doi:10.1017/aju.2017.6

SYMPOSIUM ON CYBERSECURITY AND THE CHANGING INTERNATIONAL LAW OF DATA

GENERATIVE SECURITY: ADVERSARIAL DESIGN AND CONFLICT OF LAWS

*Niranjan Sivakumar**

Introduction

The data breach of the Democratic National Committee (DNC) during the U.S. presidential election of 2016 is multi-faceted and has wide ranging implications. The discourse of "cybersecurity" is increasingly thought of through the lens of states and other powerful actors like large corporations, as a conflict or war that is waged by specialized combatants while civilians are relegated to the sidelines and are the victims of digital malfeasance or the object of regulation and education from those in power.[1]

This essay opts instead for a ground-up view using concepts of participatory, adversarial design and hybrid knowledge production from the field of science and technology studies (STS) to argue for a serious consideration of nonhegemonic configurations of knowledge and power as a source for novel and creative contributions to some of the challenges faced in global cybersecurity. The inquiry begins with one discrete example of a technological artifact adopted as a response to the DNC data breach and uses this case to advocate both for a legal climate that fosters generative production of technologies from civil society and for an analogous generative jurisprudence to address questions of cybersecurity that adapts "hacker values" through techniques of private international law.[2]

The DNC Data Breach: Looking Below for a Solution

One major technique used in the breach of the DNC was a spear phishing attack.[3] This is a technique that relies on insecure properties of email to compromise a user's account by masquerading as a legitimate service provider.[4] While there is a technological aspect to this incident, a major component of the system compromise relied on "social engineering."[5] The actors affected by the data breach were relying on a communication system that was nearly five decades old. It was originally developed in cooperation with the U.S. Defense Department and later adapted for consumer use and implemented in this case by a prominent corporation.[6] As with any other

* *King's College War Studies Department and the Sciences PO Medialab.*

[1] *See generally,* Jon R. Lindsay, *Stuxnet and the Limits of Cyber Warfare*, 22 Security Stud. 365 (2013).

[2] Gabriella Coleman's ethnography of Debian developers articulates a set of values of free software hackers. E. Gabriella Coleman, Coding Freedom: The Ethics and Aesthetics of Hacking (2013).

[3] *Threat Group-4127 Targets Hillary Clinton Presidential Campaign*, Secure Works (June 16, 2016).

[4] Sean Gallagher, *Russia-linked phishing campaign behind the DNC breach also hit Podesta, Powell*, Ars Technica (Oct. 21, 2016).

[5] Lvxferis, *Hacking the mind for fun and profit*, 67 Phrack (Nov. 11, 2010).

[6] *See generally,* Janet Abbate, Inventing the Internet (1999).

technology, the tool embodied a set of politics and values, be it as a tool of communication designed to withstand a Cold War-era nuclear strike or highly recognizable cornerstone consumer product of an advertising-revenue driven Internet company.[7] However, what the tool distinctly lacked were features of security and privacy that were desirable to, and perhaps implicitly assumed, by its users in this incident.

When the breach of the email systems came to light, it was not surprising that DNC staffers and those working with the Clinton campaign turned away from email and instead to Signal,[8] a free (as in speech) messaging platform developed by a nonprofit organization established and run by hackers and activists.[9] Signal is a tool that pairs a sophisticated and state-of-the-art cryptographic protocol[10] with a user-friendly interface that is focused on the translation and communication of complex technical concepts in an accessible and intuitive fashion.[11] It is a tool that is designed with explicit politics that not only address the infrastructure on which it relies and the technological systems with which it interfaces, but also function as a reification of ethical and legal concepts. While Signal may not have been designed as a tool *for the state*, it is designed as a tool for *democracy* and fulfilled this role in an overt fashion for Democratic party actors.

Why not the "DNC Hack"?

The digital interference during the U.S. election is commonly referred to as the "DNC hack." This essay, however, purposefully avoids this terminology. While there are overlaps in techniques and methods between hackers and the agents involved in breaching the DNC (and other political institutions), there is little evidence that the actions of the latter share a set of values with what digital anthropologists like Gabriella Coleman and Christopher Kelty categorize as hacking or how many hackers themselves define their identities. These breaches of computer systems appear to fall under what Thomas Rid has identified as three types of political crimes: "subversion, espionage, and sabotage."[12] While hackers could be involved in such activities, they are not defining characteristics of hackers, and many that engage in and organize these political crimes are not hackers.

