This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Security, Power, and Digital Privacy

https://www.e-ir.info/2015/04/30/security-power-and-digital-privacy/

THOMAS N. COOKE, APR 30 2015

Growing trepidation over the proliferation of ubiquitous surveillance increasingly resonates as a plea for further scholastic sanctification of digital privacy. When thinking about, with and through security and power online, digital privacy tends to be imagined as a container – a concept that receives meaning through its victimization by reckless tracking, invasion and profiling techniques conducted by security and surveillance regimes across the globe. The very intelligence leaks that instruct our observations about such developments indeed open numerous research opportunities to generate comprehensive, robust and novel understandings of such abuses upon digital privacy. But no matter what insight is garnered through our most critical explorations, digital privacy is becoming dead weight. A consequence not merely of how security and power unfurls on the Internet, but of how we as researchers frame that unfurling. As boundary-pushing literature continues to chart new intellectual terrain through which we understand the stakes of spying in the twenty-first century, we must reflexively ask: What of digital privacy's agential capacity? Can digital privacy be theorized as actively as its neighboring vertices, or will it continue to be a conceptual casualty of rescuing research? To release the politically expressive capacities of digital privacy, the short intervention explores the ontological capacities of anonymity software – specifically *Yale University* and *UT Austin*'s *Dissent* project.

Decades of scholarship have taken seriously the ramifications of security and power upon digital privacy. From Alexander and Pal's (1998) work exploring the affects of Internet life upon the routine function of government, or Bennett and Grant's (1999) concerns over the impacts of Internet politics upon dated privacy policies, to Nissenbaum's (2009) call for contextual integrity when circumnavigating privacy and power problematics and *Transparent Lives: Surveillance in Canada* (2014) project, much tremendously influential privacy-oriented scholarship has charted considerable conceptual terrain for thinking with, through and about the affects of security and power therein. The range of this social science literature, as complimented by and often dove tailing legal philosophical (Regan, 2000; Westby. 2004; Marcella, 2003) and computer sciences work (Acquisti, 2007), constellates for contemporary scholarship an array of catalysts charging Big Data and information domination preoccupations that demarcate routinized incursion and violation into popular understandings of digital privacy. Moreover, understandings of the acutely complex and subjective nature of digital privacy itself continue to burgeon, thus further problematizing definitional thinking about what is meant by 'digital privacy' – and for what and whom. These analytical strides are echoed by the impacts of the Snowden leaks upon our investigations (Bauman, Bigo, Esteves et al., 2014), thus further compelling calls for robust descriptive and prescriptive attitudes across the academy (Bellanova, 2014; Mitsilegas 2014).

One of the most compelling streams of analysis of security, power and digital privacy stems from surveillance studies and critical security studies literature. Amongst the array of remarkably elucidating interventions, such as de Goede and Amoore's 2014 research in the journal of *International Political Sociology*, numerous claims emerge over how digital privacy is increasingly violated in the name of predicting and pre-empting threats to national security – a familiar story in risk management (Muller, 2010; Peoples and Vaughan-Williams, 2010). Pushing beyond claims that ubiquitous surveillance is conducted by profiling individuals and their Internet behavior through the accumulation, sorting and calculation in the name of building 'data-doubles' so as to calculate risk potential (Elmer, 2003; Haggerty and Ericson, 2003; Bauman and Lyon, 2014), Amoore (2014) astutely delineates new conceptual ground. Whole datasets, such as emails, are not the *sole* object of ubiquitous surveillance – it is *fragments* of data, or *data derivatives* (Amoore, 2011), which agencies such as the United States National Security Agency (NSA) utilize for constructing security risk prediction scenarios. To Amoore, 'data' invokes thinking about pieces of information,

splintered and broken-off data floating across the Internet's pathways and marginalized at the peripheries of digital memory banks – those disaggregated from the body of lived experience and left behind by its practices, circulations and movements online. Through Amoore, how security, power and digital privacy triangulate deepens as we learn more about the ways in which novel security and surveillance power is deployed – by harnessing slivered information. Through Amoore, the perils of digital privacy also enlarge in ways previously unexpressed.

