privacy that insulates *Facebook* from the gaze and inquest of the rest of the Big Data and social media industry. It is a corporate privacy, one that monopolizes users’ data and allows *Facebook* to commoditize it. So much so that if other companies want access to it, they must pay for it. It is a kind of digital privacy that emerges through the sheer manipulation of user awareness. It is also a kind of digital privacy that is founded upon the a half-truth about the scope threat and violation upon users’ privacy. *Facebook* aimed to insulate *WhatsApp* users from hackers *and* the industry writ large, not one without the other. *Facebook* has cultivated a kind of digital privacy through this sociotechnical system that allows them the sole access and right to study the largest single entity of global, private instant messaging-based communication and sell that data in any way they please.

As articulated in the second chapter of the dissertation, one of the biggest concerns over digital privacy violations across the academy is precisely about the storing of meta data. For

example, meta data is being routinely used to predict crime (Wolpert, 2015) and has been criticized for playing a massive role in the production of false positives in particular and a reciprocal burgeoning of governing insecurity (as opposed to accuracy) in general (Amoore, 2014; de Geode, 2014). Although meta data tends not to be generally attributed as a source or realm of concern in most privacy violation inquiries – as noted in prominent privacy violations inquiries such as the USA’s FTC investigation of *Facebook*’s harvesting activities (FTC, 2012) or Canada’s Public Opinion Survey conducted by the Office of the Privacy Commissioner of Canada on Canadians’ knowledge on the nature of social media oriented privacy violations (Office of the Privacy Commissioner of Canada, 2016) (in fact, the word ‘meta’ does not appear in either of the two reports cited here) – the language of both reports infers ‘personal information’ and indexes natures of data such as ‘activity’, ‘numbers’ and ‘location’.

The point being that there is a clear disconnect between what data coders are representing as ‘the most important and worthy of protection’ and what they are actually harvesting. As the academy has routinely noted since the turn of the Age of Information, it is the ‘data double’ – the virtual double of the corporeal body – that is of greatest concern when it comes to the indiscriminate profiling and tracking of daily social life for the ways in which aggressive security algorithms piggyback corporate data pools to build assumptions about potential behaviour. Harvesting data for advertising purposes is not nearly as innocent as *Facebook* infers on its own terms for precisely that reason. Despite the fact that the public realm is undergoing a paradigm shift in terms of privacy violation literacy, particularly in relation to meta data, the point is that there are *versions* of privacy here; *Facebook* is appealing to one while completely disregarding another. And as evidenced by the kind of noise the software emits into the *WhatsApp* network itself, the meta-data collecting potential is much, much larger and much more implicating for

users than any source of criticism appears to have concerned elsewhere. And so, the point about the tension between the two kinds of privacy are the wider sociopolitical connotations attached to aggressively harvesting meta data without users' input, let alone their knowledge. There is a discernible recklessness and disregard for users' privacy in the sense that *Facebook* refuses to take responsibility for the dangers of meta data in an age of pre-emptive state security. This tension is also significant because it points towards a third kind of privacy that is birthed as a result of this tension.

There is a third understanding of digital privacy in this socio-technical system, and it is digital privacy as 'privacy between users'. Curiously enough, it is a difficult pill to swallow given the way in which the interests of the coders and the software coalesce in a way that not only insulates *Facebook* from the world around it, but in a way that is creating a communicative claustrophobia. While it was indeed the case that encryption sought to provide users the ability to not have their messages read, the encryption preconditioned a social expectation and understanding that someone's messages on *WhatsApp* are exclusively their own. It is affective, it is emotional, it is protected. It is something you can understand. It is not elusive like most of the encryption mechanisms referred to in the hard encryption discourse where some network somewhere on the other side of the planet is backed up by another separate network that has powerful computers that encrypt and decrypt your data for you. Instead, *this* encryption happens *here*, on your devices for you and your friend only. By shifting an otherwise complicated conceptualization of the world of encryption towards something more intimate such as a process that can happen on users' devices, *Facebook* attempted to make the complicated world of networking and privacy legible for users.

Take for example the ways in which the Snowden revelations acutely generated mass fear worldwide over the vulnerability of information as it flows across the planet. Soon thereafter, social media users across the planet tuned into the stakes of the ‘hard encryption’ discourse – a discourse that the Obama administration routinely weighed in on, regularly citing the necessity for hard encryption in the public sphere. The subsequent unrolling en masse of encryption technologies was dizzying and complex, from cloud services adopting encryption, to VoIP to the world’s most popular social media sites like *Skype*, *Facebook* and so on. But now, it is all done in front of users on their own devices before and between them. A dependency was cultivated between users upon the security offerings of *WhatsApp*, so much so that the introduction of the meta data visualization mechanisms only further galvanized the dependency into a kind of digital privacy expectation that no other social media users on the planet could experience.

Most importantly though, this third domain of digital privacy ‘between users’ is laden with privacy violations. These meta data mechanisms play a dangerous social role across the network, one that encourages many users to encroach upon the space between the phone, heart and mind of other users. The time stamp, status and message read indicators cultivate a system of emotional reward and punishment through positive and negative reinforcements behind the frequency and timing of responses. Users are becoming increasingly more affected by the psychological implications of communication via *WhatsApp*, specifically in a way that undermines the most important component of digital privacy: a user’s privacy to *use* a communication device altogether.

As some of *WhatsApp*’s users alienate other users’ relation to their device and their software, a new domain of infraction and violation emerges and it is one that is *not* officially documented, described or discussed by *Facebook*. To think about digital privacy on *WhatsApp*

requires thinking beyond encryption. It requires attending to these three domains of newly emergent understanding, ones that entirely rearticulate the politics of encryption on social media in general (and *WhatsApp* in particular) as much as ones that remind scholarship that digital privacy is a product of how users, technology and ownership groups react and respond to one another.

Chapter Five: Case Study Three – *SpiderOak One*

The third and final case study examines *SpiderOak One*, a file hosting/cloud service that allows users to backup and host their personal information on servers in the United States. *SpiderOak One* is selected as a case study because it represents the most privacy and security-oriented cloud service product available on the market. Created in 2007, it has been (since its release, but particularly since 2011) and remains *DropBox*'s (which is the largest file hosting/cloud service) largest rival. *SpiderOak One* is recognized popularly for its aggressive approach to encryption, which offers four layers of protocols – as well as a policy mandate – that prevent its employees from seeing or accessing users' personal information. *SpiderOak One* is also particularly interesting because, like *WhatsApp*, the evolution of the product unfolds around wider industry-related politics. Much of *SpiderOak One*'s success emerged as a function of the privacy-related controversies associated with *DropBox* during especially 2011 and 2012. Big Data security issues were more generally plaguing Silicon Valley-based social media products during that same time. *SpiderOak One* is also similar to the previous two case studies in the sense that the noise the coders make and emit towards its users is remarkably consistent. The notion that the product is trustworthy has been a longstanding consistency across the three case studies examined in this thesis.

The chapter begins by providing a brief overview of *SpiderOak One*, which includes a brief technical overview of its encryption and 'No Knowledge' corporate mandate. Part two identifies how each actor emits noise into the wider *SpiderOak One* network: coders for the ways in which they advertise their product as being more safe and secure than rivals' products. This is supported by two claims (about the strength of their encryption and the strict nature of their corporate policy); the software itself for creating a distance between itself and the users (as well

as distance between users and the programmers) because of a bizarre consistency of server disconnects and related software failures that seem to have never been solved since the product's release; the users themselves who are in the precarious situation of being disproportionately technologically literate and as such rather critical of *SpiderOak One*, resulting in noisemaking that seeks to enhance and expand *SpiderOak One*'s encryption capacities as much as they are challenging the very premise that *SpiderOak One* is any different than *DropBox* itself. Part three paints this triangulation of noisemaking together to envision *SpiderOak One* as a socio-technical system, one characterized in terms of users' simultaneous capacity and lack thereof to assist *SpiderOak* in realizing its potential as a privacy-first product. The chapter concludes by identifying the ways in which the development and issues surrounding *SpiderOak One* (as revealed by its rather competent user-ship) engenders a rupture in how users are seeking, up-taking and modulating digital privacy solutions for themselves. *SpiderOak One*'s numerous issues force many users to re-evaluate what files ought to be saved on *SpiderOak One*'s servers whilst moving larger files to neighbouring services (like *DropBox*).

This case study is unique amongst the others because it yields a completely different understanding of how digital privacy is created altogether. As articulated by Bolton's (2013) notion of *parasitic autopoeisis*, the behaviour of the users themselves is a direct and fundamental force in emitting new meaning for digital privacy itself. In Pinch and Oodshorn's (2005) work on the role and utility of users in technological systems, users play a central role in effecting the function and output of technology by virtue of the various different ways in which they interact with a given technology. As we will see here for example, and while digital privacy on *SpiderOak One* refers to the protection of personal information in general, it is in the particulars of combined user efforts that digital privacy begins to constellate in a reliable, pragmatic way.

User noisemaking pushes *SpiderOak One* to function in ways it was not intended. Their noisemaking also reaches beyond the immediate socio-technical system itself, infecting and influencing other file hosting services in a way that dramatically alters the ‘how’ and ‘what’ of digital privacy for users of multiple file hosting products. This case study highlights an unprecedented opportunity for users to reverse the conventional power structure (and as such, conventional understanding) of the ‘regulation’ and ‘control’ of digital information. Moreover, this rather unusual effect of their noisemaking also compels us as analysts to re-assess how users themselves envision and value their own digital privacy and information protection standards.

However, user noisemaking power is not without its ruptures, problems and politics. As inferred by Paddison, Philo, Routledge and Sharp (2000), meaningful change and evolution across digital privacy systems begins with the politics and inconveniences afforded by gaps in relations and experiences; as users continuously engage in hosting different sized files across different platforms, there is a subsequent increase in users’ willingness to prod, test and develop new methods and software technologies for making profit-first corporate products more ‘secure’ just as they had done with *SpiderOak One*. The chapter offers a radically different articulation of digital privacy through *SpiderOak One*, one very different than the other case studies. Users’ noisemaking exhibits disproportionate effects indeed, but that disproportionate effect is cultivated through the coalescing of previously unrelated noise sources made by different users throughout the development of *SpiderOak One* itself.

Part One: SpiderOak One, at a glance

SpiderOak owns and operates three encryption-based software technologies for users. The first is a chat-based and file-exchanging-based browser-oriented technology called *Semaphor*. The second is a password management system called *Encrypt*. The third, which is the focus of this case study, is a cloud-based file storage system called *SpiderOak One*. This software synchronizes in real-time any file a user wishes to have hosted on a server in the United States, the benefit being quick access from multiple points of entry, change and deletion. *SpiderOak One* provides software on both computers as well as mobile devices. What makes *SpiderOak One* particularly attractive as a case study is, as aforementioned, the politics of the industry in general, and the politics around *DropBox* during 2011 and 2012 in particular. This politics provides an interesting context for understanding *SpiderOak One* as a product as well as *SpiderOak One* as a socio-technical system.

As part of *The New Yorker Festival* in 2014, Edward Snowden Skyped-in as a guest speaker. His talk was an argument against using popular social media based software for users that care about their digital privacy, specifically citing companies like *Google*, *Facebook* and *Dropbox*. His point was prefaced by a call for a revision of government policies on digital surveillance, specifically those that send a message to respective populations that ‘as long as you have nothing to hide’ your privacy will not be infringed upon. His point was the way in which such an attitude tends to enable a *carte blanche* approach to data collection, handling and analysis by social media companies whereby anything and everything should be scrutinized because the content users are ‘volunteering’ is not self-evidently incriminating.

Snowden argued that the combination of government policy attitudes about ‘nothing to hide’, coupled with the way it has been subsequently taken-up as privacy policies and public

statement by social media companies, effectively inverts the model of ethical data handling responsibility (Ha, 2014). To Snowden, encouraging users to adopt the mentality of ‘I have nothing to hide’ is akin to saying ‘I don’t care about my rights’, engendering a narrative in popular privacy discourse that works against users. His point was that users will eventually need to demonstrate *why* they need to their privacy. Moreover, Snowden argued that governments and social media companies need to justify their invasion or intrusion upon privacy rights and the content of daily electronic interactions. There are companies that adopt the lattermost perspective, specifically ones that have a business model that precludes data harvesting and mining altogether on the one hand, and supports the model on the other hand through the deployment of aggressive encryption protocols. *Dropbox*, to Snowden, “is hostile to your privacy... get rid of your *Dropbox*.”

“*SpiderOak* has structured their system in such a way you can store all of your information on them with the same sort of features that *Dropbox* does, but they literally have no access to the content. So while they can be compelled to turn it over [to the government], the law enforcement agencies still have to go to a judge and get a warrant to actually get your encryption key from you” says Snowden (Kiss, 2014). Snowden’s endorsement of *SpiderOak One* made the product particularly attractive throughout the cloud services marketplace, which in part constitutes why this product was selected as a case study. But it is not the sole reason.

Further to Snowden’s point, *SpiderOak One*’s encryption protocols and protection procedures tended to be received across the industry, particularly at the beginning of the cloud-services movement in the mid-to-late 2000s, as unrivalled in terms of its encryption and policy standards. For example, *SpiderOak One* ‘hashes’ users’ passwords (a process of mapping any size of data into a fixed size prior to, during, or at the end of an encryption process) and ‘salts’

them (additional data added to ‘hashed’ data, akin to ‘noise’ in the sense that passwords are concealed by extra information) by *Password-Based Key Derivation Function 2* (PBKDF2) – an encryption system designed by the founders of the world’s most popular modality of Internet encryption (RSA – abbreviated after the designers’ last names being Rivest, Shamir and Adleman). The content of the files themselves are encrypted and decrypted with keys assigned for each file, folder and version of each file and folder. Multiple versions of each file and folder thus require different encryption keys, adding extra layers of protection between archiving, retrieval and recovery processes. All of these processes are encrypted using the *Advanced Encryption Standard* AES-256 encryption and decryption process.

To provide an idea about the integrity of this process, as the world’s most complex public-key oriented encryption protocol, it is the same level of standard used by the most sensitive data within the United States government, and twice as strong as the AES 128-bit key that has more than 300,000,000,000,000,000,000,000,000,000 possible key combinations that must be deciphered before any content is made legible to a hacker or adversary (Hacker10, 2011). The AES-256 feature, combined with how keys are generated per file and folder (and history) and unlocked via the user’s password, renders all of the user’s content completely unreadable and inaccessible to *SpiderOak*. Lastly, all of the traffic shared between the user’s device and *SpiderOak*’s servers are encrypted using *Transport Layer Security* (TSL) and *Secure Sockets Layer* (SSL) protocols that ensure uniquely generated and deciphered keys per file transmission even. It is a process that compels both the sides of the exchange (client and server) to verify the identity of one another and negotiate the terms of the file transfer before any exchange takes place (Dierks and Rescorla, 2008). The combination of these techniques underpins what *SpiderOak* calls their *No Knowledge* policy. Because of the way in which the

AES-256 encryption process is oriented towards decrypting files and folders via the user's password, *SpiderOak* cannot access and read users' content. *Dropbox* also uses AES-256 to encrypt users' content, but the unlocking keys are created, circulated and kept by *Dropbox*, which allows them to access, harvest, mine and market users' data (Sullivan, 2014). This is not a possibility for *SpiderOak*.

Taken together, *SpiderOak* differs tremendously from social media-oriented file storage and cloud-based file hosting services in the sense that their commitment and policy-attitude toward data protection not only precludes themselves from accessing users' data (and harvesting it for marketing purposes), it precludes government security and surveillance agencies from doing so as well. In order for any such agency to access users' data, they cannot simply force *SpiderOak* to turn over data via a court order or warrant. The user's device must be accessed as well. And so, the technical nuances and depth behind *SpiderOak One* make it certainly attractive to the technologically literate and illiterate, particularly in contrast to the world's largest file storage/cloud service provider, *Dropbox*.

But these technical qualities only *begin* to account for and explain digital privacy on a file hosting service for users online. Moreover, they produce a rather limited understanding of 'digital privacy' at that. The next section to follow is thus a social account of how *SpiderOak's* coders, users and the software itself all play their own role in noisemaking, processes that – analyzed and accounted for together as a socio-technical system – produce a rather different way of thinking about, with and through digital privacy across the *SpiderOak One* network.

Part Two: Coders, Users and Software Making Noise

The purpose of this section is to account for how coders, users and the *SpiderOak One* software create noise in the name of privacy. Each actor is very socially engaged in their pursuit of digital privacy, much more so than the previous case studies tend to unpack. This process is carried out through actions, exchanges, positions and proclamations that are – as the dissertation argues – akin to ‘noisemaking’: modalities through which each actor attempts to create, structure or influence the unfolding of digital privacy. The goal here is establish the way in which each actor plays a role in digital privacy – to *abstain* from thinking about digital privacy across *SpiderOak One* as merely a technical outcome of encryption processes protecting personal information. As the next section demonstrates, there are numerous stakes in the ‘how’ of digital privacy as evidenced by the preoccupations of different social actors engaged directly and indirectly with *SpiderOak One* itself.

Coders

In a reversal of Serres’ order of experience and outcome at the master/tax farmer’s dinner table, the noise emitted by the coders could not be more different than any of the other case studies. If it is indeed the case that all noisemaking activity infects neighbouring relations, as Serres argued (1982, vii), we must also attend to a less pessimistic evaluation of precisely what those infections infer and implicate. As articulated in the dissertation’s second chapter, Adler and Kretschmar (1991) infect Serres’ logic with their own spin on the nature of parasitism in social relations. Parasites, to these authors, are not only necessary for all natural systems they also make those systems ‘healthy’, ‘liveable’ and ‘thrive-able’. The noise the coders make may indeed come to cause numerous problems but also numerous opportunities for growth of the wider *SpiderOak One* system itself.

SpiderOak One's coders make two kinds of noise that directly affect users, noises that are designed to convince users that their personal information and uploaded content is protected via the most rigorous encryption protocols available, and noises that are intended to reassure users that *SpiderOak* is a privacy-first company. But these noises, as aforementioned, cannot be understood independently. They receive meaning and context via *SpiderOak*'s juxtaposition to competing technologies in general, and *Dropbox* in particular; *SpiderOak One* coder noisemaking is facilitated by the lies, deceit and manipulation of Silicon Valley-based file storage companies. This is a crucial, overarching characteristic of the coders' noisemaking. That being said, the noise coders are emitting into the wider system in general (and towards users in particular) consists of the projecting of messages and arguments depicting their product as more comprehensive and reliable than encryption protocols used by other companies (including the projection of *SpiderOak*'s 'No Knowledge' policy values). Accounting for this noise requires looking back to the founding and unfolding of *SpiderOak* as a company and subsequently *SpiderOak One* as a product.

SpiderOak was founded in 2007 by Ethan Oberman and Alan Fairless, and their first product was *SpiderOak One* (Taulli, 2012). In the product's first launch year, *SpiderOak One* was aggressively advertised as both a free and secured file sharing service. But not merely a service that was available on Macs or PCs. Since its onset, *SpiderOak One* has been programmed on operating systems and computer designs that are specifically tailored for complete user control over the nuances of information storage, flow and circulation – systems that have long since been heralded in the global computer programming community as the most privacy sensitive. Those operating systems include *Linux*, *Ubuntu*, *Debian* and *Fedora* (Haley, 2009). The third version of the software, released in the same year of the software's launch, featured

advertisements in the software's Graphical User Interface (GUI) notifying users that they could also transfer files between operating systems [Appendix L]. While this is generally not easy because different operating systems tend to store files in formats and use different file and folder indexing methods, the goal was to ensure that their product appealed directly to communities that placed emphasis on privacy as much as they did on ease of access.

In a similar vein to Bennett's (2008) observation of the influence of privacy advocacy in developing alternative modalities of digital privacy software so as to counter-act the profit-first influences of social media and government-oriented solutions, the website reviewed in Appendix L is particularly interesting accordingly. *SpiderOak One* fits Bennett's profile because it is designed and marketed towards a more technologically-literate user base than we have seen with the previous two case studies. In particular, *SpiderOak One* met a higher encryption standard for users. *SpiderOak* also appealed to these users by maintaining a company-wide commitment to transparency in their operations and requests by governments to surrender user data. We see that *SpiderOak's* commitment and appeal was maintained beyond Appendix L.

CNet's Tech Culture 2009 review featured *SpiderOak's* website promotion of the 2048-byte RSA and 256-byte AES encryption methods used by *SpiderOak One*, reminding readers that *SpiderOak One* "also encrypts the keys you use to access your data so the company itself can't access your data" (O'Reilly, 2009). In 2010, *Softpedia* reviewed *SpiderOak One* as a product that would be bundled with *Linux's* newest operating system release at the time, which was called *openSUSE 11.3* – a product that was celebrated as being one of the first and most popular cloud storage devices that encrypted all of the data users uploaded (Nestor, 2010). *SpiderOak* was often reviewed as *the alternative* to non-encrypted cloud storage systems at the time. *CNet's* review specifically targeted *Google's* online applications stored data in ways that raised privacy

concerns specifically because they did not use encryption. *PCWorld*'s 2009 review covers eight cloud storage services and emphasizes the password protection feature of one of *SpiderOak*'s encryption protocols (Fleishman, 2009).

In and amongst these reviews was not only emphasis upon the kinds of encryption the company was using. There was also emphasis on a wider, institutional value system presented for users in the form of a corporate policy. This corporate policy was designed with two objectives in mind: to constrain *SpiderOaks*' employees from accessing users' information; to respond to how other data storage companies were approaching the treatment of their users' information. The lattermost began to unfold more acutely around 2011, but there is an abundance of evidence with regards to the promotion and reception of these values in the cloud service market beforehand. Technical overviews beginning as early as 2009 (CloudStorageBuzz, 2009), user discussions on the *AskUbuntu* user forums as early as 2009 (*AskUbuntu*, 2009), *HackerNews* discussion forums (HackerNews, 2009), computer science analysis blogs (Marcey, 2009) and *AlternativeTo* – a crowdsourced voting system for the most trustworthy cloud services projects in the late 2000s, which voted *SpiderOak One* as the most secure and competitive hosting service (AlternativeTo.net, 2009) – all emphasize *SpiderOak*'s 'No Knowledge' policy.

The policy in particular states that "SpiderOak has been building products on the principle of *No Knowledge*. No Knowledge means we know nothing about the encrypted data you store on our servers. This unique design means nothing leaves your computer until after it is encrypted and is never decrypted until it is unlocked with your password on your computer. It's not just 'end-to-end' encryption, it's a No Knowledge system" (*SpiderOak*, 2009). While this policy statement was indeed emphasized as a point of promotion and intervention into a marketplace that is social media and data-mining as the first point of corporate order well into

the late 2000s, *SpiderOak* began to reap the benefits of a more acutely emitted and more warmly received noise once *DropBox* became *the* most popular – and subsequently most controversial – cloud hosting service.