Design for Humans

Hackers consider social engineering to be a fundamental approach to compromising a system as "there is no patch for human stupidity."[13] It is a technique that is commonly employed by hackers for defensive and offensive purposes, particularly for activities like gathering privileged information about systems (human or nonhuman) with the intent to disseminate or "leak."[14] It is also important to note that this technique has often been seen as a the first step in the deployment of "advanced persistent threats" (APTs), a type of activity that should be distinguished from the actions of "ordinary" hackers. The context of the deployment of similar techniques by a trickster or a soldier or a spy are dramatically different.

There are, however, alternative ways to conceptualize failures of interfaces between artifacts and users. Experts in design, like Donald Norman, would argue that there is no such thing as "human stupidity" but only poorly

[7] Langdon Winner, The whale and the reactor: a search for limits in an age of high technology 19–39 (1986).

[8] Open Whisper Systems.

[9] *What is free software?*, GNU Operating Systems.

[10] *Double Ratchet Algorithm*, Github.

[11] Moxie Marlinspike, *Safety number updates*, Open Whisper Systems (Nov. 17, 2016).

[12] Thomas Rid, *Cyber War Will Not Take Place*, 35 J. Strategic Stud. 5, 15 (2012).

[13] Tony Bradley, *No patches for human stupidity*, Computer Crime Research Center (Jan. 23, 2006).

[14] Biella Coleman & Michael Ralph, *Is it a Crime? The Transgressive Politics of Hacking in Anonymous*, Soc. Text. (Sept. 28, 2011).

https://doi.org/10.1017/aju.2017.6 Published online by Cambridge University Press

designed artifacts that do not conform to human sensibilities.[15] While there may in fact be no patch for human stupidity that would completely eliminate social engineering as a phenomenon, it is a useful exercise to consider how systems can be better tailored and responsive to the needs of nonexperts. It may be strange to think of sophisticated political actors as lacking in expertise, but tasks mediated by new technologies can turn seemingly mundane interactions into sites of implicitly contested knowledge practices and expertise.

Signal is a tool that is designed based on the latter perspective: that users are not "stupid" but that they face information asymmetry in computer mediated communication that renders them more vulnerable to the risks of social engineering than when engaging face-to-face. This risk is mitigated in one way through the use of computer science to develop a cryptographic protocol that is specifically tailored for the case of message sharing. It is also mitigated through a serious anthropological engagement with the users of the system through user studies and ethnography that inform the development of an intuitive user experience and the translation of unintuitive mathematical concepts like "cryptographic fingerprints" into more easily understood concepts like "safety numbers."[16]

Hackers and the Law

In addition to their facility with clever applications of technology and manipulation of social psychology, hackers are also defined by their unorthodox legal aptitude. Some of the earliest examples of this are seen in the free software movement where hackers kept pace with a rapidly changing statutory and judicial environment concerning the application of patent and copyright law to software.[17] Hackers acquired knowledge of the law that rivaled that of trained lawyers but "hacked" it by operating as amateurs who could cleverly invert hegemonic juridical interpretations of the law.[18]

The hackers developing Signal too show a similar facility with legal concepts but now move beyond the discourses of copyrights and patents to incorporate those of human rights through the application of computer code to protect the freedom of expression and autonomy of citizens. This legal engagement is often cast as a dichotomy between a positive response by citizens to a repressive state (or other) power and abstract ideals that are well-intentioned but naively ignorant of practical security concerns.[19] The use of this technology in the United States to help protect a democratic process shows that it need not necessarily be either of those two interpretations but that such technologies can be used in innovative ways to directly bolster trust between citizens and the state.

Object-Oriented Democracy

One lens through which Signal can be considered is that which Bruno Latour has called "object-oriented democracy."[20] This is a concept that has ironically been appropriated by social scientists from computer science and is now applied back to computer science. Latour here takes an established notion in STS, that artifacts have politics, but contextualizes these politics based on the assemblages of actors and concepts that surround an object at a given time. The temporality of these configurations means that the politics of the given object are malleable,

[15] *See generally,* Donald A. Norman, The design of everyday things (2002).