Alas, the more strides made by boundary-pushing critical scholarship, the more we inadvertently douse digital privacy in precariousness. As the depth of dangers over ubiquitous surveillance continue to descend through our research, we need to take seriously how our depth finding inadvertently constrains how we think about, with and through digital privacy itself. To be certain, our tracking of the trackers serves as signposts, signaling that the conceptual interplay between security and power leaves little room for creatively theorizing about digital privacy. And so, scholarship compensates by finding new ways to sanctify digital privacy; novel diagnoses inspire novel prescriptions for personal information violations, whether calls for re-imagining digital privacy itself, or by begging bureaucrats, politicians and policy writers to get creative. Nevertheless, it seems as though digital privacy may become nothing more than a container of security and power – responsive, not progressive. So how might we re-invigorate thinking about security, power and digital privacy?

By wondering about the ontological dimensions surrounding digital privacy itself. The paper *wonders*, as Lobo-Guerrero (2014) so deftly endeavors, about how an *object-oriented* ontology – applied upon an otherwise unsuspecting artifact – might alter the role of digital privacy in its relation to security and power. An object-oriented ontology is an approach inspired through the sociology and philosophy of science and technology. It asks a researcher how objects and things have agency unto themselves. In actor-network theory, a framework that invokes precisely these logics, non-human objects are incorporated into how we understand the 'social' and social life (Latour, 2005). The idea is to debase anthropocentric impulses and flatten the hierarchy of social interactions, thereby ensuring that the establishment of links between objects/objects, objects/humans, humans/humans are clearly legible (Hodder, 2012). The move obliges the researcher to ponder how objects gather together and render new spaces for association. Lights *illuminate* rooms, pavement *wears* rubber and wind *displaces* seed, active verbs reveal how objects mediate life. Objects authorize, allow, afford, encourage, influence, preclude, permit and to suggest how objects/humans relate to and act upon, with and through one another. To wonder about the ontological dimensions of the object-worlds of ubiquitous surveillance, such as anonymity and privacy-enhancing software technologies, is to wonder about how they *obfuscate*, *impede* and *striate* data flows on their own terms.

Meet *Dissent*: an open-source, community-based software project founded by collaborative work conducted between *Yale University* and *UT Austin*. *Dissent* is a group-based Internet communication system designed to enable its users to browse and communicate as one might on a web browser – just anonymously. What makes *Dissent* a novel intervention into the world of anonymous Internet communications is *how* it provides anonymous communication. Rather than facilitating anonymous Internet browsing and communication individually, *Dissent* facilitates such activities solely in groups. One of the rationales for a group-based design is how it guarantees anonymity. Through groups of networked computers sharing *Dissent* software, *Disssent* performs a process of checks and balances – a process that commits each individual computer to guarantee to one another that it is indeed a member of the group and not an adversary in disguise. The process, called *dining cryptography* (DC-Net), is also where inspiration is located for ontologically re-invigorating how we imagine security, power and digital privacy.

A *DC-Net* is a protocol that allows each member of a *Dissent* network to send anonymous messages across the Internet or to one another once a guarantee of anonymity can be established for all given members (Chaum, 1988). The rationale for doing so is to reassure each member of the group that all members will indeed remain anonymous in their communications (Feigenbaum and Ford, 2013). This is a particularly pertinent requirement in a day and age where fear of adversarial hacking or governmental spying is pervasive. Dining cryptography is named as such for the way in which it tends to be explained in the computer sciences, and is also useful here for understanding precisely why this protocol is charged with so much conceptual creative capacity for re-invigorating how we approach our research triangulation. Imagining that three cryptographers are dining together at a restaurant, the nature of their preoccupation and discussion over dinner is highly sensitive – so much so that the dining colleagues are concerned that an NSA agent is watching them from across the room. At the end of the meal, the waiter informs the group that

someone paid for their meals. Suspicious that it could have been the NSA agent trying to play with their minds, the cryptographers agree upon a protocol to determine whether or not it was one of them or the NSA agent who paid. The catch is that the protocol must respect each cryptographer's desire to remain anonymous throughout the process – how can they prove to each other that one of them had indeed paid, and not the NSA agent? The protocol thus begins by having each pair of cryptographers exchange coin tosses between one another. With three cryptographers seated at the table, three separate coins are required and three coins will be tossed in total. Each pair of diners tosses a coin, and each cryptographer of each pair silently records the outcome of the coin toss on their napkin. If "heads" were a result, each cryptographer would record a binary integer of "1", whereas "tails" results in the binary integer of "0". Once all coin tosses and results have been recorded, the group shares the results and balances the integers.