By early 2010, *DropBox* hosted over two million users (Gannes, 2009). By late 2011, it surpassed 50 million users and hosted over 200 million by early 2012 (Houston, 2012). As a start-up out of Silicon Valley that began at the same time as *SpiderOak*, *DropBox* was principled off of different social values – ease of access, cross-platform (mobile, PC, Mac), free use and high bandwidth/storage capabilities. Since its creation, *DropBox* has maintained a ‘freemium’ business model, which offers users a free account up to a certain amount of data storage (Teixeira, 2013). Between its rise to the top of the cloud market in 2011 and 2017, less than 4% of users actually use the pay-service; the majority of users stick with the 2gb limit. But there is a catch. *DropBox* does not merely produce its revenue from paid cloud services – it aggressively mines both the content and meta data users store on *DropBox*’s servers (Nathanson, 2014). The service is easily adaptable to popular analytics firms, such as *Google Analytics* (Zapier, 2014). *DropBox* also secretly acquired *Parastructure*, an analytics industry leader in data analysis (Lunden, 2014).

Positioning their corporate mandate as a profit-first model, as is typically the case with Silicon Valley social media-oriented business models, the choice to attract users and mine their data for profit purposes precipitated disastrous media coverage about privacy violations in and around their product. Since well before Snowden’s 2014 declaration that *DropBox* is hostile to users’ privacy (Connors, 2014), *DropBox* has been plagued with security issues that intimately dovetail their business model. Between 1:54pm PT and 5:51pm PT on 19 June 2011, *DropBox* updated its software. Any user logged in, uploading, downloading or making changes to their

files, was susceptible to a coding error that allowed any user on *DropBox* to see and access other users' accounts. Simply put, users were able to access one another's passwords (Bosker, 2011).

What is particularly interesting about the cloud service industry at the time of the issue was that the time period is characterized by widespread marketing pressure by Silicon Valley for users of numerous walks of social media to 'move' their content 'to the cloud' (Ibid). Recalling that *Sony*, for example, waited numerous days before telling 100 million users that their accounts were attacked, 2011 was a precarious year for *DropBox* to become the cloud industry leader. *DropBox* thought it was getting ahead of the security curve that year, so-to-speak, by introducing encryption to the service followed by a statement that *DropBox* – like *SpiderOak* – could not access its' users content (Singel, 2011). Prior to 19 June incident, PhD student Christopher Sogohian – a popular tech journalist and analyst through numerous US-based alternative media conglomerates and who was featured on the *Colbert Report* for his research on NSA privacy violations that year – filed a complaint to the FTC citing that *DropBox*'s claims and encryption standards were lies (Ibid).

A fundamental difference between *DropBox* and *SpiderOak* is that while they used similar encryption methods, only *SpiderOak* users had access to the decryption keys; *DropBox* kept all of the keys on their own servers (Kobie, 2011). It is perhaps important however to take into consideration the 'context' of this relationship between the coders and their users, as Nissenbaum (2009) tends to place so much emphasis upon. It is not merely a company policy about 'transparency' and a promise over a reliable hard encryption system that attracts users. It is the tension in the wider industry surrounding the distrust of profit-first file hosting services like *DropBox* that makes *SpiderOak One* a more appealing alternative. And so, with these issues on

the forefront of media webpages and the minds of users concerned about their privacy, security issues continued to unroll for *DropBox*.

DropBox's smartphone client fails to effectively utilize SSL/TLS encryption (Prinzlau, 2012); information security analyst Derek Newton uncovers that *DropBox*'s username and password encryption process did not work (Newton, 2011); researchers argue that *DropBox* has worked hard to aggressively censor internal knowledge of their own security vulnerabilities from the media (Kholia and Wegrzyn, 2011); 60 million usernames and passwords leaked from stolen employee credentials (Cox, 2016). *DropBox*'s string of follies continued for years, around security issues in general, and a lack of trust by users and media about *DropBox*'s ability to use encryption effectively, which intimately contextualizes *SpiderOak*'s noise projections and in numerous ways.

Since *DropBox*'s 2011 security follies, *SpiderOak*'s noise has amplified amongst the marketplace, users and the media. In 2011 alone, for example, there was a marked change in tone of the nature of blog-oriented review about *SpiderOak*. A long-time *DropBox* user, Brian Belshaw, blogs specifically about the year's security breaches catalyzing further concerns about his ability to protect his personal information during a time when the Snowden revelations were continuing to surface (Belshaw, 2012). Blogger *Rolfje* notes that as a user accustomed to *DropBox* since its release, he was particularly concerned about *DropBox* not using regression testing techniques to prod for their own security issues revolving around the usage of their encryption protocols. He also cites numerous changes in the privacy policy that continue to dilute users' rights over the information they store on *DropBox*'s servers (Rolfje, 2011). Blogger Jane Litte recounts *DropBox*'s susceptibility to warrantless information surrender because they do not prioritize 'No Knowledge' and privacy-first values in their corporate structure (Litte,

2012). Blogger *NetNinja* outlines *SpiderOak* as the new industry-wide favourite to *DropBox* due to 2011's proliferation of lies (Netninja.com, 2011). As a final example, Bill Latham – an American business litigator – argues that *DropBox*'s choice only to implement encryption during data transmission is ethically irresponsible, thus necessitating his argument in favour of the immediate adoption of *SpiderOak* for any individual (Latham, 2012). The change in tone and reception to *DropBox*'s follies indeed amplified *SpiderOak*'s noisemaking – that their product was the most effective privacy solution *because* they did what their competitors could not. Unfortunately for *SpiderOak*, its users emitted (and have been emitting since) a very different kind of noise.

Users

In a continued reversal of Serres' dinner table arrangement, *SpiderOak One* users embody a far more differentiated experience dining with the tax farmer than the guests considered in Serres' text. While some heeded and aligned to the noises the tax farmer or coders emitted, this is an example where the noises emitted by the coders coalesce rather efficiently and productively for the wider *SpiderOak One* network. What follows is an account of what Serres (1982, 14-16) argued to be an inescapable feature of any social system created by noise emissions – they are never static, they are never concrete. The noises the users emit into the *SpiderOak One* network have created numerous, differentiated and relatively unpredictable outcomes for the network writ large. In some ways, they instantiate growth and in others, they instantiate a complete departure from the system itself – not to escape the system, but only to revisit it, reassess it and re-harness it in different ways and for different, unanticipated purposes.

Users have been emitting their own noise into the *SpiderOak One* network by modulating their behaviour to enhance their own privacy. The character of their noise emissions is rather different than the previous case studies and for a specific reason. Perhaps as an implication of the social context around which *SpiderOak* unfolded – and upon which the Snowden revelations, security follies and general disregard for users’ privacy on the behalf of social media companies throughout the early 2010s – *SpiderOak*’s user-base tends to be disproportionately more technologically literate than *DropBox* users. So much so that they have been rather intimately involved in the evolution of *SpiderOak* altogether. The blog posts, forum discussion and computer science research papers around the follies of *DropBox* (as outlined in the previous section) are mirrored by an increasing correlation in similar posts, papers and discussions surrounding the technical dimensions of *SpiderOak*. For example, and prior to 2011, *Mac’s AppStorm* technology blog discusses how users can deploy *SpiderOak* as a data backup tool as opposed to a utility simply used for permanently transferring files ‘to the cloud’ (Johnson, 2010). Technology blogger Warren Post walks users through a solution to the difficulty of transferring file tables between versions of the *Linux* operating system (*Mint* to *Mageia*) – an issue surrounding hard drive partitioning techniques – for the ways in which such transfers can confuse *SpiderOak*’s software and thus compromise encrypted data (Post, 2012).

As another example, Tom McFarlin’s 24 October 2013 blog post guides users through the logistics behind switching mobile app platforms and computer based platforms simultaneously as he removes and transfers all of his content from *DropBox* to *SpiderOak* (McFarlin, 2012). And so, users’ noise emissions can be traced in two separate (at times reinforcing, at times contradicting) ways: manipulating *SpiderOak*’s software to enhance privacy and privacy-benefits overall; scrutinizing *SpiderOak*’s software to detect vulnerabilities.

The first modality of user-oriented noisemaking surrounds efforts to enhance their own privacy in and around *SpiderOak*. This modality unfolds a few different ways, with different purposes and with different outcomes. The first example entails the usage of *SpiderOak* to back-up the content of external devices' content data to *SpiderOak*'s servers. This modality is particularly unique because it is not a self-evident process. Rather, it is something that requires technical manipulations of operating systems in order to utilize effectively. The *Synology* community blog documents a discussion amongst *SpiderOak* users around a particularly *Synology* product, the *DS216+*. It is an external hard drive, or what is technically classified as *Network Attached Storage* (NAS) – a stand-alone computer that is networked as a server system meant solely to provide numerous individuals the ability to access and store data in large volumes. The *DS216+* in particular is an interesting case because the technology is a rather powerful computer unto itself. It uses a processor that is as fast as most shelved netbook processors found in consumer electronics stores. It houses up to 108 terabytes of information, which tremendously exceeds the storage capacities of most consumer products. The operating system on the *DS216+* also uses *Intel*'s AES-NI encryption protocols, a processor-based encryption method that is designed specifically to respond to cloud-based business needs where slow encryption times are effecting businesses. In the particular case of this community discussion, user *Krokodyle* is seeking assistance on how to use *SpiderOak* as a backup to his backup storage (*DS216+*). His NAS is established on a PC-based computer, and he wants to use the *SpiderOak* software to point towards his NAS so as to back-up the files by means of uploading them to *SpiderOak*'s servers.

The issue is that the process of uploading the information in this way creates numerous redundant relays between the PC, router, NAS then back to the router, PC, and finally to

SpiderOak. This requires leaving the PC on for extended periods of time, which runs the risk of being interrupted due to hardware or network failure, and as such, could potentially compromise the data. After three users could not assist, *Krokodyle* researched and designed a thirty-one stage solution (the details of the process are available below¹⁰). The example demonstrates a particular technological fluency amongst the user base, particularly in terms of their ability to expand and extend *SpiderOak One*'s encryption capacity, making the software perform a privacy-oriented function that it was not initially designed to conduct. The example is particularly important because, as a noise emission on its own terms, it signifies an attempt by users to structure digital privacy via *SpiderOak One* on their own terms but also in a way that compels a wider reach and coverage of digital privacy than imaginable otherwise.

Another example of user-oriented noisemaking comes in the form of a rather committed investment into enhancing and amending the coding of *SpiderOak* itself. While Paddison, Philo, Routledge and Sharp (2000) theorized that gaps facilitate forward progress for the creation of new meanings and understandings of privacy, this example fills the gap. In 2009, and as part of *SpiderOak*'s commitment to a privacy-first mentality, the company began opening up its coding as a publicly available repository on *GitHub*. *GitHub* is a social media platform for computer scientists and computer programmers. It allows them to engage one another and discuss programming problems, as well as to engage those problems directly by means of accessing the coding and software itself. The basic sharing/solving/amending process works by the owner(s) of a software product releasing the coding structure of its software and publishing it on *GitHub*. Programmers can engage the coding directly and analyze it for vulnerabilities, to find and

¹⁰ The process involves installing *SpiderOak One* directly onto the *DS216+*, adding the NAS as its own *SpiderOak* account, establishing a task order of basic commands and functions so as to automate the backup process towards *SpiderOak*'s servers and establishing a backup schedule as well. Details are available: <https://superuser.com/questions/1148309/how-to-backup-nas-to-spideroak-cloud/1150466#1150466>

address issues shared by the owners and to suggest changes for efficiency or security purposes. The collective process of sharing and fixing software openly is what is more popularly referred to as ‘open-source’.

Open-sourcing a product has become one of the most crucial signifiers of trust and reliability amongst privacy-first software companies, not only because it opens their product to public scrutiny (to check for backdoors engineered into encryption models, for example) so as to prove that the NSA (for example) does not have a secret pathway to intercept or ability to decrypt information. It also allows the company to reliably demonstrate that its encryption models are tested by a wider knowledge network about the evolution of security threats by means of algorithm-based, virus-based or other related hacking attempts. There are numerous locations on *GitHub* that allow users to engage the software directly, one of which being *SpiderOak*'s ‘crypton’ subproject. This subproject allows users (as volunteer programmers) worldwide to assist in designing a framework that translates the ‘no knowledge’ policy directly into coding for mobile and desktop products. The subproject documents a conversation between programmers and *SpiderOak One* coders – a signifier of the efficacy of user-oriented noisemaking in co-operated effort in creating a more meaningful, reliable and accountable modality of digital privacy that works for both the coders and its users.

Conversely, users also emit noise on the behalf of their own privacy that scrutinizes and criticizes *SpiderOak* as opposed to simply extending, adding or improving *SpiderOak*. Noise, as Attali (1997) argued, politicizes what someone hears. While composer John Cage opened the doors to his concert hall – inviting the noises of the cityscape into an otherwise orderly and quiet space – he effectively re-articulated the meaning and purpose of social expectation, experience and understanding. While his example refers to how listeners come to relate to the music they

hear thereafter, Attali's point is more instructive in a conceptual and abstracted sense: noise politicizes how social life experiences itself, and in doing so, calls critical attention towards the subject matter in the name of preventing the subject matter from being taken-for-granted. Like John Cage's opening of the doors, *TCnext* (a *GitHub*-oriented platform designed specifically as a social media platform for community-based encryption analysis), similarly invited a different kind of noise into the wider *SpiderOak One* socio-technical system.

On *TCnext*, user *LOVEINT* expressed a specific concern about suspicious background software activity on *SpiderOak One*. The user outlines her difficulty in an attempt to upload a rather large file to the *SpiderOak* servers. After realizing that the file upload process became very slow, she deleted the file and attempted a restart of the upload process. The user 're-scanned' her file index on her computer to signal to the software that the file was indeed deleted and available for upload. To her surprise, the software was still uploading the file since its deletion and re-scan – a process that should have refreshed the entire process altogether. After closing out the software, rebooting and deleting her temporary files folder and browser cache, only one piece of software was still attempting to engage the file, which was *SpiderOak One*. The file was still being uploaded, even though it was deleted. After presenting the problem to two separate communities, users were similarly baffled (verax74656, 2015). The problem was picked up by user verax74656 and communicated with programmers on the '/SpiderOak' subreddit.

The issue was replicated by this second user, on a completely different computer. The user encountered the exact same problem, which was also mirrored by user *jamesbritt* (verax74656, 2015). The implication of the issue is two-fold. The first being that the *SpiderOak* encryption system is not performing the way the company argues it should work. In order for the file to be continually uploaded despite being deleted, the community members' investigation

argues that the hash/checksum encryption process (of assigning data size values to fixed locations in the initial encryption process and the subsequent process of verifying the integrity of the initial process) is comparing users' files against the entire database of the entire company's user files. To be able to upload the file after it is deleted requires the *SpiderOak* cloud management software to be able to uniquely identify files across the range of connections to its servers – a capacity that is completely counter-intuitive to not only the anonymity-establishing nature of the encryption protocol itself, but also counter-intuitive to *SpiderOak*'s 'No Knowledge' policy. Since the time of the posts and after community requests to *SpiderOak* for a response, *SpiderOak* has not provided one.

The significance of this particular modality of noisemaking by users is found in the fact that it establishes a wider field of opportunity for *SpiderOak One* to extend and expand upon its digital privacy capacities. As demonstrated by the first two user-oriented examples, there is ample evidence of social activity amongst the company's user-ship that can be harnessed to expand the product. A similar opportunity is afforded, arguably more so, but 'hacking' the product to reveal any vulnerabilities. The lack of response can similarly be argued to have relevant socio-political connotations, but the point – regardless of response – is that all examples aforementioned reveal that users are intimately invested in structuring the kinds of digital privacy they expect and demand from *SpiderOak One* on their own terms.

Software

The software itself emits its own noise, a noise that plays a role in manipulating distance between itself and the programmers and users while also closing gaps between coders and users.

This noise most closely relates to the sound at the door in Serres' dinner table depiction. While Serres (1982, 3-5) argued that the bang at the door that interrupted the meal of the rats as well as the meal of the tax farmer and his guests, the noise is a source of information. It interrupted the meal. It created a pause upon which all relations and interactions were suspended. The moment upon which those interactions return is also a moment of realization that what proceeded prior to the noise cannot proceed the same thereafter. Thoughts are redirected, anxieties are heightened for some while relief is provided for others. Conversation topics may change and sightlines may change as well. Bodies are repositioned and repostured while a difference in the order of what food and drink is consumed unfolds as well. But perhaps the most significant point here is that noise at the door – as its own parasite on its own terms – does not stay. It creates a lasting impression upon the social system of the meal. And until another noise returns, the social system attempts to stabilize as best as it can. This is precisely the role embodied by the software in the wider *SpiderOak One* socio-technical system.

And so, the noise the software generates can be evaluated in one distinct way: by creating numerous, continuous and frequent disconnects from the *SpiderOak* servers despite, at times, indicating otherwise. There are numerous issues with *SpiderOak One*'s software, but issues surrounding the usability and reliability of the software have been plaguing *SpiderOak One* since its inception in the late 2000s. Prior to engaging those specific issues, however, it is important to identify a fundamental characteristic of *SpiderOak One* that has been generating issues on its own terms.

One of the most significant drawbacks of *SpiderOak One* has been reception surrounding the software itself. Appendix M is a picture of the original release of *SpiderOak One* in the late 2000s, as well as *SpiderOak One* in 2017. In terms of its graphical presentation and design of the

user interface, very little has changed. While the lack of change in terms of presentation and interface may otherwise be recognized as a commitment to sustaining a uniqueness in the cloud service marketplace, that very uniqueness has positioned *SpiderOak One* in a disadvantageous position amongst its user-ship. The issue stems from *SpiderOak*'s marketability as a privacy-first solution. The majority of the coding efforts have been invested in to *SpiderOak One* as something different than what was and is available as a cloud service solution for users. As a result, the aesthetic presentation of *SpiderOak One* is rather different than anything else available in the marketplace.

Part of what made *SpiderOak One*'s primary competitor (*DropBox*) particularly successful in late 2010/early 2011 was its aesthetic familiarity for most any PC user. *DropBox* is designed to mimic a computer folder on PC and Mac-based products [Appendix N]. *DropBox* places both a folder on users' desktops, as well as in the taskbar, that opens-up a link to *DropBox*'s server. Files and folders are simply dragged-in or dragged-out, created or deleted, inside the folder just as any other folder on a computer system. *SpiderOak One*, on the other hand, is a dramatic departure particularly in the sense that its GUI is not reminiscent of any popular computer-oriented filing and storage conventions. As depicted in Appendix N, *SpiderOak One* is a standalone minimized window in terms of a GUI. It is broken-down in terms of five sub-windows that allow users to upload, backup, manage, sync and change settings of their account. The software privileges details of synchronization and its histories for users at the expense of providing a discernible and familiar indication that files are synced as well as at the expense of allowing users to navigate folder structures easily. The unorthodox nature of its aesthetic has long since plagued *SpiderOak One*'s reception amongst users, and as such served as a barrier to users wanting to learn the software's intricacies and allow themselves to become

familiar with it. This characteristic of *SpiderOak One*'s software is particularly important to the purpose of the case study because it serves as noise in its own right – a noise that infects users' relationship to their own hosted data by means of interrupting (like a bang at the front door) that relationship and subsequently offsetting its original significance and meaning.

The second noise emanating from *SpiderOak One* is a curiously long standing issue with routine disconnects. The disconnects literally refer to a loss of connection between users and the *SpiderOak* servers, which happen with little to no indication to the user. The issue is well documented since the software's release in the late 2000s, but grew substantially throughout 2011 and into the mid 2010s. Numerous technical blogs have reviewed the issue of *SpiderOak One* routinely disconnecting the user from the *SpiderOak* servers (Cymru, 2013; Glatter-Götz, 2013; Shead, 2011). As users continued to notice these disconnects, the software's GUI – particularly during the earlier releases – did not indicate that there was a disconnection, thus requiring users to investigate whether their files were uploaded. In a *Reddit* post from mid 2016, users *pinkghost*, *blank7fan* and *amaiman* discuss discovering that while they were uploading files to *SpiderOak*, the software disconnected. "Disconnected" is indeed a status, but is one that is not immediately discernible as such to the user; no flags, indications or updates allow the user to know that the process is interrupted. Joseph Lo's technology blog reviews *SpiderOak One*, particularly around the 'bugs' and 'glitches' of *SpiderOak One*. One of the central issues discussed here on his 12 December 2013 post surrounds an issue where files sit in queue for upload near indefinitely (Lo, 2013). The blogger's primary concern is that if a file begins to be uploaded, and pauses during the upload, it will move the queue but will remove any part on the server side in the process. Game developer *KimikoMuffin* experienced similar issues that next year, not merely with the data sitting in queue but rather during the 'syndication process' (where

SpiderOak One transfer all user information to the server and back to verify a connection) indicating that the connection had frozen and eventually dropped altogether (KimikoMuffin, 2014).

In 2013, blogger *die Technik* experienced the same issue as the previous user, which prevented him from transferring files and updating *SpiderOak One* altogether (*die Technik*, 2013). Multiple users expressed frustration with the upload process being very slow and often disconnecting in a 2015 *SpiderOak One* review on *CloudWars.net* (CloudWars, 2015). Perhaps one of the more consistent issues with the disconnects altogether stems from the fact that *SpiderOak One* does not boot itself online once started altogether. This has also been a persistent issue since the software's release. These two users (Conrad, 2013; Iloncosky, 2013) not only indicated the issue, they discussed strategies for forcing *SpiderOak One* to boot and stay online by programming separate scripts or changing auto-start settings in *Windows 7* to make the software boot and stay online.

Both noises taken together – the unusual aesthetic properties as well as the curiously consistent nature of the disconnects – reveal that the software is playing its own role in the unfolding of digital privacy. It plays a role not only in the sense that it is structuring, facilitating or giving rise to a sense or experience or expectation of digital privacy for users. The software's noise emissions are also parasitic. They tend to interrupt and disrupt connections between users and coders. The following section presents evidence of the ways in which the software itself tends to discourage and distract usage amongst its user-ship because the software is glitch-y, underdeveloped aesthetically and even awkward to navigate. While there are users who are technologically savvy enough to ignore such issues and persist onwards, the amount of frustration caused by the software's graphical design and layout is particularly problematic.

To understand *SpiderOak One* as a socio-technical system depends upon this tendency to distract and discourage users, which invariably effects how users come to relate to and value the information they are attempting to upload. This development is significant for the thesis on the one hand and privacy policy literature on the other hand because it makes very legible the tangible, tractable and inextricable role and influence users play in the unfolding of digital privacy. For example, Westby (2004), Svantesson (2015) and Dowling (2009) fall prey – like most digital privacy literature – to reifying the belief that the onus of digital privacy ought to fall upon corporations and governments. This development turns this belief on its head; the tendency to approach digital privacy as a matter of regulation and control is clearly showcased in the section that follows – as well as its wide ranging implications across the file hosting industry.

Part Three: SpiderOak One as a Socio-Technical System

Taken together, the noises each actor emits intersects in ways that render an understanding of *SpiderOak One* beyond merely a technical system. As a socio-technical system, *SpiderOak One* has grown and retracted and in the process of extending privacy as much as it has constrained privacy. In order to come to a more comprehensive understanding of digital privacy in the context of *SpiderOak One* (which will be discussed in the concluding section of this chapter), this section will intersect each noise transmission and discuss the significance of those intersections so as to provide a comprehensive understanding of the unique preconditions of a different kind of digital privacy unfolding in and around *SpiderOak One*.

As *SpiderOak One* entered the cloud service marketplace, the privacy-first orientation of their product and the rather unrivaled nature of the layering, positioning and purposing of their encryption protocols quickly established *SpiderOak One* as a superior alternative to *DropBox*.