[16] Marlinspike, *supra* note 11.

[17] *See generally,* Christopher M. Kelty, Two bits: the cultural significance of free software (2008).

[18] *See id.*

[19] Daniel Moore & Thomas Rid, *Cryptopolitik and the Darknet*, 58 Survival 7 (2016).

[20] Bruno Latour, *From Realpolitik to Dingpolitik or How to Make Things Public*, *in* Making Things Public: Atmospheres of Democracy 14 (Bruno Latour & Peter Weibel eds., 2005).

https://doi.org/10.1017/aju.2017.6 Published online by Cambridge University Press

which is to say that even if a tool like Signal may have been imbued at the outset with privacy-oriented, antiauthoritarian politics by its designers, its engagement in the context of the DNC data breach illustrates how the technology can in fact work *with* democratic institutions to safeguard rights.

The availability of such tools then becomes an important element of fostering and strengthening democratic society. While this is not designed to be a replacement for state institutions and intentionally constructed policy, it is an important corollary to conventional statutory and juridical methods of security regulation. Civil actors and amateurs engage in what Carl DiSalvo calls "adversarial design," a pluralistic engagement through the production, interpretation, and reinterpretation of artifacts and systems which results in the availability of a variety of tools and techniques that can provide utility or critique during crises or unforeseen circumstances.[21] Without such a pool of relevant objects to call upon, object-oriented democracy is merely an abstract concept without substance.

Contemporary methods of free software development also foster object-oriented democracy by creating participatory sites for engagement in not only code writing but also the sharing of politics and values. Signal, hosted on the popular code repository Github[22] and with a public mailing list,[23] presents a forum for public engagement with the technology and its developers, be it through the writing of code and reporting of bugs or suggestions for new features and discussions of legal concerns and implications of the technology's use.

Protecting a Generative Environment

The utility of Signal for defending a core institution of the American democratic process is a strong practical argument for the fostering of what Jonathan Zittrain has dubbed a "generative Internet."[24] The concept of "generativity" was developed in the context of concerns that the increasing "platformization" of the Internet acted as a dampener on the epistemic affordances provided by an unrestricted medium of communication and creation.[25]

Zittrain argues that security is an important consideration for preserving a generative Internet and that fear over a lack of security could result in users turning to appliance-like devices that limit their ability to create and express themselves.[26] He advocates the development of policies that encourage good "security hygiene" and are enforced through juridical and other means than the blunt instrument of computer code that limits technological affordances. Some recent proposals for cybersecurity frameworks take seriously this call to hygiene, with some explicitly being modeled after systems of public health.[27]

Maintaining this generativity through policy is important not only to foster the development of new technologies like Signal but also to create the conditions for a recursive participatory system that reinforces and amends policy through its own generativity. Activities like adversarial design and other forms of citizen science and technology are themselves critical processes for producing new policy-relevant knowledges that drive discourses and change.[28]

[21] Carl DiSalvo, Adversarial design (2012).

[22] *Open Whispers Systems*, Gitbub.

[23] *Whisper Systems*, Rise Up.

[24] Jonathan Zittrain, *The Generative Internet*, 119 Harv. L. Rev. 1974 (2006).

[25] This has been discussed in different ways by different scholars, Lessig argues through the lens of architecture in Lawrence Lessig, Code (2d ed. 2006), Kelty for recursive publics in Two Bits (Kelty, *supra* note 17), and Gillespie against the perils of platformization in Tarleton Gillespie, *The Politics of 'Platforms'*, 12 New Media & Soc'y 347 (2010).

[26] *See, e.g.*, Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514–1516 (9th Cir. 1992).

[27] Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 Daedalus 70 (2011).

[28] Aya Kimura & Abby Kinchy, *Citizen Science: Probing the Virtues and Contexts of Participatory Research*, 2 Engaging Sci., Tech. & Soc. 331 (2016).

https://doi.org/10.1017/aju.2017.6 Published online by Cambridge University Press

Hacker Jurisprudence

If we take seriously the project of an object-oriented democracy that relies on generativity, plurality, adversarial design, and the fostering of hacker values as an important civic venue for the production of new tools and knowledges about security and other important public discourses, then the legal questions raised by legal scholars like Zittrain, Lessig, Post, Cohen, Wu and others still remain to be answered. Not only questions of how to apply abstract legal concepts like jurisdiction to the Internet, but whether the Internet can be regulated at all through juridical means has been an ongoing debate for more than two decades. While this essay does not purport to answer these questions, it does engage with a thought experiment to begin designing a novel legal approach to the Internet.