Two outcomes are particularly important. In the event that one of the cryptographers indeed paid for the meal, that cryptographer would write down the opposite or inverse of the outcome of her coin toss – thus indicating that she wanted to declare a message: "I paid, stop worrying." Like adding without carrying over the number after the "=" sign, the idea here is that an outcome of "1" will be produced collectively when one of the cryptographers inverses her coin-toss outcomes. Simply speaking, all of the "1s" and "0s" are treated as binaries – they ought to cancel each other out *except* in the case that a cryptographer wanted to anonymously declare that she paid for dinner. In the second outcome, all binaries indeed cancel each other out, resulting in a collective outcome of "0" and thus indicating that none of the cryptographers had a statement to declare. No one at that table paid for dinner – it was the NSA agent.

In the applied, computer scientific sense of the analogy, the NSA agent is merely an impetus for the group wanting to create a protocol. The practiced application of the coin tossing process is how *Dissent* allows each member of the group to *declare* whether or not they want to send a message to one another or across the Internet. As "1s" and "0s" are exchanged between computers in a group, so long as the process always balances to zero, the *Dissent* system verifies that the computers and their users are all trustworthy but that none of them at that given point in time desires to send anything across the Internet. The process recursively occurs, regardless of whether or not any user/computer desires to browse or communicate across the Internet, as it serves to constantly verify that no hackers or adversaries are interfering with the process. When a member of the group decides to browse or communicate, that coin toss process will record variations in the binary outcomes, thus allowing that computer/user to proceed anonymously.

What is important to ascertain about this process is not to concern one's self with fully comprehending the mathematics. Rather, it is to squint – to look at the process and observe the ways in which the coin toss process itself is *generating and exchanging data fragments between computers, bit by bit.* Each time a pair of computers exchanges virtual "coin tosses" with one another, mere bytes of data are being sent between computers. To look at this sort of data on a screen can be likened to seeing series of random "1s" and "0s" – data that would otherwise seem relatively meaningless. These numbers represent the creation and exchange of "keys" throughout the network – keys that allow the network to declare *when* a member wants to send a message anonymously. The idea here is to actively imagine how *Dissent* connects thousands of computers in a group, and unifies them to other *Dissent*-enabled networks, by exchanging fragments used merely to verify when and if people want to talk (Wolinsky et al., 2012). Simply speaking, *Dissent* performs by inscribing agential capacity into data fragments, *striating* flows of fragments, *identifying* and *impeding* adversarial data flows by injecting the network's pathways with balancing integers, and *obfuscating* identities by flooding the Internet with otherwise meaningless bits of data.

It does seem odd to imagine anonymity software as providing privacy. However, it is evident that *Dissent* provides its users private refuge – to protect their personal information and Internet behavior – by hiding in numbers. Digital privacy here is not articulated as an individual experience, but as a capacity *realized* through collective interaction (Ispareh and Ladani, 2009) – which is, unto itself, a novel intervention in existing conceptual frameworks of digital privacy protection and enforcement (Regan, 2000). Simply put, *Dissent* makes anonymity a *precondition* for privacy and as such, re-balances the relationship between security, power and digital privacy altogether. Rather than attribute 'power' and 'security' as beholden to the perpetrators of ubiquitous surveillance, one might approach the triangulation with more weight given to 'digital privacy'. By operationalizing the kinds of data fragments that even the most contemporary privacy and surveillance literature otherwise may belief to be dead weight or simply targets of

profile building, *Dissent* empowers digital privacy. Consequently, *Dissent* challenges how we understand 'security' as well for the "coin toss" process is unto itself a practice that identifies, insulates and thwarts adversarial attacks and interventions – a contribution to our frameworks of digital security life from an oppositional attitude towards ubiquitous surveillance, one that liberates tendencies to imagine digital security life as at the mercy of adversarial perpetration. To approach the security, power and digital privacy triangulation through *Dissent* means that we, perhaps, use 'digital privacy' as a conceptual starting point in the research triangulation – an intellectual re-positioning that embraces a shift in perspectival attitude when understanding the worlds of power, security and digital privacy.

Notes

NB: My gratitude to Matt Harker, Commissioning Security Editor from E-IR, for the invitation to contribute this piece, and sincerest thanks to David Isaac Wolinsky, Research Scientist at Yale University and a Project Leader of *Dissent* for his painstaking efforts in editing and explaining complex technical matters, of which I could not successfully navigate without his help. Sincerest thanks to Jason Chan, Julie Cumming and Benjamin J. Muller for their comments in supporting and finalizing this intervention as well. Their assistance echoes numerous mutually beneficial ongoing conversations about surveillance, programming and privacy theory.