While it was indeed the case that *SpiderOak One* was primarily received in the context of the premiere privacy-first solution, it was also marketed by *SpiderOak* as an everyday file service as well. For example, the *Mobile Mac* section of *Macworld* emphasized *SpiderOak One* as an easily accessed and used as an alternative to *Apple's MobileMe* (Kissell, 2009) with no mention of *SpiderOak One* as a secured device. Wen's 2010 review *SpiderOak* on *ITBusiness.ca* similarly compared *SpiderOak One* against *Apple*, *Google* and *DropBox* with no mention of any privacy-enhancing or encryption-related properties (Wen, 2010). The point is that as much as *SpiderOak* was heralded as a privacy-first company, it was also simply received as 'another' cloud service. The point here is that both marketing trajectories generated an expectation amongst user-ship that *SpiderOak One* could not only do what any other file hosting service could, it would do it better. This was certainly the case in terms of its securitization principles, but perhaps only for a while.

The noise the coders emitted into the *SpiderOak One* network, and into the marketplace-at-large, attracted some of the Internet's more technologically literate and encryption-literate users. Part of the reason this was the case is because, and as aforementioned, users identified very quickly that *SpiderOak One* was not easy to use. *SpiderOak One's* unorthodox GUI meant that users needed to adapt to *SpiderOak One* in order to fully harness its capabilities. In the case of users desiring to extend *SpiderOak One's* encryption talents elsewhere, tremendous commitment is required in order to investigate, script and execute external functions in order to make *SpiderOak One* speak to other parts of a host computer. But users looking for a more secured file hosting service, particularly around the time of the 2011 privacy concerns along with the wider issues surrounding security follies at *DropBox* and *Sony*, expressed frustration with the GUI. One of the more notable technology bloggers aforementioned, Doug Belshaw, amended his

original post about leaving *DropBox* for *SpiderOak One* and having to move back to *DropBox* because of *SpiderOak One*'s usability and disconnect issues (Belshaw, 2013). On that blog post's comments section, users *Moystard*, *tzo1516*, *Max*, *Antoine*, *Jackson10* and *sconaty* expressed paralleled sentiments in the sense that *DropBox* could still be used on the side for files that 'did not need as much protecting' or that *DropBox* could be made stronger via users' emitting their own noise (writing scripts, adding new encryption software to *DropBox* to make it stronger, and so on). The GUI's issues, compounded by the software's own noise emissions played a significant role then in undermining the noise emissions the programmers were emitting into the network. The software was emitting a noise that was trumping the programmers' noise, so much so that a different array of investigation amongst *SpiderOak One*'s more technologically literate began to unfold.

The unorthodox aesthetics of the *SpiderOak One* left users having to investigate for themselves whether or not files were being uploaded. Due to the constant disconnects as well, users were further disadvantaged in the sense that if large files needed to be uploaded throughout the day – a process that is already slow, especially given the fact that encryption extends any uploading and exchange process – users were required to monitor the upload process rather directly. Monitoring software, particularly cloud services software, is counterintuitive to its purpose. The onus of storage and management – and particularly the security of anonymity provided by encryption – ought to allow users to 'drop and forget' their personal information altogether. As aforementioned, part of the marketing boom for cloud services in the late 2000s was to compel users to free-up their time by allowing corporations to manage their data, and secure it. In the case of *SpiderOak One*, many users sat and monitored the software to ensure it

was working. This has corresponding implications upon how users relate not only to the software, but to themselves, other products and to the programmers of the product itself.

As a socio-technical system, *SpiderOak One* is unique in the sense that its coders and its users were rather consistently disconnected from one another through the alienating and failing dimensions of the software. How and whether those disconnects were abridged plays a significant role in giving shape to this system. Coders who envisioned a privacy-first service across numerous platforms, particularly ones outside of the PC and Mac market, reached out to a technologically literate user-ship that aspired to experience the vision – so much so that many users took it upon themselves to highlight, amend and expose vulnerabilities in and around *SpiderOak* and its services altogether. A social norm galvanized as a result. Users began engineering their own knock at the door of the diners in Bourgault's *Fables d'Espose*. But one that will have much more effect than the users who attempted a knock in the previous case study. It began to unfold within the past five years of the aforementioned user-oriented investigations into both the potentialities for further coverage by *SpiderOak One* as well as its limitations. The norm galvanized over the past five years into a deep rooted suspicion upon whether or not *SpiderOak One* works as advertised altogether, or whether or not *SpiderOak* as a company understands the coverage of their own encryption protocols work on the other.

The first stream of investigation unfolds around user-oriented analyses of *SpiderOak One*'s technical operations. Recalling *LOVEINT*'s investigation, for example, which argued that *SpiderOak One* inadvertently renders its own security practices insecure because of the way in which it does not release deleted files during the upload process. *LOVEINT* claimed that because credit card information is collected on the website (as opposed to bitcoins) it is not possible that the 'No Knowledge' policy (and the encryption protocols, subsequently) are as extensive as

SpiderOak insists. The second unfolds around user-investigation into the politics of *SpiderOak One*'s posture as an 'open-source' product. The official announcement for open-source access to *SpiderOak One* was in February 2013, at the *RSA Conference* in San Francisco, California (MarketWire, 2013). The announcement was marketed as an unprecedented opportunity for users/programmers worldwide to take part in making *SpiderOak* accountable by collaboratively working on and further developing encryption protocols and standards that are openly visible to the scrutiny of the company, industry, market, worldwide programming community and user-ship at once.

The call for open-source cloud computer solutions has, however, been persistent since the late 2000s. Open-sourcing software for security purposes has been an ideal well established in the computer sciences industry since the early 1980s (Casson and Ryan, 2010); *SpiderOak* first marketed their product as backed by founders and engineers who have strong open source backgrounds and experience (SpiderOak, 2008). In fact, *SpiderOak* has been declaring that they would release their code for open-sourcing as early as the release of *SpiderOak One* in 2007 (Garron, 2009). As of 2017, *SpiderOak One* is indeed on *GitHub* as an open-source, but only certain dimensions of *SpiderOak One* are actually accessible to user-ship. *SpiderOak One* is, so-to-speak, *partially* open-source, which has generated controversy amongst users and programmers¹¹ regarding whether or not *SpiderOak* – after ten years – is hiding something by not sticking to their promise to release the product to open source.

¹¹ See discussions amongst users from aforementioned blog posts and subsequent discussions on *Reddit* (https://www.reddit.com/r/SpiderOak/comments/3rv9ax/something_very_fishy_about_spideroak_can_someone/?st=j0spnw3u&sh=af3d2423), *ArsTechnica* (<https://arstechnica.com/civis/viewtopic.php?t=1204257>) and *TCNext* (<https://forum.truecrypt.ch/t/something-very-fishy-about-spideroak/826>)

The development of these modes of questioning and investigation about *SpiderOak One*'s user-ship is a particularly dynamic characteristic of *SpiderOak One* as a socio-technical system. It reveals the way in which the noise the software and the programmers emit clash at the site of experience and interaction for users. While part of the backbone theory of the dissertation draws upon the notion that gaps in relations facilitate opportunities for bridging and thusly creating new relations (Paddison, Philo, Routledge and Sharp, 2000), the clash of coder oriented and user oriented noise maintains gaps. It is important to recognize that the evolution socio-technical systems do not depend upon a strict coalescing and co-operation of efforts. Tensions, ruptures, preclusions and gaps also play a pertinent role in creating new avenues for recovery and recollection which in turn instantiates new (although unanticipated) growth; this is a crucial implication of Bolton's (2013) notion of *parasitic autopoiesis* – in order for social behaviour to catalyze meaningful change about how social groups engage and understand digital privacy itself, conflict and clash are necessary and inescapable preconditions as such.

On the one hand, *SpiderOak One* gains tremendous support because of external controversies and displacements from previous and current *DropBox* (or other rival cloud service products). And the level of technological literacy amongst that group has made *SpiderOak One* stronger in the sense that its vulnerabilities and limitations are being exposed, negotiated and amended. On the other hand, however, *SpiderOak One* is as susceptible due to the dual pronged nature of the noise tensions. Users are also demonstrating frustration to the point of abandoning *SpiderOak One* altogether, and perhaps most curiously and most interestingly, in an attempt to regain usability *despite* the cost of lost privacy in returning to products like *DropBox*.

As the next section will discuss, the norm that has emerged amongst *SpiderOak One*'s most committed user base has positioned them to re-evaluate and re-assign their own meaning

and priority over their personal information particularly in terms of where it is hosted and by whom – a position that radically alters our analysis and understanding of digital privacy by calling attention to the relationship users of digital privacy systems are building and amending on their own terms with their own personal information on the one hand but also who/where that personal information is managed/located on the other hand. And in a dramatic turn from Serres' account of the dining room experience in Bourgault's *Fables d'Espose*, users successfully engineered the knock at the door in a way that not only interrupted the existing social system of relationships arranged around the dinner table, but in a way that carried the noise to neighbouring homes. In doing so, it effectively re-organized how others experience and expect digital privacy itself.

Part Four: Conclusion

As evidenced by the efforts and lengths taken to measure electrical interference in communications system, Shannon (1965) theorized that noise is an inescapable characteristic of any system. Shannon's theory was purposed normatively – a response not merely to the study of electrical communication but also a response to the growing perception that 'interference' obfuscated meaning and interaction. Through similar analytical lenses, one might conclude that noisemaking conducted by the routine failures of the *SpiderOak One* software demands refinement. But that set of lenses delineates the kind of normative judgement that this dissertation avoids – the preoccupation with making digital privacy 'better' by strengthening *SpiderOak One*'s encryption protocols, staff-oriented information-access procedures and website data-handling scripts. The point here is to lean into the noise. Make it legible – just as Wiener (1949) set out to accomplish in his early twentieth-century technical study of noise. The goal is

embrace the noises the software creates and to embrace both the otherwise ‘helpful’ and ‘critical’ noises emitted by the users as well for the ways in which they levy themselves as mechanisms and avenues of trust-building between the coders, the software and the users altogether.

Digital privacy via *SpiderOak One* is not merely afforded by multiple layers of advanced encryption that obfuscates any outsiders’ gaze from its users’ personal data. Nor is digital privacy via *SpiderOak One* merely guaranteed as a matter of control or regulation vis-à-vis the company’s ‘No Knowledge’ policy. Digital privacy via *SpiderOak One* is a matter of trust. This matter of trust is reflected as a connection between the three groups of actors whose noisemaking practices and preoccupations constellate a social system around *SpiderOak One*’s technical and networked infrastructure. The system itself is not a stable system. It is characterized by the contingent nature of its social connections, the majority of which are established as much as they are broken down via matters of trust. Matters of trust in the sense of how and whether users believe in the protection *SpiderOak* and *SpiderOak One* provide. This trust is not simply – as aforementioned – a question of using encryption and backing it with a policy. Trust here is conditional, and a question of perspective. There are numerous degrees and extents of technical and political scrutiny waged by the *SpiderOak One*’s users and volunteer programmers.

These actors are embedded in a particularly problematic position because they are burdened by an unusually high level of technological literacy on the one hand and but also compelled by the politics of a corporate policy and Big Data discourse on the other. It is a precarious situation particularly in the sense that users of *SpiderOak One* cannot merely engage the product and its preceding ideology as consumers. While it might be arguable that most politically, socially and technically conscious users of any social media product similarly occupy the rather unenviable position of weighing the industry’s politics against evidence of technical

workings/un-workings, *SpiderOak One* users are unique in the sense that they were drawn towards *SpiderOak* not merely as one of the first cloud services available but as the first to appeal to the ‘most’ politically and technically conscious.

This marketing was also carried out in a particular juxtaposition to the habits of rival social media companies that did not privilege privacy-first approaches to personal information retention. Many of *SpiderOak One*’s users came to *SpiderOak One* to get away from the news events of 2011, as well as the security follies and Big Data impulses of *DropBox*. These developments were not merely catalysts drawing users to *SpiderOak One*, but incentives in the sense that these users encountered a guarantee to anonymity that was particularly unique given the political developments of the time (for example, the hyper-securitized Western political climate propagated by neo-conservatism post 11 September 2001, exacerbated by the already prevalence of the Network-Centric Warfare military doctrine in the United States that demanded information domination across the Internet).

The precarious positions of these users is particularly important for understanding digital privacy in *SpiderOak One* because the notion of privacy itself is never static. It does not have a stable referent to which it points, like a Terms of Use Agreement or ‘No Knowledge’ policy. Although the conceptual stakes here are rather high in arguing that digital privacy is not a stable concept, particularly for literature engaging digital privacy as a matter of government vis-à-vis the institutions of domestic and international law (Westby, 2004; Svantesson, 2015; Dowling, 2009), the subjective basis of how it is experienced from user-to-user is a widely accepted academic belief as evidenced in the second chapter’s discussion of literature within communications studies (Grant and Bennett, 1999; Elmer, 2003; Cavoukian, 1998; Goldberg, 1997), which is due to two reasons.

First, the degree to which digital privacy is provided is a reflection of whether or not its users investigate or are made privy of particular technical and political issues. Some users entrust *SpiderOak One* enough to amend its capacities to extend its encryption protocols for special hardware, while other users encountered random errors that suspended altogether whether or not *SpiderOak One* effectively utilized their encryption protocols altogether. Some users appear to celebrate the efforts and declarations of *SpiderOak One*, particularly for the ways in which they produce transparency reports and openly challenge state surveillance and legal demands for users' personal information, while others have become frustrated with the lack of move to a fully open-source platform along with the continuing trend of software issues (by means of routine server disconnects) that have been persisting for years on end.

Secondly, each of these experiences demonstrate that there are numerous different options in terms of management choices users have for choosing who and where their personal information is handled on the one hand but also what they need to do to ensure it is protected on the other hand. The point is not merely that each new category of management reminds our analysis that digital privacy is indeed a subjective experience. The point is also that each subjective experience is located at the site and politics of data management, which is highly delineated by numerous complex social relations enabling that site as a research subject altogether; the site of analysis is not merely technical, but social through and through.

As a socio-technical system, our analysis must take into account how these social relations translate into social flows and influences that are noisemaking activities on their own terms – infections that encourage the further development of *SpiderOak One* as much as they conversely encourage the development of what we might otherwise dismiss as 'competing' profit-first services. As discussed throughout the chapter, there is discernible empirical evidence

that users are *returning* to the realm of Big Data and cheaply deployed encryption. They are returning to the domain of haphazard privacy promises from social media companies like *DropBox* because *SpiderOak One* continues to be challenged by the most technologically literate of cloud services users across the Internet. As these users move towards more accessible, faster and more reliable cloud service products, their move signifies a troubling prospect for thinking about, with and through digital privacy as a matter of both technical and social development.

These users straddle completely different conceptual territories about digital privacy, and in this case, such developments ought to be celebrated analytically as such. *SpiderOak One*'s users' personal information may never be empirically resolvable in terms of who manages that information and where that information resides. The security status of their personal information, so to speak, is never certain; while they understand entirely that *DropBox* does not privilege users' privacy, *SpiderOak One* users who have returned to *DropBox* are also using *SpiderOak One* for smaller files and on a less frequent basis. But the point is to engage this lack of certainty as a conceptual opportunity to open-up an entirely different horizon for understanding digital privacy itself. An alternative understanding here implies that digital privacy on *SpiderOak One* is invariably bound to the politics and influence of the Big Data industry on the one hand, but also upon the creativity and decision-making of users on the other hand – the lattermost of which tends not to be taken into consideration when thinking about the 'who' and 'what' of personal information regulation and control by most digital privacy literature today.

The economic competition between privacy-first and profit-first file hosting services is a productive analytical tension. This tension instructs that for *SpiderOak One* users, understanding digital privacy depends upon abridged and abridging experiences. Digital privacy is as much a reflection of the hands of *SpiderOak One* users as it is a reflection of their minds. Whether using

DropBox, SpiderOak One or both together, the impetus is very clear: cloud services and digital privacy most certainly do not provide the ‘ease of access’ and benefits of cloud storage that initially spawned this industry in the late 2000s.

Chapter Six: Case Study Comparison

This chapter compares and contrasts the three case studies on Tor, *WhatsApp* and *SpiderOak One*. The goal of the chapter is to determine why each case study is different, particularly in terms of how digital privacy ought to be understood differently than a matter of regulation and control on the behalf of governments and corporations. It serves as a summary of particular points of comparison and contrast as well – of noises emitted by all users, coders and software systems, of the shape, behaviour and momentum of each respective and corresponding socio-technical system thereof and finally of the differences and similarities in the kinds of digital privacy each socio-technical system reflects and engenders. Accordingly, the chapter is structured into three parts: noises; socio-technical systems; digital privacy.

Noises

Users

Across all case studies, users clearly act upon their own volition, impulses and ideas to enhance their own privacy. Despite some Privacy Studies scholarship implies otherwise, users are not docile. Users are not merely subjects of digital privacy, nor are they merely subjects of corporate policies, encryption algorithms and political rhetoric as such as some of the computer sciences literature reviewed in the second chapter implied. Each case study is thus similar in the sense that there is ample evidence of users at least attempting to be actively engaged in the conditions, processes and outcomes of digital privacy. One of the most consistent features of Serres' (1982) *Parasite* is that each literary example explored across each chapter offers differentiated logical orderings about the extents of the agential capacity of each individual

noisemaker. And as the case studies, demonstrate each noisemaker faces different challenges and conditions upon which their noises are mounted, projected and received.

In the case of Tor, three different varieties of preoccupation and interest made it rather discernible that users directly manipulated Tor to make it stronger (by adding plug-ins to the browser and even changing their behaviour to blend-in to Tor's encrypted streams more effectively). While there is one discernible body of users using Tor to merely browse the World Wide Web, an opposing body manipulates Tor to conceal its illegal activity (World Wide Web versus '.onion' sites, for example). Each user group thus has different destinations online. But the differences in their destinations are partially motivated by the extent to which users can effectively tweak or modulate Tor to support their desire to reach their respective destinations. Recalling that, for example, the 'green onion slider' plays an intimate role in constraining or liberating website access, how and whether the World Wide Web is experienced is rather different than how '.onion' websites are experienced. And so while it is indeed the case that the software gently encourages all of its users to engage the 'deep web' as opposed to the World Wide Web, users have – since the software's onset – needed to adapt and decide as to how Tor would be used in order to browse the Internet.

The third user group of Tor, those that tended to break Tor accidentally by not being aware of the fact (or even intentionally disregarding the fact) that Tor cannot, for example, encrypt P2P file transfers (.zip and .rar), emit a different kind of noise. Their noise was merely 'using the software' because they *believed* the software would do its job, so to speak – despite the fact that many of their activities undermined Tor's capabilities. It is an accidental noise, a reverberation of their actions that invariably but intimately affects their own and other users' digital privacy. The consequence of their behaviour on a software system that cannot support

their browsing activities is catalyzed by the fact that the majority of Tor's traffic uses Tor like they would any other Internet browser.

One of the most important consequences of this third modality of noisemaking is that it not only undermines the technical capacity of Tor itself, but it also encourages like-behaviour from the other user groups. Their noise encourages like-noise productions by new and existing users (again, via P2P, for example) with little understanding of what they are doing. The case study also evidenced that there tends to be a blatant disregard or care of the fact that 'digital privacy' in a technical sense is not 'working'. This reckless behaviour is founded upon the belief that digital privacy 'just happens' because one simply uses the software. This phenomenon is only found in the case of Tor, and it is particularly unique because it is the only example that evidences the way in which an over-abundance of careless noisemaking begins to choke or constrain neighbouring noise emissions from within the same user group. As Schneier (2016) theorized, too much noise production in terms of information density and volume flow tends to bottleneck the efficiency of communication. While he was referring to more technical and literal information flows in terms of the production of too much excess data (as in Big Data, for example), his point translates metaphorically here in the sense that the legal usership on Tor that tends to stand out and apart from illegal flows is pressured to be subsumed at the risk of being choked out of privacy protection from Tor itself.

Noise producing practices by users that seek to enhance digital privacy are mirrored across *WhatsApp* and *SpiderOak One* as well. The first two categories of noise-emitting behaviour on Tor are similarly located on *WhatsApp*. The Biomedical Research study presented in the second case study demonstrated that more introverted personality types on *WhatsApp* are far more likely to hesitate in what they were saying, which is argued to represent a noise in the

sense that the subject filters or self-screens what information is shared on the network before it enters the network whatsoever. The case of *SpiderOak One* is similar in the sense that users who actively prodded and poked the software to test its vulnerabilities to enhance and extend how and what personal information would/could be protected. A crucial difference between *WhatsApp* and *SpiderOak One* users, in terms of emitting noise in the name of their own privacy, is that the latter are far more technologically literate than the former.

There is also a considerable and rather discernible level of technologically literate users amongst the more illegal traffic flows on Tor. The illegal flows on Tor require a certain knowledge of the addresses, procedures and behaviours required in order to access the ‘deep web’, and the majority of Tor’s traffic is indeed located ‘under’ the World Wide Web so to speak. The most significant observation to be made about ‘users’ noise making behaviours across the three case studies is thus that Tor and *SpiderOak One* levy *more* opportunity for users to make noise; *WhatsApp* users indeed make noise but rather in a sense that undermines privacy directly. The majority of noisemaking on *WhatsApp* was cultivated by the noise the software and its coders produced – noises that encouraged users to infringe upon other users’ privacy directly.

Coders

In terms of the noises coders make, there are notable differences but even more significant consistencies and similarities across the case studies that are rather problematic for each respective unfolding of digital privacy. The most straightforward way of articulating these issues is by calling attention to the tension between privacy and profit. This tension precedes, and as such preconditions, each case study considered. And so one of the most common feature across each case study is, on the one hand, the need to promote privacy products in the Age of

Information where Big Data dominates capital endeavours. On the other hand, the notion of privacy online generally infers closure, preclusion of access and accountability in terms of the circulation of any information collected about how people engage social media software. Privacy itself, simply speaking, is its own hindrance to privacy software. Although Serres himself had a blatant disregard for individual privacy (1982, 142-4), calling it the selfish act of withholding information, goods and ideas from the public, does signify the problematic nature of privacy itself. And so while it is the case that privacy is a counter-intuitive capitalist logic, it is also the case that any noisemaking in the name of digital privacy will ruffle the feathers of most any neighbouring actor, relationship or institution. This is precisely what each study reveals.

All noisemaking by any actor is problematic. But this is particularly the case for coders – disproportionately. Coders with *Tor*, *WhatsApp* and *SpiderOak* thus occupy similar space when it comes to the promotion of their products, thus serving as their own source of constraint upon the effectiveness of their noisemaking. While they all have vested interests in promoting their products as ‘privacy-oriented’, another similarity converges at a specific point of tension: marketing ‘privacy’ conflicts with ‘marketing’ in general. This is specifically because all three case studies are examples of software that are subject to social demands and expectations over ease-of-use, accessibility and reliability. As discussed in the example of *Tor*, for example, development of a reliable anonymity onion routing protocol depends upon strength-in-numbers – the larger the number of users, the larger the number of volunteer nodes required. And so, while *Tor*’s coders promoted a product that was a world leader in anonymous communication and web browsing, a reality of the growth of volunteer nodes stagnated while user-ship increased. Their response to the problem was to make *Tor* more ‘user-friendly’ and more ‘attractive’ aesthetically. The consequence was a social engineering of ‘how to’ experience the Internet in

contradictions – to use Tor to be anonymous, but only if a user is willing to abstain from the vast majority of sites available on the World Wide Web, for example. The noise began as a message to trust the product and browse liberally.