The DNC turned to a technology steeped in hacker ethics to protect and support their engagement in a presidential election. If hackers can be counted on to help secure such a critical democratic process then it seems they could also provide inspiration to legal practitioners and scholars. Gabriella Coleman argues that hackers may be thought of as trickster figures from myth: cleverly disruptive, highly skilled, and privileging humor.[29]

A legal analogue incorporating these values could be derived from the discipline of conflicts of laws. While not yet a popular doctrinal approach in American courts, Canadian legal scholar Andrea Slane has advocated for a conflicts-based approach to Internet cases that is grounded in the materiality and technology of the Internet but resistant to hyperbolic claims of cyber-utopianism or dystopianism.[30] Slane addresses jurisdictional questions on the Internet through a "connecting factors method" that does not simplify the reach of law to a single factor such as receipt of content over the Internet or the physical location of computing equipment as championed by Goldsmith and Wu.[31] This approach is contextual and grounded in the particulars of a given case making it a good match to the shifting politics of an object-oriented democracy.

At a broader level, Karen Knop, Annelise Riles, and Ralf Michaels have proposed an "intellectual style" based on feminist jurisprudence in conflicts of laws.[32] This style captures the playful, clever, and irreverent ethos of the hacker, advocating for an "as if" modality of theorizing that uses legal fictions and technique as serious tools for conflict resolution. It also has a deep technicality that mirrors hackers' proficiency with code and their ability to deconstruct and repurpose a system. Just as a hacker might use a decompiler to take apart a program, Knop, Riles, and Michaels advocate for a technique called *dépeçage* which allows for the "slicing" of questions in a conflict and to reconfigure it to reach a pragmatic solution that engages with the values of civil society and specific individuals rather than escalating the conflict into an unwieldy deadlock between competing abstract normative systems. Such an intellectual legal style is an innovation commensurate with technological innovations for protecting rights and political innovations, like microdemocracy, for increasing citizen participation in politics.[33]

This style of jurisprudence is particularly needed for questions of cybersecurity. Security can often be at odds with the rights of citizens and flexible legal techniques are critical for avoiding otherwise irreconcilable conflicts between techniques of security, like surveillance and control, and citizens' rights to privacy, expression, and autonomy.[34] These legal techniques can function as a juridical analogue to participatory and adversarial design's function

[29] *See* Coleman, *supra* note 2.

[30] Andrea Slane, *Tales Techs and Territories: Private International Law, Globalization, and the Legal Construction of Borderlessness on the Internet*, 71 Law & Contemp. Probs. 129 (2008).

[31] Jack Goldsmith & Tim Wu, Who Controls the Internet?: Illusions of a Borderless World (2006).

[32] Karen Knop et al., *From Multiculturalism to Technique: Feminism, Culture, and the Conflict of Laws Style*, 64 Stan. L. Rev. 589 (2012).

[33] Malka Older, *Are We Heading Towards an Infomocracy?*, Tor (Nov. 8,2016).

[34] *See* Mulligan & Schneider, *supra* note 27.

https://doi.org/10.1017/aju.2017.6 Published online by Cambridge University Press

as a venue for engaging with citizens' alternative knowledge practices with respect to issues of security. Cultivating and using this intellectual style creates a set of legal "objects" in addition to adversarial technological artifacts.

Conclusion

This essay has argued for using the DNC data breach as an opportunity to engage with civil society in a participatory fashion rather than to set aside issues of cybersecurity as abstract issues relegated solely to the realm of diplomacy, statecraft, and war. This is not to suggest that participation is a substitute to other political measures but rather an important process by which emergent tools and techniques develop that could be to the benefit of various actors. A legal complement to a participatory, object-oriented democratic technological approach to security could be developed through novel approaches that embody a similar set of creative, flexible values.

https://doi.org/10.1017/aju.2017.6 Published online by Cambridge University Press