References

Acquisti, A. et al. Eds. 2007. *Digital privacy: theory, technologies and practices.* New York, NY: Auerbach Publications.

Alexander, Cynthia and Leslie A. Pal. Eds. 1998. *Digital Democracy: Policy and Politics in the Wired World.*

Amoore, Louise. 2011. "Data Derivatives: On the Emergence of a Security Risk Calculus for our Times" in*Theory, Culture & Society* (28)6: 24-43.

Amoore, Louse. 2014. "Security and the Claim to Privacy" in *International Political Sociology* (1)8.

Bauman, Zygmunt and David Lyon. 2013. *Liquid Surveillance: A Conversation.* Cambridge, MA: Polity Press.

Bauman, Zygmunt and Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance" in *International Political Sociology* (8)2: 121-144.

Bellanova, Rocco, 2014. "Data Protection, with Love" in *International Political Sociology* (8)1: 112-115.

Bennett, C. J. Ed. 2014. *Transparent Lives: Surveillance in Canada.* Athabasca, AB: AU Press.

Bennett, Colin J. and Rebecca Grant. Eds. 1999. *Visions of Privacy: Public Choices for the Digital Age.* Toronto: University of Toronto Press.

Chaum, David. 1988. "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability."*The Journal of Cryptology*, (1): 65-75.

de Goede, Marieke, 2014. "The Politics of Privacy in the Age of Preemptive Security" in*International Political Sociology* (1)8: 100-104.

Elmer, Greg, 2003. *Profiling Machines: Mapping the Personal Information Economy.* Massachusetts: MIT Press.

Feigenbaum, Joan and Bryan Ford. 2015. "Seeking Anonymity in an Internet Panopticon." *DBLP-CS Bibliography*, Cornell University Library. V3 submitted on 3 January 2015.

Haggerty, Kevin D. and Richard V. Ericson, 2003. "The Surveillant Assemblage" in the *British Journal of Sociology* (51)4: 605-622.

Hodder, Ian, 2012. *Entangled: An Archaeology of the Relationships between Humans and Things.* Wiley-Blackwell.

Ispareh, Marzieh and Behrouz Tork Ladani, 2009. "A Conceptual Framework for Specification, Analysis and Design of Anonymity Services." Published in: Proceedings of the 2009 *EDBT/ICDT Workshops*: NY, New York: 131-138.

Latour, Bruno, 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory.* London: Oxford University Press.

Lobo-Guerrero, Luis, 2014. "Wondering as Research Attitude" in Mark B. Salter and Can E. Mutlu (eds)*Research Methods in Critical Security Studies: An Introduction.* London: Routledge.

Marcella, A. J. 2003. *Privacy Handbook: guidelines, exposures, policy implementation and international issues.* Hoboken, NJ: John Wiley & Sons, Inc.

Mitsilegas, Valsamis, 2014. "The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance" in *International Political Sociology* (8)1: 104-108.

Muller, Benjamin J., 2010. *Security, Risk and the Biometric State: Governing Borders and Bodies.* NY, New York: Routledge.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford: Stanford Law Books.

Peoples, Columba and Nick Vaughan-Williams, 2010. *Critical Security Studies: An Introduction.* NY, New York: Routledge.

Regan, Priscilla M. 2000. *Legislating Privacy: Technology, Social Values and Public Policy*. North Carolina: University of North Carolina Press.

Westby, J. R. 2004. *International guide to privacy.* Chicago, IL: ABA.

Wolinsky, David Isaac and Henry Corrigan-Gibbs, Bryan Ford, Aaron Johnson. 2014. "Dissent in Numbers: Making Strong Anonymity Scale." Presented at the *10th USENIX Symposium on Operating Systems Design and Implementation (OSDI '12)*, 8-10 October, 2012, Hollywood, CA.

About the author:

Thomas N. Cooke is an Adjunct Professor of Political Science at King's University College, PhD Candidate in the Communication & Culture program at York University and Student-at-Large Representative for the International Studies Association Executive Committee Canada. Cooke's research intersects privacy theory, design theory, algorithmic profiling, big data tracking, technoscience, surveillance studies and critical security studies. Cooke's dissertation explores how open-source privacy enhancing technology project design philosophies are fundamentally re-articulating popular understandings of digital privacy. You can follow him on Academia, and Twitter at @thomasncooke.