This is no different on *WhatsApp* whose coders marketed aggressively after the *Facebook* buyout (and with the assistance of *Open Whisper Systems*), encouraging users that *WhatsApp* prevented anyone at the company (including anyone, worldwide) from seeing the content of users' messages. *SpiderOak*'s coders did not and do not deviate from this noisemaking activity either; the combination of the layered encryption protocols and backed by the consistent advertising of their 'No Knowledge' policy suggests to users that the product prevents and precludes information access.

The final commonality amongst the case studies' coders' noisemaking is that all of their noises actively undermine how digital privacy unfolds. They generally implicated users' experiences, and encouraged behaviours that rearticulate the prerequisites of digital privacy in a way that is generally incompatible with all of the companies' images of secure data protection. Tor's coders emitted a noise that encouraged most of its users to use Tor in a way that accidentally precluded its encryption protocols from working, while precluding access to the majority of the World Wide Web at the cost of encouraging access to the 'deep web' (where most casual users that Tor markets to, such as journalists and academics, tend not to require access). *WhatsApp*'s coders' noisemaking played a particularly curious role in falsely reassuring its users that no one can access their data. While it is indeed the case that content information cannot be viewed, meta-data is clearly harvested. So much so that users themselves are increasingly socializing into an interactive experience whereby meta-data indicators are engendering social behaviours that undermine privacy expectations and norms *between* users.

SpiderOak One's coders noisemaking have been remarkably consistent. In fact, they have not changed in a decade: 'we have the best encryption protocols available, and we – by mandate – cannot and will not look at your personal data'. The consistency of their noise emission resulted in the cultivation of user behaviour that, rather ironically, deflected back towards the coders. Users developed behavior that sought to scrutinize *SpiderOak One* in a way that undermined the integrity and value of the product as much as it assists. While it could be argued that critical examination of a product by its consumers can be utilized to improve a product, there is an absence of empirical evidence that *SpiderOak* acknowledged many of the issues its users located. The overarching point of significance in terms of similarity then between the sets of coders across each case study is that their noisemaking attempted to encourage digital privacy, but in a way that was out of tune with users' values. Coder noise was a catalyst for the amplification of user noise.

Software

One of the largest consistencies in terms of noises emitted between the different software systems studied is the distancing effect created by the software itself. Granted that the notion of an object having agency unto itself is a rather alien logic to privacy studies, the logic is actually advanced by a pupil of Serres: Latour (2007). Actor-Network Theory flattens the ontological playing field, so to speak, between users, coders and the software. The largest implication of doing so is that the network of possible relations between each actor is given equal analytical and conceptual attention. In the case studies reviewed, we see that objects – like Shapin's (2010) account of Hooke and Boyle's air pump – have the power to compel social actors to re-assess how they relate to their spaces and places around them. How people draw lines, how they

see/understand points of slippage/blurring between private and public spheres, is indeed a matter of object-life as much as it is a matter of human-life. These case studies demonstrate that each software plays a fundamental role in manipulating users' and coders' sense of proximity – not only from the software itself, but also from other coders and users.

There is indeed a theme of continuity in terms of the way in which the software manipulates proximity and intimacy with the user. In the case of Tor and *WhatsApp*, for example, they both exhibit aesthetic qualities that encourage users to engage software and use it liberally. Tor is designed to 'look' and 'feel' like anything but itself; modelling the interactive experience after *Firefox* encourages a kind of usage for the user that precludes hesitation and interruption from the user as she browses the Internet whereas *WhatsApp* similarly replicates the experience of instant messaging, which is dovetailed by meta-data indicators that also encourage users to be accountable to themselves and one another in the name of producing not only consistent interaction but a consistent expectation of said interaction as well. This distance manipulating effect, of drawing users in to the software as intimately as possible, is characterized by the social and political consequences of that drawing-in. The aesthetical qualities of both Tor and *WhatsApp* conversely generate a separation between users from the software's coders as well as from other users.

In the case of Tor, the standardization of the browsing experience inherently creates a two-tiered browsing trend whereby users using Tor legally are more susceptible to external traffic monitoring attacks; there is an implicit encouragement for standard World Wide Web users to use the Dark Web more so as to blend in with illegal browsing and file exchange activity that. This encouragement to change browsing atmospheres, in turn, generates a more comprehensive and robust ability to 'hide' from external traffic monitoring attacks. The point is,

rather simply, that using Tor to browse the Internet ‘as usual’ – despite the fact that it is designed for precisely that purpose – places the onus on the user to determine what kind of privacy she expects and desires whereby a change in behaviour is virtually mandatory. How users engage and behave on Tor is shifting dramatically, and in such a way that is challenging coders in terms of facilitating a universal and standardized ‘safe browsing experience’ on the one hand, while having to reconcile not only the needs of various user groups but also the changes in their browsing behaviour as well.

The consequence of *WhatsApp* drawing users in, so much so that a social trend of borderline obsessive usage seems to proliferate exponentially year over year, is that users are being drawn closer in terms of intimate conversation with one another. The ‘look’ and ‘feel’ of instant messaging, wedded to visual indicators of when users were last seen, last responded and the average time it takes for them to respond, engenders a systemic and internal realm of privacy violations amongst users. Whether this intended by the coders is an issue that is trumped by the observation that continuous user interaction ubiquitously produces more meta-data — data that is a marketing trove for *Facebook*.

Upon first glance at empirical evidence, *SpiderOak One* seems to create a significant distance between itself and the users, as well as the coders and the users. It is problem-laden from the onset. The gaps set in by that distance, so to speak – gaps in usage, gaps in expectation, gaps in trust. But in the space of those gaps is also a time – create a prolonged waiting time between users and their ability to access their hosted information. In those gaps of time and space *SpiderOak One* users learned to reverse-engineer the software. They learned to find more vulnerabilities. They learned to take their findings elsewhere, and mobilize them as aides in the creation of a stronger, more reliable digital privacy. While it could very well be the case that the

problems the users found may have closed the gaps, so to speak, by fixing issues the users found in the software. Alas, *SpiderOak One*'s coders never came around to addressing these issues in their severity. And so, to most users – even today – the issues persist and as such, the gaps and distancing persist as well. Curiously enough, the outcome is still a relatively positive a re-ignition for users because they are encouraged to re-relate and re-prioritize their own personal information. Accordingly, we as analysts utilize the distancing effects created by the software's shortcomings as an analytical opportunity to critically re-articulate how we understand the mechanisms driving digital privacy itself.

While most cloud services products are designed with intuitive usage and efficiency in mind, *SpiderOak One* deviates in the sense that there is not only a learning behind the software itself but there was also (for some time) a lack of visual indicator about whether or not files were successfully synced and a solid connection was maintained. The distancing effect of the software as such is the opposite of the previous software mentioned – the software alienated a significant number of users, creating tension in the usage experience that in turn placed onus on users to build their own regimes of problem solving, verification and information security. One of the most significant differences between *SpiderOak One* and the other software is thus the inescapably challenging position of pushing users to critically reassess how they related to their own personal information. Many users were positioned in such a way that they went back to other more mainstream cloud services products that were far less privacy-oriented, which dramatically alters users experience and expectation of digital privacy itself.

Socio-Technical Systems

As articulated in Pinch, Bijker and Hughes' seminal work (1993) on socio-technical systems, analyzing technological systems as inescapably and fundamentally related to the social life forces around them provides fruitful conceptual and theoretical outcomes in terms of understanding the 'how' and 'what' of the objects we analyze. What their work also contributes is a way of understanding how the outcome or output of technological systems is as much a matter of technological purpose as it is about human contingency, resistance and desire. Moreover, avoiding the conceptual impulse to 'see' each case study as merely 'a matter of regulation and control' by its designers, we as analysts strive to understand digital privacy beyond merely technical processes of binaries, computation and electricity. The technical *is* social, and vice-versa – through and through (Flanigan, Flanigan and Flanigan, 2010, 179-180). Theoretically speaking, socio-technical systems are thus social in terms of the social activities the dissertation refers to as 'noisemaking'. To Serres, any social activity produces noise – noise that infects or parasites neighbour social relations (1982, vii). But as Adler and Kretschmar (1991) iterate, and as echoed by Serres himself (1982, 114): parasites keep systems alive, for better or for worse. And how each system lives, for better or for worse, provides key analytical inside and novel conceptual opportunity to re-discover who and what constitutes digital privacy itself.

In the case of Tor, the first noises made came from the US Naval Research Lab and soon thereafter from DARPA. Tor was not preordained as a public communications and web browsing technology whatsoever. It was designed as a military communications technology. Tor's release to the public sector is thus fraught with the inescapable politics of using the system simultaneously to protect users from government surveillance while also enabling government

surveillance. Both modalities of usage cannot be separated from one another. This is a particularly important design dynamic of Tor as a digital privacy system because of the way it influences the kind of social relations users established amongst themselves and to Tor itself. Tor was and is marketed for World Wide Web usage. But usage on the World Wide Web is most susceptible to external traffic monitoring analysis attacks. What the case study revealed is that users were compelled to decide how much of the World Wide Web they desired to access, and whether or not they ought to shift their priorities to accommodate the differences in content that exist across both domains of the ‘Internet’ (so to speak); Tor on the World Wide Web is far less secure than Tor on the ‘deep web’. What is particularly significant then about the noisemaking process coming from the coders themselves – from the onset of Tor – is how it affected users’ relation to Tor on the one hand but also other users on the other. Users were initially encouraged to use Tor liberally, freely and openly – in any manner that would suit users’ browsing expectations. After Tor began experiencing issues in its size and function, the coders shifted the tone of their noise to encourage users to browse uniformly.

The tension therein is that uniform browsing behaviour is not self-evident to users, nor is the idea that browsing behaviour could be imagined as something like a ‘norm’. The technology enables access to two completely different realms of ‘Internet’ access. Each realm embodies very different kinds of browsing behaviour, and as such, very different concentrations and dimensions of routed, packaged data flow. The largest data flow, or the noisiest concentration of encrypted information across Tor, is found in illegal activity on the deep web. In order to use Tor effectively, users need to be aware of this dimension on the one hand, and then engage it on the other – the decision to do so directly compromising how the Internet can be accessed altogether. As a socio-technical system, Tor is a reliable privacy system for only a certain modality of

browsing experience and expectation, which in turn directly affects what kind of digital privacy its users not only experience but come to expect.

WhatsApp, on the other hand, striates and organizes its social relations more linearly, thus having dramatically different implications for *WhatsApp* as a socio-technical system. Because *WhatsApp* came together through social and political controversies (the trend of rather discernible dishonesty by the history of its ownership that has played a direct role in attracting different kinds of users), there was a similar noisemaking process by its coders to Tor in the sense that *WhatsApp* was marketed as a private, safe product. But where it differs tremendously is in the nefariousness behind those noises. Regardless of statements regarding privacy and the inability for *Facebook* to access data content shared between users, *what* was being encrypted was falsely marketed as the most important dimension of information protection. Meta-data is not encrypted, and leaves users susceptible to intense marketing analysis and subsequent advertising in the app.

Subsequently, the system took social shape due to users increasingly relying upon a false sense of privacy. The app exploded in popularity worldwide, and as the case study discussed, many users engaged *WhatsApp* because they felt as though it was the most private, free and globally-connected instant messaging service. And so one of the most salient differences between Tor and *WhatsApp* is the concentration and magnitude of its information flows. Tor is characterized by diffuse, decentralized information flows – and its content, regardless of the difference in content or meta data – is all encrypted. *WhatsApp* connects millions upon millions of individuals across the globe and *only* encrypts the content of their messages – a perversion so to speak and at the very least a radical departure from even computer scientists themselves who

are vested in leading the charge in theorizing the application of advanced cryptographic protocols (Acquisti, 2007; Bodo, 2014; Marcella, 2003).

Unlike Tor, the location and destination of those data flows – as well as the personal information about who those users are – is disclosed to *Facebook*. There is a socialization process in and around these technical dimensions that are particularly significant because the trust the noisemaking process emanating from the coders normalizes intimate interactions. Because users were told that ‘their’ personal information is *the* most important dimension of privacy according to *Facebook* and *WhatsApp*, users tend not to be aware of the extents of the *meta data* mining taking place. These implications are particularly significant for two reasons. The first is that users are increasingly susceptible to advertisements crafted on an individual basis depending upon their messaging behaviour. Secondly, and accordingly, how users came to interact with one another reflects the meta data visualizations displayed in *WhatsApp* itself. These meta data visualization mechanisms catalyzed the emergence of an entirely different realm of privacy as well as an entirely different realm of privacy concerns therein.

Unlike Tor, *WhatsApp* as a socio-technical system is relatively well insulated from external surveillance and hacking attempts, but marketing and mining of the internal flows takes advantage of the increasing frequency of privacy violations between users who are (as numerous studies demonstrated in the case study) holding one another accountable to the timing and frequency of their interactions. But the noises emitted by the software upon the users of each system are different in a specific sense. While both systems’ own software-oriented noisemaking is the same in the sense that their aesthetic dimensions draw users in to encourage liberal, intimate and familiar experiences, *WhatsApp*’s software encourages most of its users to interact more often and frequently than Tor’s. Tor is dramatically different in the sense that its

noisemaking is designed to mimic *Firefox* – it encourages users to browse openly. For those that do browse openly, particularly on the World Wide Web, users are at higher risk of traffic analysis hacks because they constitute the minority of Tor’s traffic flows. For users aware of this process, they can engineer the software to enable higher security – but only to the extent that the majority of the World Wide Web becomes unusable. The software’s noise is thus notably different from *WhatsApp* in the sense that it implicitly punishes users for *not* using Tor on the deep web, whereas *WhatsApp*’s noise implicitly encourages users to browse the same way.

Perhaps the largest overarching difference between the two systems then is in the way in which the noise from *WhatsApp*’s software dovetails and reinforces the noise from the coders in a way that coalesces for mutual benefit: privacy is not the priority, mining excessive usage is. Tor’s coders noisemaking encourages uniform behaviour because its software encourages users to browse just as they would on any popular browsing technology.

SpiderOak One is similar to *WhatsApp* in the sense that it came together via tensions and controversies, but different in the sense that those tensions and controversies were external to itself. *SpiderOak One* came together in juxtaposition to more popular, mainstream cloud services products in general but in contrast to *DropBox* in particular. The majority *SpiderOak One* users were initially attracted by its privacy-first orientation, but thereafter because of the wider security issues of 2011 as well as the privacy issues surrounding *DropBox* in 2012. The noise the coders emitted into the system attracted users before the controversies of 2011 and 2012, and rather acutely so thereafter. As a socio-technical system, *SpiderOak One* is significantly different than *WhatsApp* and Tor in the sense that it attracted a very specific kind of user. The technological literacy, and the approach to developing a software cross-compatible with non-mainstream PC or

Mac based products meant that *SpiderOak One* receives a disproportionate expectation from its users about the calibre and reliability of encryption the service and software provide.

Another significant difference from the other two case studies however is that the noise the coders emitted only coalesced with the noise the software emitted, and only for a time. Despite the software being rather unorthodox in aesthetical representation, it did provide a sense or idea to the user about where files were sent and some insight into their status. But over time, the noise of the software intensified in terms of its affect upon users. Users began investigating the software and the company itself. In some cases, it levied new opportunity to reconstitute noises, for further coalescing. The evidence of which is yet to be seen; the ‘No Knowledge’ policy is vulnerable to practical and technical limitations of the encryption process itself, as too is the lack of open-ness (so to speak) with regards to the company’s release of *SpiderOak One* in its entirety to the public domain.

But perhaps most significantly, there are two differences that set *SpiderOak One* apart from the other two systems. The first is that users, as a result of the coders’ and the software’s noises bifurcating, are compelled to adopt other cloud services which dramatically changes their relationship to their own data. Because *SpiderOak One* often disconnects and leaves files in synchronization limbo, there appears to be a trend where users are using other cloud services products in tandem with *SpiderOak One*. While this presents a unique file management strategy, it sets *SpiderOak One* apart from *WhatsApp* and *Tor* in the sense that it is the only entity studied that leans upon the existence of other competing services in order for its users to feel fulfilled. Of particular interest is evidence of former *SpiderOak One* users finding ways to make profit-first products more private – experience translated into a social expectation for privacy where it is not usually suspected let alone believed to exist. And so it follows, secondly, that *SpiderOak One*’s

users never engage *SpiderOak One* as a socio-technical system exclusively. The noise *SpiderOak One* users emit into the system is unique in the sense that they play intimate roles in making very legible the limitations of *SpiderOak One*. In doing so, their noise charted the edges of the system thus making the ability for users to carry forward their noises into neighbouring systems. As a socio-technical system, *SpiderOak One* truly stands apart from the rest in the sense its user-ship uniquely influences the outcome of a bottom-up vision and realization of digital privacy in neighbouring socio-technical systems.

Digital Privacy

Digital privacy is not merely a matter of regulation and control by social media owners and coders. It is not also a reflection of merely ‘software’ doing what it was ‘programmed’ to do. Digital privacy is a reflection of the kinds of relationships and behaviours exhibited by networks of social relations in and amongst technical processes. And those technical processes need not function perfectly. As Serres argues, stations and paths formulate lines upon which messages are transmitted and delivered: “points and lines, beings and relations. What is [most] interesting is its construction... A system has flow, but it also has accidents, such as changes and metamorphoses... Difference and concept, difference and design, produces things together. The origin of things is difference” (Serres, 1982, 13). ‘Systems work because they do not’ is the message Serres contributes to privacy analysis. And by shifting our analytical expectations and empirical starting points, we begin attending to the way in which digital privacy unfolds imperfectly, unusually and contingently. This, above all, is the most important lesson to be taken from the dissertation when it comes to locating alternative understandings of digital privacy across the case studies.

The most significant differences in each understanding of digital privacy are revealed by *how* social activities – what the dissertation identifies as ‘noisemaking’ by the various actors considered – relate to and alter technical processes on the one hand, and simultaneously relate to and alter social relations on the other hand. The consequence is the unique way in which these dimensions of social relations, particularly due to their variegated nature across each case study, generate different networks of behaviour and interaction between coders, software and users. Depending upon how noises coalesce/clash, engender/preclude and liberate/constrain, each system reveals different context of social and political values, lives, rules and norms. By attending to those contexts, we locate different stories about digital privacy. We learn how digital privacy is constituted, prioritized and organized. We learn who and what it includes and excludes. We learn how digital privacy cannot merely be accounted for as a process of encryption, but also a process of social and political developments as a result of noisemaking. Simply speaking, what all of these case studies have in common is the ownership’s declaration that their technical processes provide the best digital privacy available. But this is hardly interesting on its own terms to the dissertation. What is more interesting is what that declaration cannot say: from system to system, digital privacy is never the same.

On Tor, digital privacy is not merely the concealing of a user’s location, destination and content information via an onion routing encryption and data transfer process. It is a highly subjective and individualized experience that varies user to user, and this is because of a very complex web of rules, constraints, norms and values clashing with one another. The majority of this complexity is located in and around the tension between the coders’ and the software systems’ noisemaking. The former has always projected an aggressive message towards current and potential users that Tor is the most reliable and secure anonymity browsing and

communication technology in the world. But that message is contingent upon another message those coders provide users, requesting that they self-regulate their behaviour in order to make up for the system's technical shortcomings.

This tension in-and-of-itself conflicts with the noise the software makes, which encourages users to do to the opposite: to browse the Internet as liberally as they would with any other browsing technology. How people use Tor is, consequently, extremely different. As discussed earlier, some Tor users consistently fail to use the technology in ways that support and operate within the limitations of what kinds of data can actually be encrypted. Some Tor users browse the World Wide Web's most popular websites exclusively, the majority of which consist of a javascript or HTML design that often precludes Tor from functioning altogether or prevents users from actually loading the website.

The majority of Tor users browse the deep web and/or conduct illegal activity, which leaves legitimate browsing activities susceptible to traffic analysis attacks because their traffic flows on the 'cusp' or 'edge' of mainstream data flows. All of these differences instruct us that there is a correlation between the tensions in the noises projected upon users, so much so that a variety of browsing behaviours proliferate – behaviours that indicate that only *some* data, *some* flows, *some* destinations, *some* locations are better protected than others. The conditions upon which that level of protection is afforded is largely up to the user and her preferences, browsing behaviour and her expectations as deciding factors. Digital privacy on Tor is not guaranteed, nor is it a priority of the software itself. Its history and its tensions reveal to us that usability, marketability, ease of use/access and efficiency are prioritized much higher than providing a universalized, non-discriminatory basis of coverage for users.

WhatsApp is radically different, and not because it uses a different kind of encryption process. It is different because of the kinds of socio-political implications emerging in and around coding values. *WhatsApp* uses an End-to-End encryption process that hides the content of instant messages sent between users. The encryption process is marketed towards users as the most reliably guarantee of privacy available on such a platform found anywhere in the world. But *what* is being protected is merely a distraction from what is *not* being protected. What is marketed towards users is a value or belief that their messages are the ‘most’ private information that ought to be protected. As discussed earlier, it is a manipulation of the concept of privacy itself. *WhatsApp* pitches the idea to users that surveillance and monitoring from outside the app is the *most* invasive and *most* dangerous realm of privacy invasions. In 2016, Sir David Omand – former Director of the UK’s Government Communications Headquarters – argued that the increase in ‘terrorist’ presence across the Internet is akin to an explosion of ‘noise’ confusing and strangling social media networks. Omand concluded publicly for *WIRED Magazine* that in order to prevent terrorism activity, an increase in surveillance was the only way forward.

Just like the way in which Omand postures ‘terrorists’ online as noisemakers, *WhatsApp* in turn frames governmental surveillance as ‘bad’ noise to the wider *WhatsApp* network. Simply put, the call for greater encryption to ‘keep noise out’ postures *WhatsApp* to make its own noise. The noise the coders emit here manifests in the form of fearmongering. The intentional framing of external surveillance as an intrusion upon users’ privacy also levies itself as a means of creating docility amongst its user-ship. What *WhatsApp* is essentially portraying for their users is that the encryption process not only protects the content of users’ messages from external gaze, it also prevents *WhatsApp*’s own gaze upon content as well. Alas *WhatsApp* deploys does *not* protect hide meta data from *Facebook*.

Meta data is not only absent from any discussion or declaration about privacy values by *Facebook*, it is not generally understood by users as a priority or concern whatsoever. The impetus is very simple. *Facebook*'s aggressive behavioural mining about users' behaviour on *WhatsApp* levies numerous avenues for behavioural manipulation (which, as discussed, is not unusual for *Facebook*) and novel modalities of product placement and marketing that invites third parties into users' inboxes. Moreover, the meta data is cross-referenced with personal data collected on *Facebook* anyhow, which furthers *Facebook*'s capacity to mine users' interactions.

But these observations about manipulation and deception over what is and what is not protected by the encryption mechanism barely scratch the surface of the most significant difference between digital privacy on Tor and *WhatsApp*. Because of the way in which the encryption process precludes *any* third party from not only seeing but interacting with users, *Facebook* has a monopoly over adjusting the conditions and dimensions of how users interact with one another. As evidenced by the meta data visualization mechanisms ('last seen' time stamp, as one example), *Facebook* directly creates and controls the conditions through which any notion of social accountability between users unfolds. The promise to abstain from seeing personal information insulates users from fear of monitoring or intervention, so much so that the instant messaging process 'feels' liberal. Another way of putting this, rather simply, is that many users tend to feel as though they govern one another in terms of the nature of their communicative relationships. If a user does not respond or takes too long to respond, users have the choice of acting upon a new dimension of fear that supersedes fears experienced by users on Tor: Is anyone else watching? What can they see? How do I protect myself?

Facebook gives rise to an entirely different realm of digital privacy on the one hand, but also an entirely different realm of digital privacy violations – and inextricably so – on the other.

Digital privacy could not ‘possibly’ be a concern over the corporation ‘seeing’ users’ messages – that much has been promised. Digital privacy on *WhatsApp* is *as much* about users encroaching upon one another’s spaces and expectations of interaction instead. By not responding, or taking too long to respond, the research studies discussed in the *WhatsApp* chapter reveal that there is a proliferation of anxious social behaviour across *WhatsApp* that challenges *where* we locate conditions and spaces upon which digital privacy can be founded – between users, not merely between *Facebook* and users. On Tor, many users take it upon themselves to blend-in with different usage flows and areas of browsing so as to extend and enhance their expectation and experience of digital privacy, whereas on *WhatsApp* users are more isolated in their decision making and do not have the option to merely alter where they send messages, where they are routed and whether or not they are data mined.

Digital privacy on *WhatsApp* is similar to Tor in the sense that digital privacy ‘as usual’ is not the priority of its design. Ease of use, accessibility and efficiency are the priority for the latter, while ease of mining and encouragement of the volume and frequency of interaction between users is the priority for the former. Perhaps most significantly, where we find digital privacy as researchers across both case studies occupy very different social and political spaces of interaction. Tor concerns *which* data flows are most protected versus *which* data flows are most vulnerable to external traffic monitoring attacks, while a close study of *WhatsApp* concerns *which* behaviours are encouraged to make users accountable towards one another versus *which* behaviours recoil from usage and interaction as a result.

Digital privacy on *SpiderOak One* is significantly different from the other case studies particularly in the sense that users have the onus placed upon themselves to decide which personal information is most important and most worthy of protection on *SpiderOak One*, not

merely because of their content but because of their size. Digital privacy is also different from the other case studies because users are compelled to split their expectations and experiences of digital privacy across multiple platforms to provide one purpose, which splits said expectations and experiences across domains of corporate management that value privacy and profit rather differently. A significant difference from *WhatsApp* and Tor is thusly centered around the disproportionate implications of user-oriented noise. Unlike the other two case studies, *SpiderOak One* empowered users from its onset not merely because it was juxtaposed to other services, but that its user-ship was and is far more technologically literate. The noises the coders emitted upon potential users from the time of the software's release was to seek out privacy-first oriented users. The noise emitted into the marketplace was that the coders were designing a product that could be used on operating systems that are premised on high extents of user control and data management transparency.

The consequence of which is that users' noises had a rather differentiated degree of affect upon the outcomes of *SpiderOak One* as a socio-technical system, which in turn affects how we understand digital privacy therein. After the controversies of 2011 and 2012, user-oriented noise emissions amplified significantly. Although Westerkamp (1988) argued that the purposeful introduction of disruptive noise fundamentally constrains how people relate to their environments, we see the inversion of the logic here – much like the way in which John Cage opened the doors to his concert hall (Attali, 1997) – *SpiderOak One* users emitted their own disruptive noisemaking capacities in an attempt to force significant and meaningful change in *SpiderOak One*. After nearly six years of noisemaking from coders who promised to be a privacy-first company with privacy-first encryption standards, users took the onus upon themselves to investigate the extents of these promises and priorities. The outcome was the

location of numerous issues with the encryption not protecting information exchanged via the website and mobile app, as well as issues with the software indexing files on the server in a way that undermined its own encryption protocol. Combined with numerous issues with the software itself, many users quickly recognized that the onus must be taken upon themselves to determine the extents of their digital privacy via *SpiderOak One*. And so one of the most fundamental differences from the other case studies is that *SpiderOak One* compels users to re-assess their own value system around which information would be protected. This is not merely a concern over content data.

Tor and *WhatsApp* exhibit rather discernibly the extents to which users are concerned with what is ‘inside’ the messages and content they are exchanging and circulating between one another and across the Internet. *SpiderOak One* on the other hand positions users to reassess the value of their data in terms of its size. Because of the inability for *SpiderOak One* to consistently demonstrate reliable protection mechanisms, combined with the nature of frequent disconnections and other related software shortcomings, there is evidence of users developing file hosting behaviour that is premised upon whether or not the files would successfully synchronize – an issue surrounding the size of files itself. The larger the file, the longer the uploading time, the higher potential for issue therein. Digital privacy on *SpiderOak One* is as much a question of trust and transparency with the company not merely because of suspicion of lies and deceit, but perhaps of the technical inability to meet the disproportionately higher demands and expectations of its user-ship.

But the differences in digital privacy here from the other case studies extends into further, more deeply implicating considerations. Unlike Tor users and *WhatsApp* users who tend to use those softwares and services exclusively to find digital privacy, many *SpiderOak One* users are

compelled to split the protection of their data across different platforms. This is particularly significant because there is evidence of users needing to retract and go back to profit-first cloud service solutions, such as *DropBox*. This is significantly different from the other case studies for two reasons.

First, *SpiderOak One* users are forced to re-visit their own values and priorities over data protection across distinctly juxtaposed domains of corporate priority. *SpiderOak One* is not data mining oriented, but the wedding of its unreliability and potentially broken encryption protocols positions *SpiderOak One* users to re-assess how they can split file hosting and file hosting privacy simultaneously on products and services that are conversely profit-first. Many users, as discussed in the corresponding chapter, investigated alternative methods for protecting their personal information on *DropBox* much in the way they had tried with *SpiderOak One*, which leads to point two.

The second significant difference is that our understanding of digital privacy on *SpiderOak One* cannot be contextualized *without* its relation and tension with mainstream services. This context does not merely begin with the noises the coders emitted from the service's onset in 2007, nor does it simply surround the controversies of 2011 and 2012. It *also* includes the way in which the lineage of these socio-political trends amplified user-oriented noises in a way that is cross-influencing the unfoldings and dimensions of digital privacy elsewhere. One of the most significant differences of *SpiderOak One* as a socio-technical system is that its user-ship is abridging socio-technical systems together so as to provide digital privacy, a digital privacy that is founded acutely upon the notion that tension between services plays a central role in not only compelling users to re-assess their own values and understandings of

what 'is' private, but also in compelling users to build their own versions of digital privacy across domains of political life that are inherently juxtaposed to one another.

Chapter Seven: Conclusion

Digital privacy tends to be a matter of regulation and control – of the entry points, movement, visibility, awareness and storage of content data and meta-data. It is governments and corporations that tend to be the purveyors of that regulation and control. What these previous two sentences embody is the prevailing scholastic attitude towards the study of digital privacy. What conventional thinking contributes is a compendium of privacy violations and privacy responses. From hacking, cyberwarfare, state surveillance and relentlessly aggressive data mining, conventional privacy studies scholarship is well equipped to continue constellating threat. It is also well equipped to continue constellating responses. But both of these preoccupations with constellating threat and response operate in institutional level abstractions; the scope and means through which privacy is violated and repaired exists at the level of large-scale actors. This modality of thinking, or what the dissertation has come to identify as conventional thinking, handcuffs critical, theoretical flexibility. Conventional thinking has created its own paradigm of diagnosis and prescription, so much so that it has developed an analytical tunnel vision – one that cannot so easily see beyond itself. Beyond itself are simple questions about *who else* and *what else* is involved in digital privacy in the twenty-first century. If we as analysts loosen our grip over the ontological categories upon which our analytical tendencies are mounted, we begin to wonder once again. We will stop approaching privacy as a matter of regulation and control, and begin embracing privacy as a matter of the *surrender* of regulation and control carried out by an entirely different realm of actors who pursue, negotiate and construct digital privacy on their own terms. The goal of the dissertation is not to abandon conventional thinking; there is crucial ethical and critical merit in pressuring governments and corporations to be responsible about information control. Rather, the goal is to look beyond conventions and inject new theory.

To look beyond, the dissertation calls proposes the development of new ontological lines of inquiry in hopes of developing more compelling theories about the ‘how’ and ‘what’ of digital privacy altogether. This is precisely why the dissertation offers a theoretical framework wedding theories of noise to questions of actors. Noisemaking is the heart of privacy. To purposely or even accidentally emit, interrupt, conceal, protect, obfuscate, confuse and mislead access, inquiry, consideration, thought, movement and theft of any and all content or objects originating from or belonging to another individual or group is to make ‘noise’. Who makes noise is not self-evident, which is precisely why Actor Network Theory is so important to the dissertation. Acknowledging humans and machines as equal actors, occupying the spaces on the ontological horizon diversifies how we as analysts recognize the constitution of spaces, flows and the powers flowing through and around them. Each actor brings into a network of interactions their own presuppositions, values, beliefs and intentions. As they engage networks, they also engage other actors. They build relationships with other actors through negotiating, co-opting, navigating and circumnavigating barriers to their own ideas, values and perceptions of individual and collective privacy. Their interactions shift our conceptual understanding of digital privacy networks from purely literal, technical accounts to socio-technical accounts. Accounts about systems where social processes and technical processes become inextricably bound to one another.

On Tor, we see that users generate all sorts of different kinds of noise based upon who they are, where they are from and where they are heading. We learn that Tor users have different expectations, experiences and visions that they carry into and across Tor. And those differences play an intimate role in how they perceive and react to their environment around them. Part of their environment is conditioned by noises emitted by other actors, such as the coders who promoted the product as safe, reliable and efficient despite its obvious technical shortcomings

and limitations. Their environment is also conditioned by the noise the software emitted, a noise that clashed with noise from the coders. A noise many users interpreted and responded to differently. What we learn overall from this complex array of noise emissions coming from three different sources of actors is that it is impossible to imagine digital privacy as a one-size-fits-all solution. Digital privacy on Tor is not merely a protection guarantee afforded by a large-scale onion routing protocol. It is a matter of contextually specific conditions surrounding different tendencies of different users. And we learn that digital privacy tends to work most efficiently for user groups that Tor was *not* initially designed to support whatsoever.

On *WhatsApp* we see that users are far more constrained in their noisemaking capacity. The intense coalescing of noises between the coders and the software severely restricted not only the conditions through which users could emit their own noise. It also severely restricted the social environment around users themselves. Their environment was prefabricated with aesthetic properties that encouraged users to inquire into the status and response time of other users. These conditions gave rise to a social phenomenon best characterized by paranoia, distrust and loathing. Many users experience the space between their eyes, hands, thoughts and mobile device rather differently due to the acute increase in user inquiry into users' whereabouts. These conditions are ones we learn about through the coalescing of noise between coders and software. A coalescing that instructs analytical re-consideration of precisely *where else* digital privacy unfolds in and around *WhatsApp*. We learn that there is an entirely understudied realm of digital privacy violations on *WhatsApp*, a realm that points towards a kind of digital privacy that entirely escapes the conventional wisdom of 'end-to-end encryption' as forwarded by *Facebook*.

On *SpiderOak One*, we learn about nearly the opposite – of the power of noises coalescing from different users. We learn that the technological literacy primed a different

calibre of noise effect. We learn that users' noise emissions carry the capacity to radically re-deploy the purposes of the software itself – to make the software extend its own encryption protocols to provide information protection to data that was never considered by its designers. We also learn that this same noise also radically re-delineated the limitations of the software and of the coders' influence as well. *SpiderOak One's* has numerous flaws that were only levied as a technical issue once users began informing one another of its potential dangers. These user-oriented noises compelled many to take their experience and expertise elsewhere – towards profit-first platforms that are otherwise avoided by such users altogether. Upon doing so, they reverse-engineered services like *DropBox* to make it 'safer'. They also began splitting which files were stored between both services. These noise emissions chart for us as analysts the unfolding of digital privacy in a radically different way than any of the other case studies. Digital privacy here is a reflection of the critical re-assessment and re-valuing of users' own personal information on the one hand, and a reflection of the splitting of data file locations across juxtaposed software platforms – a move that conventional wisdom might otherwise argue to be counterintuitive to 'true' file protection altogether.

Noise is indeed at the heart of digital privacy, and the value of approaching digital privacy in this manner has numerous theoretical, methodological or conceptual implications for wider studies of digital privacy itself. The dissertation makes more contributions to the study of digital privacy, particularly for the fields of Communications Studies and the wider multi-disciplinary approach the dissertation otherwise identifies as 'Privacy Studies' as well.

Contributions

Communications Studies

The dissertation's theory and methodology makes a few contributions to different fields of study, including Privacy Studies and Communication Studies as well a contribution to the study of digital software/technology as an object of analysis throughout these fields combined. For the field of Communication Studies, the dissertation makes a contribution by shifting analytical attitudes surrounding the engagement with the concept of 'noise'. Simply put, noise is as productive as it is destructive. But never one without the other. As demonstrated in the *SpiderOak One* case study, for example, the noise the software emits upon its users is one that deters interaction and dependency as much as it was originally intended to do otherwise. The intention, nonetheless, is to support users but the outcome, its routine failures, are not without merit and value for digital privacy. The noise the software emits catalyzed a series of new chains of interactions, new avenues for relation building – between existing news, with new users, with new software and even old software (like *DropBox*) that was otherwise deemed untrustworthy. The noise the users emit, in turn, multiples in origin and as such, destination. Users begin working on micro systems of amendments, systems of rules, of presupposition and exchange. All in an effort to not only make *SpiderOak One* more transparent in terms of its flaws for the coders and other users, but also to make that software more dependable. The initial coalescing of noisemaking between users and the software centralized *SpiderOak One* as *the* industry alternative, particularly in 2011/2012 during what is evidenced as the most turbulent years for digital surveillance and digital privacy.

But those noises split, they conflicted and clashed with one another thereafter. Once users began working on the issues and making them aware to their own communities – for example, on

both *GitHub* and *TCnext* – their noises amplified above and beyond the noise of the software. As awareness grew and solutions began to unravel – when users began splitting where their data was stored, as opposed to simply leaving it all with *SpiderOak One* – the users’ noises began influencing relations in neighbouring systems. What might otherwise seem like the defeat of *SpiderOak One*, the service still functions – and rather well – amongst its user base, despite the fact that the basis is smaller than it used to be. But that is not the point. The point here is that digital privacy shifted in meaning, orientation and above all, understanding. Reliable digital privacy on file hosting services is not simply a matter of ‘going to’ the most ‘reliable’ company with ‘the strongest’ encryption. It is a matter of how flows and systems of noises coalesce to reveal a different accounting of digital privacy therein. Digital privacy for *SpiderOak One* is as much about the relationship users have with the software interface, their own curiosity and technical expertise and their willingness to take the onus of file protection on themselves in building new systems of solutions that are inescapably multifaceted in purpose and design.

The point, very simply, is that the dissertation contributes to the field of Communications Studies an alternative and reinvigorated approach to the study of noise. This approach differs radically because it is a value-neutral approach – a non-normative, non-judgemental approach. The goal of this alternative methodology is to locate noise as a force that creates *variegation* in social systems. It serves as a reminder that although noise is inherent in all systems (Shannon, 1949), noise is also a fundamental component of all social life and social activity (Serres, 1982). Moreover, noise makes *every* social or technical system we study a unique case to study. Noise is quintessential to the very coalescing and clashing of social and technical flows in any socio-technical system. And as such, each socio-technical system is unique. As analysts, we must attend to the way in which systems are not only similar and different – particularly in terms of

the kinds of alternative understandings of digital privacy they reveal – but also to ways in which noisy systems can never be replicated *despite* coders’ and owners’ belief to the contrary.

Privacy Studies

The dissertation makes two contributions to Privacy Studies. The first is found in the fundamentality of noise to the notion of privacy. Between historical and contemporary approaches to privacy studies, the often implied but mutually agreed upon precondition for privacy is the ability to reduce, hide, conceal, withdraw, confuse, upset, obfuscate, smear or displace gaze, access, knowledge and control. As the second chapter discussed, even the most fundamental notions of noise become both the placeholder and modality through which the ability to achieve or make privacy takes place (Serres, 1982ii, 61-2). For example, consider how a window shopper may place sunglasses over her eyes while strolling through a shopping centre. The sunglasses make it more difficult for others to see the gaze of the window shopper. It challenges simple assumptions or understandings about what the window shopper is looking at, what direction the shopper is heading or even how the shopper is feeling. It is not merely the case the sunglasses are introduced to interrupt information flows. The idea is not to reduce privacy to a matter of merely confusion or inconvenience. The sunglasses may also insulate the wearer’s feelings. The sunglasses obfuscate signals about what her eyes might reveal about the kind of day she is having. The tint of the sunglasses is purposed fashionably and practically, indeed. But that same tint can be directly deployed differently, as both the deliberate and even incidental introduction of noise around gazes that otherwise access information flows in the name of creating a private experience or private condition.

The inextricability of noise to privacy implicates many of these pieces of literature the dissertation reviewed. As such, it also compels many of those pieces to amend their own lines of empirical and conceptual inquiry. For example, works in International Legal approaches to digital privacy, like Westby's (2004) work that mounts the idea that domestic state governments must work together with International bodies of privacy authority (i.e. the *European Union*), benefit from locating noisemaking activities from an individual and group level basis. Part of the task for Westby is relating privacy to individual rights and liberties from a very specific moral and ethical perspective, which is argued to be fundamental to the backbone of the constitutions of the governments she analyzes. The analysis of a constitution suspends and isolates individuals' relationships to a matter of the interpretation of codified ethical frameworks. This connection poses itself as a barrier in motivating domestic legislation to codify international law regarding privacy quickly and effectively. This kind of work can reinvigorate connections between individuals and the constitution by bringing specific empirical attention to the evidence that communities like *GitHub* are playing increasingly important roles in determining the outcome of the very privacy systems (like *Tor* and *SpiderOak One*) that are becoming increasingly commonplace technologies for governmental, university and corporate use.

Work in the social sciences would similarly benefit from such a methodology, particularly Bennett's *The Privacy Advocates: Resisting the Spread of Surveillance* (2008) which is one of the few examples of literature that attempts to expand the ontological playing field of the how and what of digital privacy. His work explicates that there is an entirely different and taken-for-granted domain of opinion and expertise upon the matters of privacy policy and legislation formation between governments and corporations. His work points towards the ongoing proliferation of advocacy networks, like the *American Civil Liberties Union*, who are

finding novel ways to speak on the behalf of individuals and social groups regarding concerns such as surveillance and hacking. The approach would benefit – like Westby’s – from locating the fundamental role users play in the outcome of digital privacy via their noisemaking on new and previously existing communications systems. A particular drawback of approaches in the social sciences that fail to recognize the role users *and* software plays on its own terms, for example, is not limited to Bennett (Bauman and Lyon, 2013; Amoore, 2014; de Geode, 2014). Advocacy networks are indeed empowering, but the issue is that their emphasis appears to (if only accidentally) reify the issue of centralizing noisemakers to government, corporations and large-social bodies. The emphasis on small-scale noisemaking prevents the further monopolizing of the origin and flow of noisemaking in the hands of venture capitalists in Silicon Valley. The prevention of galvanizing noisemaking into some sort of Neo-Marxist nightmare would be helpful beyond measure. By returning to the fundamentals of privacy, which we re-discovered together through the dissertation’s second chapter, we remind ourselves that privacy is a very social activity. One that unfolds in much more discrete and simple ways, one that unfolds in ways that we as analysts tend to dismiss and take for granted.

The computational sciences approach to the study of privacy (Marcella, 2003; Acquisti, 2007; Dingedine et al., 2004) would similarly benefit by expanding the scope of relations between the outcome of privacy as an object embodied by software and ‘who’ does the coding. While it is conventionally documented across this body of literature that ‘programmers’ ‘write’ ‘privacy’, the noisemaking efforts of users through accidental discoveries, conversations thereof and direct engagement in source-code repositories on open-source platforms is enough to begin radically and fundamentally altering the ontological landscape of some of the most foundational and important literature in contemporary privacy studies today.

The second major contribution the dissertation makes to Privacy Studies is importance of the role of users and the software itself in the unfolding of digital privacy. As discussed above, and throughout the dissertation's introduction and second chapter, privacy does not merely unravel through legislation, policy and software design. The case studies demonstrate that users play an exceptionally intimate role in the unravelling of their own privacy. Their noisemaking capacities directly spawned the realization of an entirely different domain through which digital privacy might otherwise be understood across file hosting services. The case studies also demonstrate that the software itself plays an equally important noisemaking role. The logics of Actor-Network Theory (Latour, 2007) are almost entirely absent from Privacy Studies literature. What the dissertation brings to Privacy Studies accordingly is a modality through which software ought to be treated as an actor unto itself – particularly in terms of the ways in which the software's aesthetics manipulates notions of proximity and intimacy with both the user and the coder. Actor-Network Theory within privacy studies flattens the ontological playing field, so to speak, and along-side the emphasis of user-oriented noisemaking as well, the project compels existing Privacy Studies literature to analyze privacy networks by triangulating noisemaking and social relationships between coders, users and software equally – a radically different approach to studying digital privacy as a matter of legislation, policy making and computer programming.

Final Word

What is emphasized repeatedly throughout the dissertation is the fundamentality of privacy to noise, and vice versa. The former implies notions of ‘reduction’, ‘retreat’ and ‘removal’ of awareness and knowledge. The latter is a modality of the former. It is the *act* of reducing and removing access, knowledge and control by introducing mechanisms of distraction, confusion and fuzziness. What the two notions – privacy and noise – have in common is that they are both solutions as much as they are problems. For example, privacy is resoundingly accepted across the academy as the ‘solution’ to ‘too much’ surveillance, data mining and hacking. The logic also mobilizes an intellectual attitude whereby ‘more privacy’ is universally prescribed for all victims – from governments and corporations to communities and individuals. A consequence of such thinking is the failure to recognize that ‘privacy’ is also a universal problem; it tremendously interferes with economic flow, ‘fact finding’ and relationship building.

Like privacy, ‘noise’ is as equally enabling as it is disabling. Where it differs from ‘privacy’ is in its reception across the academy. Privacy is heralded, while noise is feared. Surveillance is ‘noise’, ‘privacy’ is silence; noise signifies signal loss, the interruption of flow and the degradation of meaning. But as the dissertation demonstrates, the very act of making the edges of access, knowledge and control less sharp – the process of blurring the contents, location and destination of information – levies noise as a *tool* of privacy.

The future of privacy research in part rests upon further theoretical inquiry into privacy and noise as ‘privacy/noise’. One always with the other. As both solution and problem simultaneously, but never one without the other. From cultivating intellectual awareness and engagement accordingly, the academy distances itself from treating ‘privacy’ and ‘noise’ as normative subject matters. Rather, privacy/noise is a matter of variegation. It is a matter of

cultivating the intellectual attitude required to release the very human desire to control information flow. The goal is to release control, to allow flow to proceed from even the most seemingly infinitesimal actors so that we as analysts can get back to observing, documenting and pondering digital privacy 'in the wild'. It is a crucial requirement for the future of digital privacy because digital privacy is fraught with politics, tension and conflict. By promoting intellectual tolerance for locating the politics, tension and conflict inescapably surrounding and preceding privacy/noise, we learn to *lean into* noise as opposed to resisting it, repairing it and destroying it. The future of digital privacy studies will benefit by developing a passionate scholastic preoccupation with *wondering* about privacy. And by wondering about privacy, we will *attend* to privacy as opposed to *prescribing* it.

Bibliography

- ‘Cymru’. “[Dissolved] Spideroak Troubles – Networking, Server, and Protection.” *Arch Linux Forums*, 27 November 2011. Web. 27 March 2017. Available: <https://bbs.archlinux.org/viewtopic.php?id=169734>
- ‘dieTechnik’. “SpiderOak Is Stuck on ‘Waiting to Receive Initial Updates from Server’.” *dieTechnik Technology Blog*, 26 July 2013. Web. 27 March 2017. Available: <http://dietechnik.tumblr.com/post/93079762397/spideroak-is-stuck-on-waiting-to-receive-initial-updates>
- ‘KimikoMuffin’. “@SpiderOak It Is Stuck on ‘Syndication Process: Step 3 of 10, Getting List of Metadata from server’ [2/2].” *Twitter* microblog @kimikomuffin, 12 September 2014. Web. 21 March 2017. Available: <https://twitter.com/kimikomuffin/status/510485630225485824?lang=en>
- ‘lloncosky.’ “How Can I Add Delay to KDE Autostart Items.” *KDE Community Forums*, 25 September 2013. Web. 27 March 2017. Available: <https://forum.kde.org/viewtopic.php?f=225&t=117662>
- ‘Netninja’. “A few months with SpiderOak as DropBox replacement.” *NetNinja Technology Blog*, 5 July 2011. Web. 28 March 2017. Available: <https://netninja.com/2011/07/05/a-few-months-with-spideroak-as-dropbox-replacement/>
- ‘Rolfje’. “Replacing Dropbox with Spideroak.” *Rolfje Technology Blog*, 3 July 2011. 28 March 2017. Available: <https://rolfje.wordpress.com/2011/07/03/1355/>
- ‘verax74656’. “Something very fishy about SpiderOak. Can Someone Explain This?” */SpiderOak Sub Reddit*, 2 June 2016. Web. 30 March 2017. Available: https://www.reddit.com/r/SpiderOak/comments/3rv9ax/something_very_fishy_about_spideroak_can_someone/
- Acquisti, Alessandro. *Digital Privacy: Theory, Technologies, and Practices*. Boca Raton: Auerbach Publications, 2008.
- Adler, F. R. & M. Kretschmar. “Aggregation and stability in parasite-host models.” *Parasitology*, no. 104, 1992, pp. 199-205.
- Agosto, Denise E. and June Abbas. “Don’t be Dumb – that’s the rule I try to live by.” *New Media & Society*, vol. 19, no. 3, March 2017, pp. 347-365.

- AlBarashdi, Hafidha Sulaiman; Bouazza, Abdelmajid; Jabur H., Naeem and Abdulqawi S. Al-Zubaidi. "Smartphone Addiction Reasons and Solutions from the Perspective of Sultan Qaboos University Undergraduates: A Qualitative Study." *International Journal of Psychology and Behaviour Analysis*, no. 2, 2016, pp. 113-123. Web. Available: <https://www.graphyonline.com/archives/archivedownload.php?pid=IJPBA-113>
- Alexander, Cynthia Jacqueline, and Leslie Alexander Pal. *Digital Democracy: Policy and Politics in the Wired World*. Toronto: Oxford UP, 1998.
- AlternativeTo. "LogMeIn Backup Alternatives and Similar Software." *AlternativeTo*, 4 January 2010. Web. 23 March 2017. <http://alternativeto.net/software/logmein-backup/>
- Aly, Anne, Weimann-Saks, Dana and Gabriel Weimann. "Making 'Noise' Online: An Analysis of the Say No to Terror Online Campaign." *Perspectives on Terrorism*, vol. 8, no. 5, 2014.
- Amoore, Louise. "Security and the Claim to Privacy." *International Political Sociology*, vol. 8, no. 1, 14 March 2014, pp. 108-112.
- Aristotle, and Benjamin Jowett. *Aristotle's Politics*. New York, NY: Modern Library, 1943.
- Aroldi, Piermarco and Nicoletta Vittadini. "Children's rights and social media: Issues and prospects for adoptive families in Italy." *New Media & Society*, vol. 19, no. 5, May 2017, pp. 741-749.
- AskUbuntu. "Software Recommendation – Comparison of Backup Tools." *StackExchange*, 18 August 2010. 23 March 2017. Available: <http://askubuntu.com/questions/2596/comparison-of-backup-tools>
- Attali, Jacques. *Noise: The Political Economy of Music*. Minneapolis: U of Minnesota, 2011.
- Ayan, Arashful. "Is There Any Way to Overcome WhatsApp Addiction Without Uninstalling?" *Ayan's Blog*, 27 November 2012. Web. 2 March 2017. Available: <http://www.ashrafulayan.com/2012/11/whatsapp-addictive-dangerous-read-how.html>
- Barber, J. R., Crooks, K. R. and K. M. Fristrup. "The costs of chronic noise exposure for terrestrial organisms." *Trends in Ecology and Evolution*, vol. 25, no. 3, 2010, pp. 180-189.
- Baruh, Lemi and Mihaela Popescu. "Big data analytics and the limits of privacy self-management." *New Media & Society*, vol. 19, no. 4, April 2017, pp. 579-596.
- Bauman, Zygmunt and David Lyon. *Liquid Surveillance: A Conversation*. Cambridge, UK: Polity, 2013.

- Bea, Francis. "Facebook to Follow you Offline and See If You're Buying What They're Selling." *DigitalTrends News*, 25 September 2012. Web. 1 March 2017. Available: <http://www.digitaltrends.com/social-media/facebook-partners-with-datalogix-to-track-offline-retail-purchases/>
- Bellanova, Rocco. "Data Protection, with Love." *International Political Sociology*, vol. 8, no. 1, 14 March 2014, pp. 112-115.
- Belshaw, Doug. "Why I'm Saying Goodbye to Dropbox and Hello to SpiderOak." *Open Educational Thinkering Technology Blog*. 28 August 2013. Web. 23 March 2017. Available: <http://dougbelshaw.com/blog/2013/08/28/why-im-saying-goodbye-to-dropbox-and-hello-to-spideroak-hive/>
- Bennett, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT, 2008.
- Bijker, Wiebe E., Hughes, Thomas P. and Trevor J. Pinch (Eds). *The Social Construction of Technology Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1993.
- Bloch-Rozmej, Anna. "Noise as a Phonological Element: On the Representation of Plosives" *New Perspectives in Language, Discourse and Translation Studies*. Springer, 2011.
- Bodó, Balázs. "Hacktivism 1-2-3: How Privacy Enhancing Technologies Change the Face of Anonymous Hacktivism." *Internet Policy Review*, 2016, <https://policyreview.info/articles/analysis/hacktivism-1-2-3-how-privacy-enhancing-technologies-change-face-anonymous>
- Bolton, Michael Sean. "Digital Parasites: Reassessing Notions of Autonomy and Agency in Posthuman Subjectivity." *Theoria and Praxis: International Journal of Interdisciplinary Thought*, vol. 1, no. 2, 2014, pp. 14-26.
- Bosker, Bianca. "Dropbox Bug Made Passwords Unnecessary, Left Data at Risk For Hours." *Huffington Post Tech*, 21 June 2011. Web. 21 March 2017. Available: http://www.huffingtonpost.com/2011/06/21/dropbox-security-bug-passwords_n_881085.html
- Brandom, Russell. "FBI Agents Tracked Harvard Bomb Threats despite Tor." *The Verge*, 18 December 2013, <http://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor>
- Burrell, Henry. "How Secure is WhatsApp? WhatsApp Security and Encryption Explained." *TechAdvisor*, 27 March 2017. Web. 30 March 2017. Available: <http://www.pcadvisor.co.uk/feature/internet/how-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780/>

- Carey, James. *Communication as Culture*. New York, NY: Routledge, 1989.
- Carlson, Nicholas. "Well, These New Zuckerberg Facebook IMs Won't Help Facebook's Privacy Problems." *Business Insider*, 13 May 2010. Web. Accessed 29 February 2017. Available: <http://www.businessinsider.com/well-these-new-zuckerberg-ims-wont-help-facebooks-privacy-problems-2010-5>
- Cavoukian, Anne. "Data Mining: Staking a Claim on your Privacy." Information and Privacy Commissioner, Ontario, <http://www.ipc.on.ca/images/resources/datamine.pdf>
- Chaabane, Abdelberi, Manils, Pere and Mohammed Ali Kaafar. "Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network." MS. *INRIA Rhone-Alps*, Grenoble, France. Web. 9 March 2017. Available: <http://planete.inrialpes.fr/papers/TorTraffic-NSS10.pdf>
- Chakraberty, Sumit. "The Psychology behind the Rise of WhatsApp." *YourStory.com*. 21 February 2014. Web. 21 March 2017. Available: <https://yourstory.com/2014/02/whatsapp-rise/>
- Chowdry, Amit. "WhatsApp hits 500 million users." *Forbes*, 2014, <https://www.forbes.com/sites/amitchowdhry/2014/04/22/whatsapp-hits-500-million-users/#7b9f7e9d702a>
- Christensen, Chris. "Polish Mathematicians Finding Patterns in Enigma Messages." *Bulletin of Sociological Methodology*, vol. 103, 2009, pp. 88-91.
- Clark, Ellison, Southall, Hatch, Van Parijs and Ponirakis Frankel. "Acoustic masking in marine ecosystems: intuitions, analysis, and implication." *Marine Ecology Progress Series*, vol. 395, 2009, pp. 201-222.
- CloudStorageBuzz. "SpiderOak Review." *Cloud Storage Buzz*, 19 April 2009. Web. 24 March 2017. Available: <https://cloudstoragebuzz.com/spideroak/>
- Cloudwards. "SpiderOak Review." *Cloudwards*, 19 September 2016. Web. 27 March 2017. Available: <https://www.cloudwards.net/review/spideroak/>
- Cochin, Brian, Seufert, Michael, Tobias Hossfeld, Anika Schwind, Valentin Burger, Phuoc Tran-Gia. "Group-based Communication in WhatsApp." *GlobalMediaInsight Research*, 12 January, 2014. Web. 6 March 2017. Available: <http://www.globalmediainsight.com/blog/whatsapp-users-statistics/>
- Coen, Deborah R. *Vienna in the Age of Uncertainty: Science, Liberalism, and Private Life*. Chicago: U of Chicago, 2007.

- Cohen, David. "More Millennials Use Facebook Messenger, WhatsApp." *Adweek.com Digital*, 9 March 2014. Web. 26 February 2017. Available: <http://www.adweek.com/digital/infographic-gwi-millennials-messenger-whatsapp/>
- Connors, Devin. "Snowden Says Dropbox, Condoleezza Rice Are Hostile to Privacy" *The Escapist*, 18 July 2014. Web. 23 March 2017. Available: <http://www.escapistmagazine.com/news/view/136245-Snowden-says-Dropbox-Condoleezza-Rice-are-Hostile-to-Privacy>
- Conrad, Claus. "Restarting SpiderOak after Switching Networks" on *Claus Conrad Technology Blog*, 10 December 2013. Web. 27 March 2017. Available: <http://www.clausconrad.com/blog/restarting-spideroak-after-switching-networks>
- Cooke, Thomas N. "Cookies." *Making Things International II: Catalysts and Reactions*. Mark Salter (Ed.), University of Minnesota Press, 2016.
- Cooke, Thomas N. "Security, Power and Digital Privacy." *E-IR, The Journal of Electronic International Relations*, 2015. Web. Available: <http://www.e-ir.info/2015/04/30/security-power-and-digital-privacy/>
- Cox, Joseph. "Hackers Stole Account Details for Over 60 Million Dropbox Users." *Motherboard VICE*, 30 August 2016. Web. 23 March, 2017. Available: https://motherboard.vice.com/en_us/article/hackers-stole-over-60-million-dropbox-accounts
- Crocker, Stephen. "Noises and Exceptions: Pure Mediality in Serres and Agamben." *CTheory*, 24 October 2016. Web. 3 April 2017. Available: <https://journals.uvic.ca/index.php/ctheory/article/view/14508/5349>
- Crowcroft, Jon. "Net Neutrality: The Technical Side of the Debate ~ A White Paper." *International Journal of Communication*, vol. 1, 2007, pp. 567-579.
- Crowley, Jenny L. "A Framework of Relational Information Control: A Review and Extension of Information Control Research in Interpersonal Contexts." *Communication Theory*, vol. 27, no. 2, May 2017, pp. 202-222.
- CyberPsychology Institute. "How WhatsApp Is Ruining Relationships." *CyberPsychology*, 19 August 2016. Web. 20 March 2017. Available: <http://cyberpsychology.in/whatsapp-relationships>
- Day, Dennis G. "Learning and Communication Theory." *Central States Speech Journal*, vol. 15, no. 2, 2009, pp. 84-89.
- De Goede, Marieke. "The Politics of Privacy in the Age of Preemptive Security," *International Political Sociology*, vol. 8, no. 1, 26 October 2016, pp. 100-104.

- De Vries, Imar O. *Tantalisingly Close: An Archaeology of Communication Desires in Discourses of Mobile Wireless Media*. Amsterdam, Netherlands: Amsterdam University Press, 2012.
- Decew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Ithaca, NY: Cornell University Press, 1997.
- Devereaux, Claire L., Denny, Matthew J. H., and Mark J. Whittingham. "Minimal effects of wind turbines on the distribution of wintering farmland birds." *Journal of Applied Ecology*, vol. 45, no. 6, 2008, pp. 1689-1694.
- Dierks, T. and E. Rescorla. "The Transport Layer Security (TLS) Protocol Version 1.2." *Internet Engineering Task Force*, August 2008. Web. 20 March 2017. Available: <https://tools.ietf.org/html/rfc5246>
- Dingledine, Roger, Mathewson, Nick and Paul Syverson. "Tor: The Second-Generation Onion Router." Tor Project Database, 2004. Web. Available: <https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>
- Dolan, Daniel. "Cultural Noise: Amplified Sound, Freedom of Expression and Privacy Rights in Japan." *International Journal of Communication*, vol. 2, 2008, pp. 662-690.
- Dowling Jr., Donald C. "International Data Protection and Privacy Law." Published by *White & Case Law*, September 2014. Web. 30 November, 2016. Available: https://intellicentrics.ca/wp-content/uploads/dlm_uploads/2014/09/article_intldataprotectionandprivacylaw_v5-1.pdf
- Elmer, Greg. *Profiling Machines: Mapping the Personal Information Economy*. New York, NY: MIT Press, 2003.
- Enns, Anthony. "The Parasite (review)." *Project MUSE*, vol. 42, no. 2, April 2009. Web. 4 April 2017, pp. 170-1. Available: <https://muse.jhu.edu/article/259902/summary>
- Evans, John. "WhatsApp Partners with OpenWhisper Systems to End-to-End Encrypt Billions of Messages a Day." *TechCrunch.com News*, 24 November 2014. Web. 1 March 2017. Available: <https://techcrunch.com/2014/11/18/end-to-end-for-everyone/>
- Fagoyinbo, Joseph Babatunde. *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity*. London, UK: Author House, 2013.
- Federal Trade Commission of the United States of America. "FTC Approves Final Settlement with Facebook." *The Federal Trade Commission of the United States of America*, 10 August 2012. Web. 2 March 2017. Available: <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>
- Flanigan, Andrew J., Craig Flanigan and Jon Flanigan. "Technical code and the Social Construction of the Internet." *New Media & Society*, vol. 12, no. 2, 2010, pp: 179-196.

- Fleishman, Glenn. "Online Backup Services." *PCWorld*, 7 November 2009. Web. 29 March 2017. Available: http://www.pcworld.com/article/171547/online_backup_services.html
- Foucault, Michel. *Power*. The New York Press, 2000.
- Fiske, John. *Introduction to Communication Studies*. London, UK: Routledge, 1982.
- Frosch, Tilman, Mainka, Christian, Bader, Christoph, Bergsma, Florian, Schwenk, Jörg, and Thorsten Holz. *How Secure is TextSecure?* 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrücken, Germany: IEEE. March 2016, pp. 457–472.
- Fulton, R. Barry. "Information Theory and Linguistic Structuring." *Central States Speech Journal*, vol. 14, no. 4, 2009, pp. 247-257.
- Gannes, Liz. "Dropbox Raises \$7.25M, Crosses 3M Users." *GigaOM*, 24 November 2009. Web. 21 March 2017. Available: <https://gigaom.com/2009/11/24/dropbox-raises-7-25m-crosses-3m-users/>
- Garron, Guillermo. "SpiderOak Cross Platform Backup Service." *Guillermo Garron Technology Blog*, 12 February 2009. Web. 27 March 2017. Available: http://go2linux.garron.me/spideroak_backup_server/
- Gates, Kelly and Shoshana Magnet. "Communication Research and the Study of Surveillance." *The Communication Review*, vol. 10, no. 4, 2007, pp. 277-293.
- Glatter-Götz, Henning. "Bye Bye Spideroak." *Glatter-Gotz Technology Blog*. 12 January 2016. Web. 27 March 2017. Available: <http://www.glatter-gotz.com/blog/2015/01/12/bye-bye-spideroak/>
- Golomb, Solomon M. "Claude E. Shannon (1916-2001)." *Science*, vol. 292, no. 5516, 20 April 2001, pp. 455.
- Goldberg, Ian. "Privacy-Enhancing Technologies for the Internet III: Ten Years Later," MS. University of Waterloo, 2002.
- Grant, Rebecca A., and Colin J. Bennett. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press, 1999.
- Gumpert, Gary and Susan J. Drucker. "The Demise of Privacy in a Private World: From Front Porches to Chat Rooms." *Communication Theory*, vol. 8, no. 4, November 1998, pp. 408-425.
- Gunkel, David. "We Are Borg: Cyborgs and the Subject of Communication." *Communication Theory*, vol. 10, no. 3, August 2000, pp. 332-357.

- Gustin, Sam. "Facebook's WhatsApp Data Gambit Faces Federal Privacy Complaint." *Motherboard*, 26 August 2017. Web. 1 March 2017. Available: https://motherboard.vice.com/en_us/article/whatsapp-facebook-privacy-complaint
- Ha, Anthony. "Edward Snowden's Privacy Tips: 'Get Rid Of Dropbox,' Avoid Facebook And Google." *TechCrunch*, 11 October 2014. Web. 20 March 2017. Available: <http://social.techcrunch.com/2014/10/11/edward-snowden-new-yorker-festival/>
- Hacker10. "How Does Encryption Work?" *Hacker10 Technology Blog*, 23 April 2011. Web. 23 March 2017. Available: <http://www.hacker10.com/computer-security/how-does-encryption-work-encryption-for-dummies/>
- HackerNews YCombinator. "Ask HN: Who Is Hiring Remote Workers? (First Edition, November 2010)." *Hacker News*, 6 June 2007. 23 March 2017. Available: <https://news.ycombinator.com/item?id=1857051>
- Hafer, Nina and Manfred Milinski. "When parasites disagree: Evidence for parasite-induced sabotage of host manipulation." *Evolution*, vol. 69, no. 3, January 2015, pp. 611-620: 10.1111/evo.12612
- Hainge, Greg. "Of Glitch and Men: The Place of the Human in the Successful Integration of Failure and Noise in the Digital Realm." *Communication Theory*, vol. 17, no. 1, February 2007, pp. 26-42.
- Haley, Fiona. "SpiderOak 3.0 Review." *ComputerShopper*, 5 May 2009. Web. 30 March 2017. Available: <http://www.computershopper.com/software/reviews/spideroak-3.0>
- Hanson, Matthew. "40% of Italian Divorces over Cheating Involve WhatsApp." *T3*, 4 December 2014. Web. 5 March 2017. Available: <http://www.t3.com/news/40-of-italian-divorces-over-cheating-involve-whatsapp>
- Hildebrand, John A. "Anthropogenic and natural sources of ambient noise in the ocean.: *Marine Ecology Progress Series*, vol. 395, 2009, pp. 5-20.
- Hodkinson, Paul. "Bedrooms and beyond: Youth, identity and privacy on social network sites." *New Media & Society*, vol. 19, no. 2, February 2017, 272-288.
- Houston, Drew. "Thanks a (Hundred) Million." *Dropbox Blog*, November 2012. Web. 23 March 2017. Available: <https://blogs.dropbox.com/dropbox/2012/11/thanks-a-hundred-million/>
- Huber, Markus, Mulazzani, Martin and Edgar Weippl. "Tor HTTP and Information Leakage." Presented in the Proceedings of the 11th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security (CMS 2010), Linz, Austria, May 2010, <https://www.freehaven.net/anonbib/cache/huber2010tor.pdf>

- Hughes, Thomas P. "The Evolution of Large Technological Systems." in Wiebe E. Bijker, Hughes and Trevor J. Pinch (Eds.) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987.
- Igo, Sarah Elizabeth. *The Averaged American: Surveys, Citizens, and the Making of a Mass Public*. Cambridge, MA: Harvard UP, 2007.
- Johnson, Bobby. "Privacy no longer a social norm, says Facebook founder." *The Guardian*, 11 January 2010. Web. 24 February 2017. Available: <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>
- Johnson, Chalmers. *The Sorrows of Empire: Militarism, Secrecy and the End of the Republic*. New York, NY: Metropolitan Books, 2004.
- Johnson, K. P.; Richards, Adam J.; Page, Roderic D. M. and Dale H. Clayton. "When do Parasites Fail to Speciate in Response to Host Speciation?" *Systemic Biology*, vol. 52, no. 1, February 2003, pp. 37-47.
- Katamba, Francis and Michael Dobrovolsky "Phonetics: The Sounds of Language." *Contemporary Linguistics: An Introduction*. (Eds.) William O'Grady, Michael Dobrovolsky and Francis Katamba. New York: Longman, 2011.
- Kholia, Dhiru, and Przemys Węgrzyn. "Looking Inside the (Drop) Box." Proceedings of the 7th *USENIX Conference on Offensive Technologies*, 9–9. WOOT'13. Berkeley, CA, USA: USENIX Association, 2013. Accessed 21 March 2017. Available: <http://dl.acm.org/citation.cfm?id=2534748.2534760>
- Kirk, Jeremy. "Tor Project: Stop Using Windows, Disable JavaScript to Protect Your Anonymity." *PCWorld*, 6 August 2013, <http://www.pcworld.com/article/2046013/tor-project-stop-using-windows-disable-javascript.html>
- Kiss, Jemima. "Snowden: Dropbox Is Hostile to Privacy, Unlike 'Zero Knowledge' Spideroak." *The Guardian Technology*, 17 July 2014. Web. 21 March 2017. Available: <https://www.theguardian.com/technology/2014/jul/17/edward-snowden-dropbox-privacy-spideroak>
- Kissell, Joe. "Alternatives to MobileMe." *Macworld*, 29 January 2009. Web. 23 March 2017. Available: <http://www.macworld.com/article/1138481/mobilemealternatives.html>
- Klapp, Orinn E. "Meaning Lag in the Information Society." *Journal of Communication*, 1982.
- Knibbs, Kate. "9 Things We Learned from Mark Zuckerberg's Appearance at Mobile World Congress." *Digital Trends*, 24 February 2014. Web. 3 March 2017. Available: <http://www.digitaltrends.com/social-media/learned-mark-zuckerberg-2014-mobile-world-congress/>

- Kobie, Nicole. "Researcher Files FTC Complaint against Dropbox." *Alphr*, 16 May 2011. Web. 23 March 2017. Available: <http://alphr.com/news/cloud/367387/researcher-files-ftc-complaint-against-dropbox>
- Koebler, Jason. "How the NSA (Or Anyone Else) Can Crack Tor's Anonymity." *Motherboard*, 2014, https://motherboard.vice.com/en_us/article/how-the-nsa-or-anyone-else-can-crack-tors-anonymity
- Latham, Robert. *The Politics of Evasion: A Post-Globalization Dialogue Along the Edge of the State*. Routledge, 2016.
- Latour, Bruno. *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford University Press, 2007.
- LaRose, Robert and Nora Rifon. "Your privacy is assured – of being disturbed: websites with and without privacy seals." *New Media & Society*, vol. 8, no. 6, December 2006, pp. 1009-1029.
- Lee, Timothy B. "Everything you need to know about the NSA and Tor in on FAQ" in *The Washington Post*. 3 October 2013. Web. Available: https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/?utm_term=.8a6dae1e814b
- Leigh, David and Luke Harding. *WikiLeaks: Inside Julian Assange's War on Secrecy*. London, UK: Guardian Books, 2011.
- LeJacq, Yives. "Facebook Ad Exchange Boasts Massive Return on Investment; Is The Social Network Finally Ready to Take on Google?" *International Business Times*, 13 October 2013. Web. 1 March 2017. Available: http://www.ibtimes.co.uk/articles/384116/20120913/facebook-ad-exchange-mark-zuckerberg-shares-google.htm?utm_source=dlvr.it&utm_medium=twitter
- LeJacq, Yives. "Facebook Raises Privacy Concerns With DataLogix Partnership." *International Business Times*, 24 September 2012. Web. 1 March 2017. Available: <http://www.ibtimes.com/facebook-raises-privacy-concerns-datalogix-partnership-795325>
- Leuz, Christian and Felix Oberholzer-Gee. "Political Relationships, Global Financing, and Corporate Transparency: Evidence from Indonesia." *Journal of Financial Economics* vol. 81, no. 2, 2006, pp. 411–39.
- Levine, Yasha. "Almost Everyone Involved in Funding Tor was (or is) Funded by the US Government." *Pando Blog*. 16 July 2014, <https://pando.com/2014/07/16/tor-spoofs/>

- Litte, Jane. "A Secure Alternative to Dropbox: Tondio, SpiderOak, Cubby, and GoodSync." *Dear Author Blog*, 23 December 2012. 29 March 2017. Available: <http://dearauthor.com/ebooks/a-secure-alternative-to-dropbox-tondio-spideroak-cubby-and-goodsync/>
- Livingstone, Sonia. "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression." *New Media & Society*, vol. 10, no. 3, June 2008, pp. 393-411.
- Lo, Joseph. "SpiderOak – Why It Is Not Working for Me." *Joseph Lo Technology Blog*, 12 December 2013. Web. 23 March 2017. Available: <https://josephlo.wordpress.com/2013/12/12/spideroak-why-it-is-not-working-for-me/>
- Locke, John. *The Second Treatise of Civil Government and A Letter Concerning Toleration*. Oxford, UK: B. Blackwell, 1948.
- Lomas, Natasha. "WhatsApp to Share User Data with Facebook for Ad Targeting — Here's How to Opt out." *TechCrunch*. 25 August 2016. Web. 1 March 2017. Available: <http://social.techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/>
- Lundblad, Nicklas. "Privacy in the Noise Society." Published by the *Stockholm Institute for Scandinavian Law*, 2010. <http://www.scandinavianlaw.se/pdf/47-16.pdf>. Accessed 30 November 2016.
- Lunden, Ingrid. "Dropbox Has Quietly Acquired Parastructure, A Big Data Startup In Stealth." *TechCrunch*, 16 June 2014. Web. 23 March 2017. Available: <http://social.techcrunch.com/2014/06/16/dropbox-has-quietly-acquired-parastructure-a-big-data-startup-in-stealth/>
- Macke, Jeff. "Facebook Shares Heading Back to \$38 IPO Price Says Kilburg." *Yahoo! Finance News*, 29 October 2013. Web. 9 March 2017. Available: <http://finance.yahoo.com/blogs/breakout/facebook-shares-heading-back-38-ipo-price-says-132702382.html>
- Makrushin, Denis and Maria Garnaeva. "Uncovering Tor Users: where anonymity meets the Darknet" on *SecureList – AO Kaspersky Lab*. 18 June 2015, <https://securelist.com/analysis/publications/70673/uncovering-tor-users-where-anonymity-ends-in-the-darknet/>
- Marcella, Albert J. and Carol Stucki. *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues*. Hoboken, NJ: J. Wiley, 2003.
- Marcey, Joel. "Choosing an Online Backup Service – Revisited." *Joel Marcey Technology Blog*, 28 March 2009. Web. 23 March 2017. Available: <http://www.joelmarcey.com/blog/2009/03/28/choosing-an-online-backup-service-revisited>

- MarketWired Newsroom. "SpiderOak Announces Penetration: Privacy Matters." *Marketwire*, 19 February 2013. Web. 27 March 2017. Available: <http://www.marketwired.com/press-release/spideroak-announces-penetration-privacy-matters-1758061.htm>
- McBride, Sarah. "Ukrainian Roots shine through at WhatsApp." *Reuters.com*, 19 February 2014. Web. 26 February 2016. Available: <http://www.reuters.com/article/us-whatsapp-facebook-ukraine-idUSBREA1J07N20140220>
- McFarlin, Tom. "My First Two Months with SpiderOak Hive." *Tom McFarlin Technology Blog*, 25 October 2013. Web. 24 March 2017. Available: <https://tommcfarlin.com/spideroak-hive/>
- McWhirter, Darien A, and Jon D. Bible. *Privacy As a Constitutional Right: Sex, Drugs, and the Right to Life*. New York: Quorum Books, 1992.
- Mehta, Ivan. "Sorry! You Can't Opt Out Of WhatsApp-Facebook Data Sharing." *Huffington Post India*, 26 August 2016. Web. 4 March 2017. Available: <http://www.huffingtonpost.in/2016/08/26/sorry-you-cant-opt-out-of-whatsapp-facebook-data-sharing/>
- Merchant, Brian. "The Facebook Manipulators." *Motherboard*, 3 July 2014. Web. 1 March 2017. Available: https://motherboard.vice.com/en_us/article/the-facebook-manipulators
- Michallon, Clemence. "Mark Zuckerberg sues to protect HIS privacy: Facebook CEO in legal battle to force hundreds of native Hawaiians who have ancestral rights to patches of his vast \$100m estate to sell up." *The DailyMail News*, 19 January 2017. Web. 21 February 2017. Available: <http://www.dailymail.co.uk/news/article-4134654/Mark-Zuckerberg-sues-families-force-sell-land.html>
- Mill, John Stuart. *On liberty*. London, UK: Longman, Roberts & Green, 1869.
- Montag, Christian, Błaszkiwicz, Konrad, Sariyska, Rayna, Lachmann, Bernd, Andone, Ionut, Trendafilov, Boris, Eibes, Mark and Alexander Markowetz. "Smartphone Usage in the 21st Century: Who Is Active on WhatsApp?" *BMC Research Notes* vol. 8, 2015, pp. 331-361.
- Muller, Benjamin. *Security, Risk and the Biometric State: Governing Borders and Bodies*. London: Routledge, 2010.
- Nathanson, Jon and Will Oremus. "But Google Drive Does the Exact Same Thing!" *Slate News*, April 2014. Web. 28 March 2017. Available: http://www.slate.com/articles/technology/technology/2014/04/dropbox_three_big_questions_about_the_company_that_should_be_google_s_next.html
- National Security Agency of the United States of America. "Civil Liberties and Privacy." *NSA-CSS*, 3 May 2016. Web. 11 July 2017. Available: <https://www.nsa.gov/about/civil-liberties/>

- Nelsen, Arthur. "Number of criminal gangs operating in Europe urges to 5,000, Interpol says." *The Guardian News*, 9 March 2017, <https://www.theguardian.com/uk-news/2017/mar/09/more-than-5000-criminal-gangs-operating-in-europe-warns-europol>
- Nestor, Marius. "openSUSE 11.3 Available for Download." *Softpedia*, 15 July 2010. Web. 23 March 2017. Available: <http://news.softpedia.com/news/openSUSE-11-3-Available-for-Download-147735.shtml>
- Nevitt, Barrington. "Visible and Invisible Bias via Media." *Canadian Journal of Communication*, vol. 7, no. 3, 1981, pp. 9-42.
- Nissenbaum, Helen Fay. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law, 2010.
- O'Reilly, Dennis. "Three Approaches to Free Encrypted Online Storage." *CNET*, 24 June 2009. Web. 23 March 2017. Available: <https://www.cnet.com/how-to/three-approaches-to-free-encrypted-online-storage/>
- Office of the Privacy Commissioner of Canada. "Public Opinion Survey: 2016 Survey of Canadians on Privacy." *The Office of the Privacy Commissioner of Canada*, 9 November 2016. Web. 2 March 2017. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#fig3
- Office of the Privacy Commissioner of Canada. "WhatsApp's violation of privacy partly resolved after investigation by data protection authorities." *The Office of the Privacy Commissioner of Canada*, 2 February 2014. Web. 2 March 2017: Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2013/nr-c_130128/
- Oliver, Paul. *The Student's Guide to Research Ethics*. Maidenhead: Open University Press, 2003.
- Olson, Parmy. "Exclusive: The Rags-to-Riches Tale of How Jan Koum Built WhatsApp Into Facebook's News \$19 Billion Dollar Baby" *Forbes*, 2014, <https://www.forbes.com/sites/parmyolson/2014/02/19/exclusive-inside-story-how-jan-koum-built-whatsapp-into-facebooks-new-19-billion-baby/#1f87e0532fa1>
- Omand, David. "Surveillance Is 'Essential' When Terror Fills the Web with Noise." *WIRED UK*, 11 April 2016. Web. 5 April 2017. Available: <http://www.wired.co.uk/article/gchq-cyberterrorism-surveillance>
- Oodshorn, Nelly and Trevor. *How Users Matter: The Co-Construction of Users and Technology*. Cambridge, MA: MIT Press, 2005.
- Opinion Panel Community Editorial Team. "8 types of WhatsApp users that are driving us crazy." *The Opinion Panel Community*, 17 March 2015. Web. 1 March 2017. Available: <https://www.opinionpanel.co.uk/2015/03/17/8-most-annoying-whatsapp-users/>

- Orlin, Lena Cowen. *Private Matters and Public Culture in Post-Reformation England*. Cornell University Press, 1994.
- Paddison, Ronan, Chris Philo, Paul Routledge, and Joanne Sharp. *Entanglements of Power: Geographies of Domination/Resistance*. Routledge, 2002.
- Paganini, Pierluigi. "81 Percent of Tor Clients Can Be Identified with Traffic Analysis Attack." *Security Affairs*, 15 November 2014. Web. 3 March 2017. Available: <http://securityaffairs.co/wordpress/30202/hacking/tor-traffic-analysis-attack.html>
- Panzarino, Matthew. "Facebook Buying WhatsApp for \$19B, Will Keep the Message Service Independent." *TechCrunch News*, 19 February 2014. Web. 14 March 2017. Available: <https://techcrunch.com/2014/02/19/facebook-buying-whatsapp-for-16b-in-cash-and-stock-plus-3b-in-rsus/>
- Peoples, Columba and Nick Vaughan-Williams. *Critical Security Studies: An Introduction*. Routledge, 2014.
- Porter, James E. *Rhetorical Ethics and Internetnetworked Writing*. Greenwood Publishing Group, 1998.
- Post, Warren. "Moving to a New Device with SpiderOak." *Warren Post Technology Blog*, 25 October 2012. Web. 26 March 2017. Available: <https://warrenpost.wordpress.com/2012/10/25/spideroak-migration/>
- Prinzlau, Mauricio. "Dropbox Is Only 'Quite Secure'." *Cloudwards*, 12 November 2012. Web. 23 March, 2017. Available: <https://www.cloudwards.net/news/dropbox-is-only-quite-secure-727/>
- Rawlins, William K. "Theorizing Private and Public Domains and Practices of Communication: Introductory Concerns." *Communication Theory*, vol. 8, no. 4, November 1998, pp. 369-380.
- Reddy, Michael J. "The Conduit Metaphor: A Case of Frame Conflict in our Language about Language." Andrew Ortony (Ed.), *Metaphor and Thought*. Cambridge, UK: Cambridge University Press, 1979.
- Reinke, Edgar C. "Classical Cryptography." *The Classical Journal*, vol. 58, no. 3, 1962, pp. 113-121.
- Rousseau, Jean-Jacques and Donald A. Cress. *On the Social Contract*. Indianapolis: Hackett Publishing Company, 1987.
- Rowan, David. "WhatsApp: The inside Story." *Ars Technica*, 20 February 2014. Web. 23 February 2017. Available: <https://arstechnica.com/business/2014/02/whatsapp-the-inside-story/>

- Ruskin, Steven. *John Herschel's Cape Voyage: Private Science, Public Imagination and the Ambitions of Empire*. New York, NY: Routledge, 2004.
- St. Pierre, Joshua. "Crippling Communication: Speech, Disability, and Exclusion in Liberal Humanist and Posthumanist Discourse." *Communication Theory*, vol. 25, no. 3, August 2015, pp. 330-348.
- Scherschel, Fabian A. "Keeping Tabs on WhatsApp's Encryption." *Heise News*. March 2015. Web. 1 March 2017. Available: <https://www.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html>
- Schneier, Bruce. "The Difficulty of Routing around Internet Surveillance States." *Noise*, 14 December 2016, <https://noise.getoto.net/2016/07/07/the-difficulty-of-routing-around-internet-surveillance-states/>
- Scott, Craig R. "To Reveal or Not to Reveal: A Theoretical Model of Mass Communication." *Communication Theory*, vol. 8, no. 4, November 1999, pp. 381-407.
- Sennett, Richard. *Flesh and Stone: The Body and the City in Western Civilization*. New York: W.W. Norton, 1994.
- Sennett, Richard. *The Fall of Public Man*. New York: W. W. Norton, 1977.
- Serres, Michel. *Genesis*. The University of Michigan Press, 1982.
- Serres, Michel. *The Parasite*. Baltimore: Johns Hopkins University Press, 1982.
- Shannon, C. E. "Communication in the Presence of Noise." *Proceedings of the IRE* 37.1. 10-21, 1949.
- Shapin, Steven. *Never Pure: Historical Studies of Science as If It Was Produced by People with Bodies, Situated in Time, Space, Culture, and Society, and Struggling for Credibility and Authority*. Baltimore, MD: Johns Hopkins UP, 2010.
- Shead, Mark. "SpiderOak Storage and Backup Review." *Productivity501 Technology Blog*, 21 December 2010. Web. 27 March 2017. Available: <http://www.productivity501.com/spideroak-storage-and-backup-review/8405/>
- Singel, Ryan. "Dropbox Lied to Users About Data Security, Complaint to FTC Alleges." *WIRED*, May 2011. Web. 23 March 2017. Available: <https://www.wired.com/2011/05/dropbox-ftc/>
- Skufca, Lawrence Christopher. "The Pros and Cons of Using Tor." *Pando Blog*. 8 January 2016, <https://camdencivilrightsproject.com/2016/01/08/the-pros-and-cons-of-using-tor/>
- Smith, Brian Cantwell. *On the Origin of Objects*. New York, NY: The MIT Press, 1998.

- Sousa-Lima, Renata S. and Christopher W. Clark. "Whale sound recording technology as a tool for assessing the effects of boat noise in a Brazilian marine park." *Park Science*, vol. 26, 2016, pp. 59-63.
- SpiderOak. "Private by Design." *SpiderOak*. Web. 27 March 2017. Available: <https://spideroak.com/features/private-by-design>
- Steinen, Richard. "Network-Centric Warfare Set the Stage for Cyberwar." *Cicero Magazine*, 9 November 2014. Web. 10 July 2017. Available: <http://ciceromagazine.com/features/network-centric-warfare-set-the-stage-for-cyberwar/>
- Sullivan, Denise. "Is Dropbox Security Truly Poor?" *Cloudwards*, 8 August 2014. Web. 24 March 2017. Available: <https://www.cloudwards.net/is-dropbox-security-truly-poor/>
- Svantesson, Dan. "The Concept of 'extraterritoriality' in Law." *OUPblog*, 17 November 2015, <http://blog.oup.com/2015/11/extraterritoriality-law/>
- Takayasu, Misako, Hideki Takayasu, and Takamitsu Sato. "Critical Behaviors and $1/\Phi$ Noise in Information Traffic." *Physica A: Statistical Mechanics and Its Applications*, vol. 233, no. 3, 1 December 1996, pp. 824–34:10.1016/S0378-4371(96)00189-6.
- Taulli, Tom. "SpiderOak CEO Ethan Oberman Talks Cloud, Facebook IPO." *InvestorPlace*, 17 May 2012. Web. 22 March 2017. Available: <http://investorplace.com/ipo-playbook/interview-spideroak-ceo-ethan-oberman/>
- Teixeira, Thales and Elizabeth Anne Watkins. "Freemium Pricing at Dropbox." *Harvard Business School Case Collection*, 2013. Web. 25 March 2017. Available: <http://www.hbs.edu/faculty/Pages/item.aspx?num=45910>
- The Opinion Panel Editorial Team. 2015. "8 Types of Whatsapp Users Driving Us Crazy." *The OpinionPanel Community*. Available: <https://www.opinionpanel.co.uk/2015/03/17/8-most-annoying-whatsapp-users/>
- Thompson, Rachel. "This One WhatsApp Feature Can Make or Break Relationships." *Mashable*, 6 June 2016. Web. 5 March 2017. Available: <http://mashable.com/2016/06/07/whatsapp-last-seen/>
- Tsotsis, Alexia. "Telegram Saw 8M Downloads After WhatsApp Got Acquired." *Techcrunch.com News*, 14 October 2014. Web. 1 March 2017. Available: <https://techcrunch.com/2014/02/24/telegram-saw-8m-downloads-after-whatsapp-got-acquired/>
- Tumarkin, Robert, and Robert F. Whitelaw. "News or Noise? Internet Postings and Stock Prices." *Financial Analysts Journal*, vol. 57, no. 3, 1 May 1, 2001, pp. 41–51: doi:10.2469/faj.v57.n3.2449.

- Tung, Liam. "Spamhaus: Uptick in Tor-Using Botnets May Force ISPs to Block All Tor Traffic." *CSO Online Technology Blog*, 24 January 2017, <http://www.cso.com.au/article/613097/spamhaus-uptick-tor-using-botnets-may-force-isps-block-all-tor-traffic/>
- Turing, Alan M. "Computing Machinery and Intelligence." *Mind*, vol. 59, 1950, pp. 433-460.
- Warman, Matt. "Mark Zuckerberg: Facebook Founder Admits 'Bunch of Mistakes' amid Privacy U-Turn." *The Daily Telegraph*, 30 November 2011. Web. 4 March 2017. Available: <http://www.telegraph.co.uk/technology/facebook/8924714/Mark-Zuckerberg-Facebook-founder-admits-bunch-of-mistakes-amid-privacy-u-turn.html>
- Wen, Howard. "Five Best Free Ways to Sync Your Data with the Web." *IT Business*, 26 July 2010. Web. 23 March 2017. Available: <http://www.itbusiness.ca/news/five-best-free-ways-to-sync-your-data-with-the-web/15183>
- Wessels, Bridgette. "Identification and the practices of identity and privacy in everyday digital communication." *New Media & Society*, vol. 14, no. 8, December 2012, pp. 1251-1268.
- Westby, Jody R. *International Guide to Privacy*. Chicago, IL: ABA Publishing, 2004.
- Westerkamp, Hildegard. "Listening and Soundmaking: A Study of Music-as-environment." MS. Ottawa: National Library of Canada. Simon Fraser University, Jan. 1988.
- WhatsApp. "Facebook." *WhatsApp Blog*, 7 January 2017. Web. 1 March 2017. Available: <https://blog.whatsapp.com/499/Facebook>
- WhatsApp. "Legal Information." *WhatsApp Blog*, 3 August 2015. Web. 1 March 2017. Available: <https://www.whatsapp.com/legal/?doc=privacy-policy&version=20120707>
- WhatsApp. "Looking Ahead for WhatsApp." *WhatsApp.com Blog*, 24 April 2014. Web. 1 March 2017. Available: <https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp>
- Wiener, Norbert. *Cybernetics: or Control and Communication in the Animal and the Machine*. Second Edition. Cambridge, MA: The MIT Press, 1965.
- WikiHow. "How to Know If Someone Has Blocked You on WhatsApp." *wikiHow*. Web. 5 March 2017. Available: <http://www.wikihow.com/Know-if-Someone-Has-Blocked-You-on-WhatsApp>
- Wolpert, Stuart. "Predictive policing substantially reduces crime in Los Angeles during months-long test." *UCLA Newsroom*, 7 October 2015. Web. 3 April 2017. Available: <http://newsroom.ucla.edu/releases/predictive-policing-substantially-reduces-crime-in-los-angeles-during-months-long-test>

Yarow, Jay. "Facebook Employee: Mark Zuckerberg 'Doesn't Believe' In Privacy." *Business Insider*, 28 April 2010. Web. 2 March 2017. Available: <http://www.businessinsider.com/mark-zuckerberg-doesnt-believe-in-privacy-2010-4>

Zapier. "Connect Dropbox to Google Analytics Integration." *Zapier*. Web. 23 March 2017. Available: <https://zapier.com/zapbook/dropbox/google-analytics/>

Appendices

Appendix A: Tor Anonymity Protocol Vulnerability Disclaimer

Staying anonymous

Tor can't solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want the sites you visit to see your identifying information. For example, you can use [Tor Browser](#) while browsing the web to withhold some information about your computer's configuration.

Also, to protect your anonymity, be smart. Don't provide your name or other revealing information in web forms. Be aware that, like all anonymizing networks that are fast enough for web browsing, Tor does not provide protection against end-to-end timing attacks: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit.

This reminder appears on the Tor overview page, and can be found at <https://www.torproject.org/about/overview.html.en#stayinganonymous>

Appendix B: Tor User Browsing Habit Warning

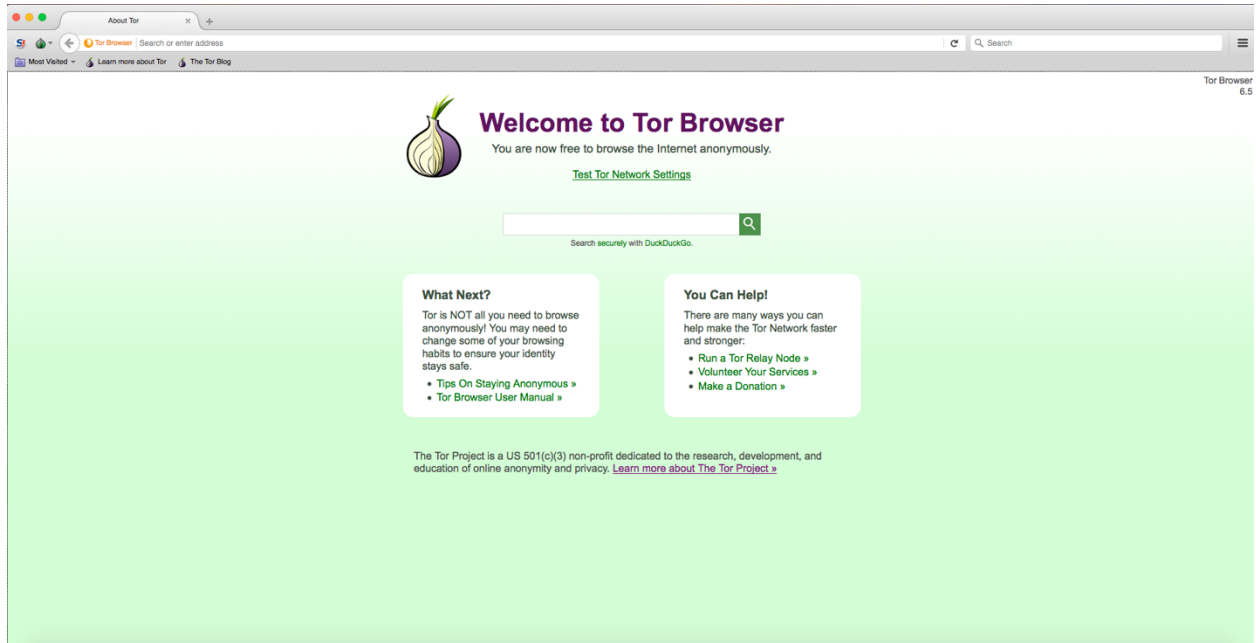
What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

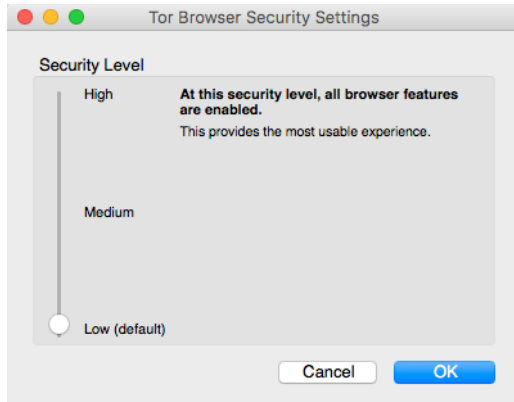
- [Tips On Staying Anonymous »](#)
- [Tor Browser User Manual »](#)

This warning is the first to appear on the loading page of the Tor browser on a desktop or laptop for both Windows and Mac based computers.

Appendix C: Tor Browser Startpage

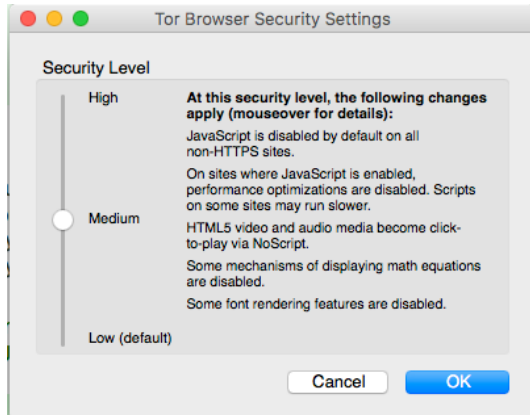


The Tor standalone browser for PC and Mac. Note the 'green onion' icon to the left of the browsing bar, which enables access for users to control the 'level' of security. Detailed in appendices four through six.

Appendix D: Tor Browser Security Setting – Low

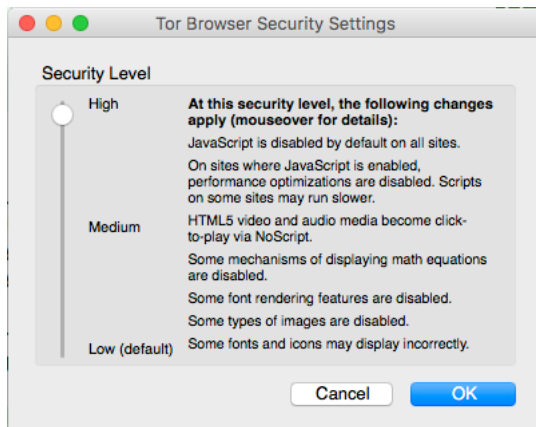
Tor's lowest security setting.

Appendix E: Tor Browser Security Setting – Medium



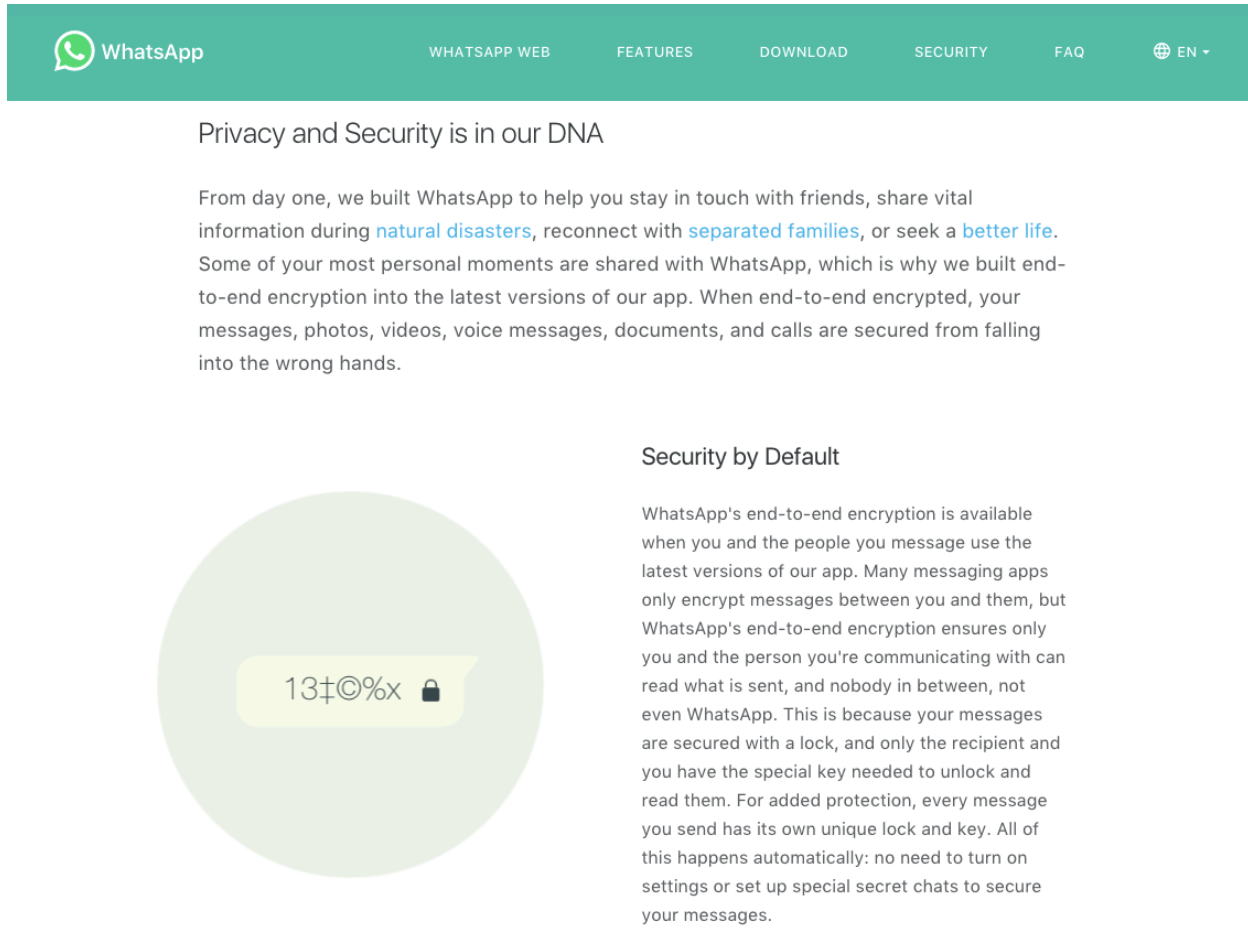
Tor's middle security setting.

Appendix F: Tor Browser Security Setting – High



Tor's highest security setting.

Appendix G: WhatsApp ‘Encryption by Default’ Advertisement

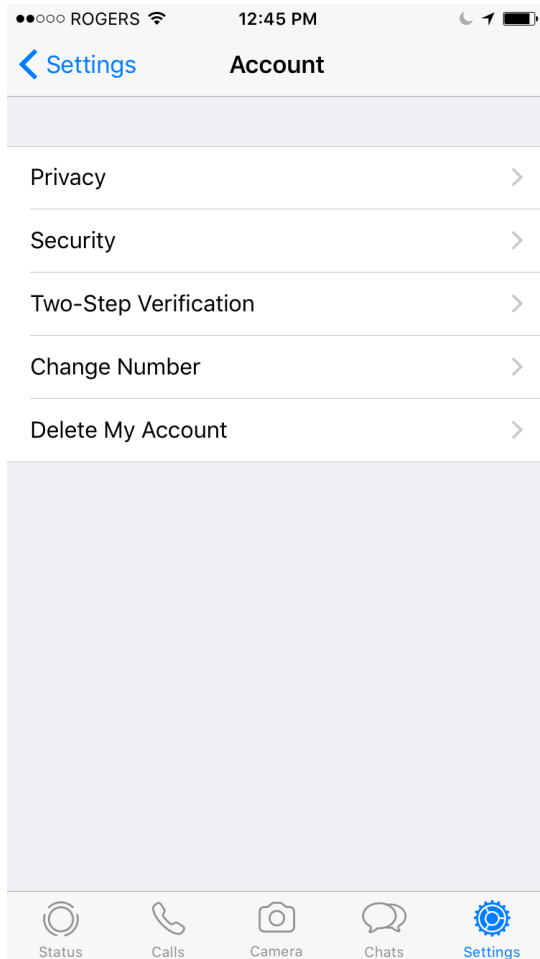


The image is a screenshot of the WhatsApp website's 'Security' page. At the top, there is a green navigation bar with the WhatsApp logo and the text 'WhatsApp' on the left. To the right of the logo are several menu items: 'WHATSAPP WEB', 'FEATURES', 'DOWNLOAD', 'SECURITY', 'FAQ', and a globe icon followed by 'EN'. Below the navigation bar, the main heading reads 'Privacy and Security is in our DNA'. The text below this heading states: 'From day one, we built WhatsApp to help you stay in touch with friends, share vital information during [natural disasters](#), reconnect with [separated families](#), or seek a [better life](#). Some of your most personal moments are shared with WhatsApp, which is why we built end-to-end encryption into the latest versions of our app. When end-to-end encrypted, your messages, photos, videos, voice messages, documents, and calls are secured from falling into the wrong hands.'

Below the text is a large light green circle containing a white speech bubble with the text '13†©%x' and a small black padlock icon. To the right of this graphic is the section header 'Security by Default'. The text under this header reads: 'WhatsApp's end-to-end encryption is available when you and the people you message use the latest versions of our app. Many messaging apps only encrypt messages between you and them, but WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp. This is because your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. For added protection, every message you send has its own unique lock and key. All of this happens automatically: no need to turn on settings or set up special secret chats to secure your messages.'

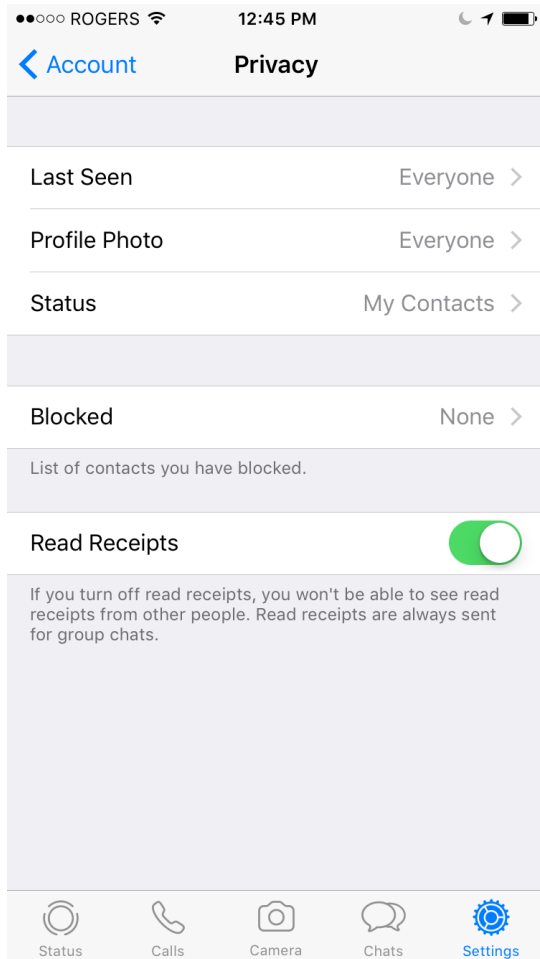
WhatsApp's security information page as seen on their website and within the mobile version of the app.

Appendix H: WhatsApp Mobile 'App' Settings Menu



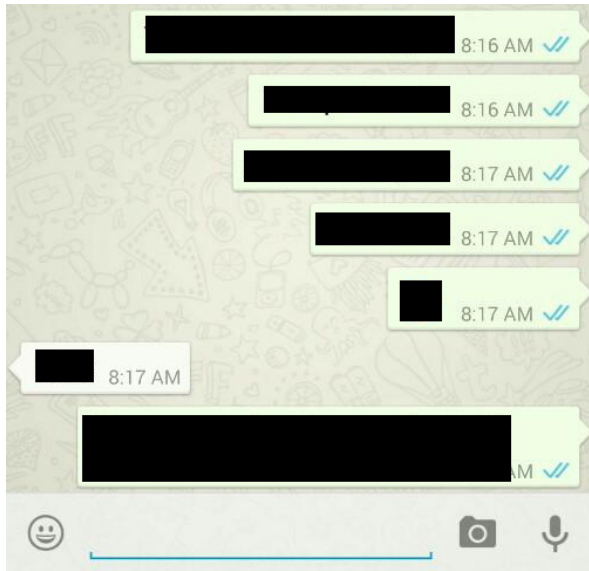
The first page of the 'settings' component of the *WhatsApp* mobile app.

Appendix I: WhatsApp Privacy Settings Submenu



The 'privacy' settings page.

Appendix J: WhatsApp Mobile 'App' Message Status System

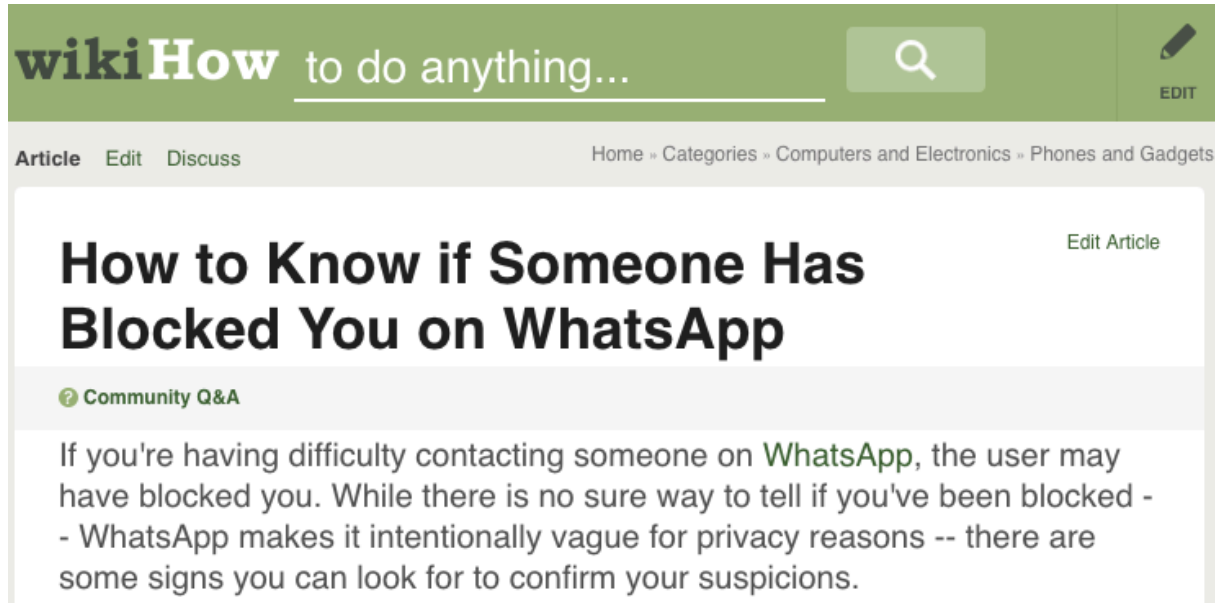


Check marks will appear next to each message you send. Here is what each one indicates:

- ✓ message successfully sent.
- ✓✓ message successfully delivered to the recipient's phone.
- ✓✓ the recipient has read your message.

The 'message sent' and 'message received' indicators on the *WhatsApp* mobile app.

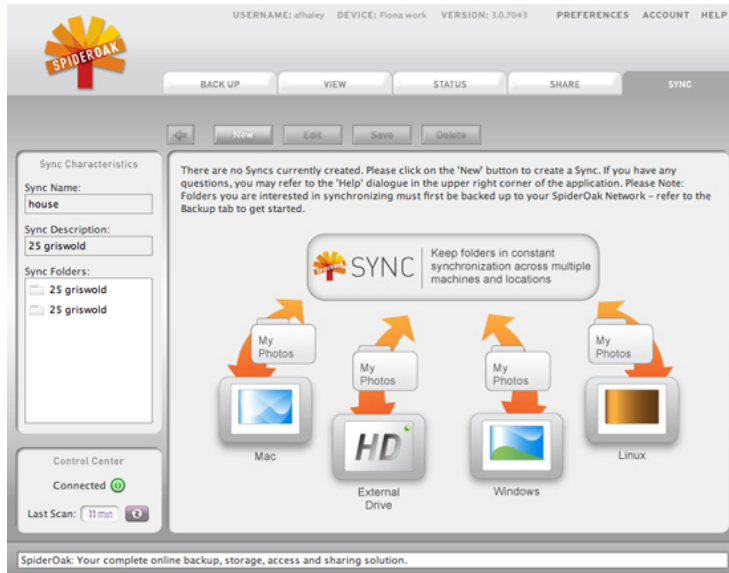
Appendix K: 'WikiHow' – 'How to Know if Someone Has Blocked You on WhatsApp'



The image shows the top portion of a WikiHow article page. At the top is a green header with the 'wikiHow' logo and the tagline 'to do anything...'. To the right of the logo is a search bar with a magnifying glass icon and an 'EDIT' button with a pencil icon. Below the header is a navigation bar with links for 'Article', 'Edit', and 'Discuss', and a breadcrumb trail: 'Home » Categories » Computers and Electronics » Phones and Gadgets'. The main content area features the article title 'How to Know if Someone Has Blocked You on WhatsApp' in large, bold black text. To the right of the title is a link that says 'Edit Article'. Below the title is a section labeled 'Community Q&A' with a question mark icon. The text of the Q&A entry reads: 'If you're having difficulty contacting someone on WhatsApp, the user may have blocked you. While there is no sure way to tell if you've been blocked - - WhatsApp makes it intentionally vague for privacy reasons -- there are some signs you can look for to confirm your suspicions.'

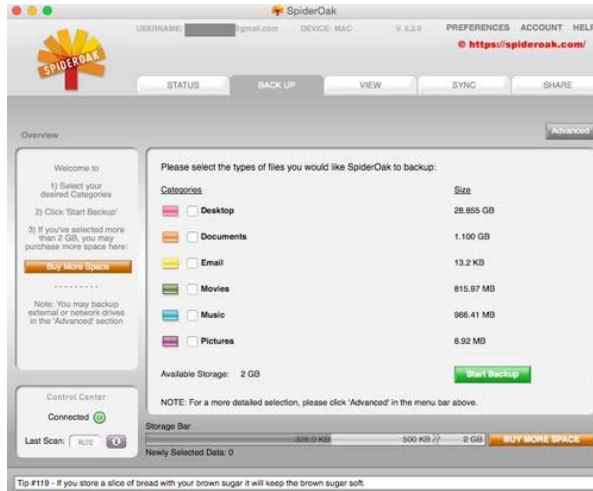
The header of the *WikiHow* page that instructs users via a 11-step process on how to discover whether or not another user blocked them on the *WhatsApp* mobile app.

Appendix L: *SpiderOak One* Version 3.0; Multiplatform Synchronization Advertisement



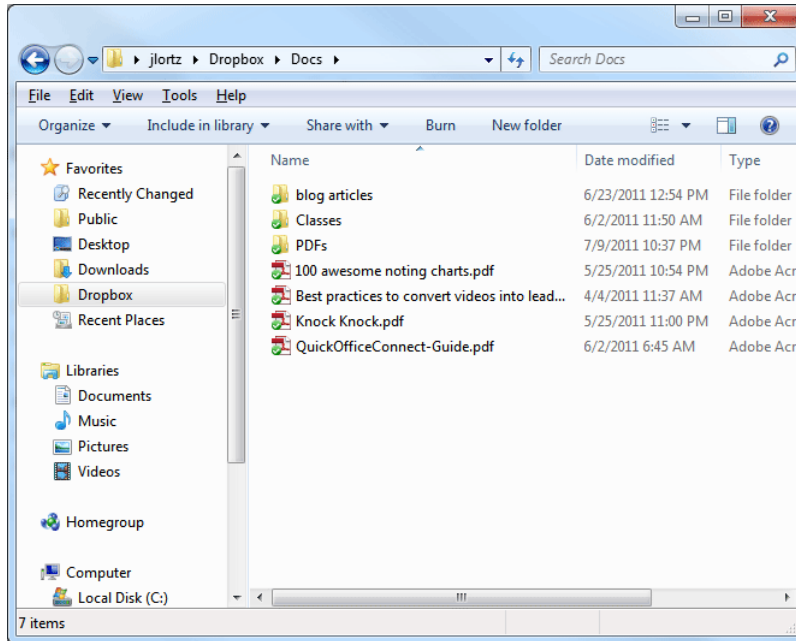
The third version of *SpiderOak One*, advertising to users the ability to sync files across different platforms and operating systems simultaneously (Windows to Linux, for example).

Appendix M: SpiderOak One Version 1.0; Original Release, 2007



The original release of *SpiderOak One*, version one from 2007.

Appendix N: DropBox – File Synchronization Status System



The current PC-based version of *DropBox*. The ‘green check marks’ indicate that a file has been successfully synced. They begin as blue during the upload process. Red circles indicate the file was not successfully uploaded.
