Secrecy and Society

ISSN: 2377-6188

Manuscript 1072

Technologies and Time Tempers: How Things Mediate a State's (Cyber Vulnerability) Disclosure Practices

Clare Stevens

Technologies and Time Tempers: How Things Mediate a State's (Cyber Vulnerability) Disclosure Practices

Abstract

State secrecy and disclosure practices are often treated as processes of intentional and strategic human agency, and as forms of political time management (Bok 1982; Horn 2011). Through a critical analysis of the United States government's disclosure practices in the context of their discourse around the cybersecurity "Vulnerabilities Equities Process" (VEP), this paper will present a two-fold argument against these conventional treatments of secrecy and disclosure. While government secrecy and disclosure can certainly be understood as a form of (agential) timing, orientation and control (Hom 2018), this paper will also show how government secrecy practices are emergent at the point of relations with the structuring (but not over-determining) temporalities of various technologies. More than just the procedural containment of information, in which time and technologies feature as passive substrates, the paper will instead help scholars explore the ways that technologies and their times actively mediate the production of secrecy, disclosure and knowledge. By shifting beyond linear conceptions of cause-and effect, the paper will therefore theorize the understudied but important temporal dynamics of disclosure, thereby allowing for richer conceptualizations of the role of digital technologies in contemporary secrecy practices.

Keywords

cybersecurity, disclosure, mediation, secrecy, technology, temporality, U.S. National Security Agency, Vulnerabilities Equities Process

Technologies and Time Tempers: How Things Mediate a State's (Cyber Vulnerability) Disclosure Practices

Clare Stevens[1]

Abstract

State secrecy and disclosure practices are often treated as processes of intentional and strategic human agency, and as forms of political time management (Bok 1982; Horn 2011). Through a critical analysis of the United States government's disclosure practices in the context of their discourse around the cybersecurity "Vulnerabilities Equities Process" (VEP), this paper will present a two-fold argument against these conventional treatments of secrecy and disclosure. While government secrecy and disclosure can certainly be understood as a form of (agential) timing, orientation and control (Hom 2018), this paper will also show how government secrecy practices are emergent at the point of relations with the structuring (but not over-determining) temporalities of various technologies. More than just the procedural containment of information, in which time and technologies feature as passive substrates, the paper will instead help scholars explore the ways that technologies and their times actively mediate the production of secrecy, disclosure and knowledge. By shifting beyond linear conceptions of cause-and effect, the paper will therefore theorize the understudied but important temporal dynamics of disclosure, thereby allowing for richer conceptualizations of the role of digital technologies in contemporary secrecy practices.

Keywords: cybersecurity, disclosure, mediation, secrecy, technology, temporality, U.S. National Security Agency, Vulnerabilities Equities Process

1 Clare Stevens is a Teaching Fellow in International Security with the University of Portsmouth. Her research is concerned with looking at the controversies and politics of defining "cybersecurity," including what those political efforts of definition can teach us more broadly about security, secrecy, and technologies in contemporary international security. Clare.stevens@port.ac.uk

Between 2013 and 2018, a series of cyber breaches and international cybersecurity incidents[2] prompted criticisms from diverse commentators outside of the U.S. government. As a result of these incidents, critics challenged the rationales and legitimacy of the government's use of software and hardware vulnerabilities[3] in the course of intelligence and law enforcement missions. As one critic described it, "the NSA – despite what it and other representatives of the U.S. government say – [is] prioritizing its ability to conduct surveillance over our security" (Schneier 2016). In response, government representatives and White House administration officials

2 These included the controversy around Edward Snowden, as well as technical incidents like the Heartbleed Vulnerability, and the leaking of NSA hacking tools by a group called Shadow Brokers, tools that were subsequently repurposed by North Korea to enable the WannaCry ransomware attacks in 2017. These incidents will all feature in the story this paper tells.

3 Vulnerabilities in this context refer to undiscovered flaws in the software and hardware that make up cyberspace. Such flaws can be present in the systems from the day of their launch: discovering all the potential bugs in the millions of lines of code in a piece of equipment or software is time-consuming and not always economically induced for the vendors. They can emerge as code, interfaces, and users interact and behave unexpectedly and unpredictably, resulting in bugs or "vulnerabilities." A bug is when a system isn't behaving as it's designed to behave. A vulnerability is a way of abusing the system (most commonly in a security-related way) - whether that's due to a design fault or an implementation fault. In other words, something can have a vulnerability due to a defective design, even if the implementation of that design is perfect." (StackOverflow, 2008). When vulnerabilities are unknown to the vendor or manufacturer, they are often referred to as "zero-day vulnerabilities," or "0-days," because developers have had zero days to address and patch the vulnerability. Not all vulnerabilities are problems, but when such bugs in coding and technical configurations can be intentionally exploited through research and the development of specifically tailored code ("exploits") then they can create the means for unauthorized access and modifications of systems. Knowledge of these vulnerabilities, as a precursor to hacking techniques, can thus be incredibly valuable. See Stack Overflow (2008) and Rapid7 (2022).

over the course of two administrations would gradually release details of an interagency deliberation process called the Vulnerabilities Equities Process (VEP). The VEP was designed as an interagency process to weigh up the risks against the benefits associated with government agencies discovering vulnerabilities in widely-used technologies, and the decision to keep them secret or to disclose them to manufactures to be fixed. Details of the existence and parameters of the procedure's justifications were articulated in terms of disclosures in the name of "transparency" and "accountability." The first White House Cybersecurity Coordinator, Michael Daniel (2014), reflected these motives in his explanation for the need to disclose details of the interagency process: "…[t]oo little transparency and citizens can lose faith in their government and institutions, while exposing too much can make it impossible to collect the intelligence we need to protect the nation."

Efforts to segregate governmental discovery and use of vulnerabilities from the risks they posed to wider society in this way was characteristic of a tendency to treat secrecy and disclosure in informational terms, one where the language of containment remains the most common imaginary used by politicians, policy experts, military strategists, scholars and the general public to make sense of (secrecy in) international affairs. Such an informational tendency also

assumes that the means of disclosure are followed by the ends of specifiable political outcomes. Here, processes of state secrecy and its related processes of disclosure are thought to be the results of human agency.

Disclosures, as a related and co-dependent element of secrecy practices, are thus treated in both everyday parlance and in politics as a necessary part of a linear process of knowledge transfer, automatically leading to predictable outcomes (such as trust, transparency, changes of behavior or in the case of this paper's focus, cybersecurity). State secrecy and their related practices of disclosure are often treated in this sense of strategic practical and intentional action, as a locking away (or releasing) of secrets to gain time, or forestall the ill-effects of time's passing, as a form of political time management (Bok 1982; Horn 2011). Even the NSA's mission statement reflects this conception of the need for secrecy and its activities as a form of strategic time management, highlighting how the NSA's role is to enable "computer network operations (CNO) in order *to gain a decision advantage* for the Nation and our allies under all circumstances" (U.S. National Security Agency 2018).[4] In the case of the VEP, the assumption is that segregating this knowledge can give the government a time advantage, can protect the autonomy of state

4 The phrasing of this mission statement changed sometime around 2018, reading now as "gaining a decisive advantage" (NSA, quoted in Manach 2018).

actors to carry out actions in the name of security, can protect the social order, and that trust or accountability, or *security*, will follow.

However, as the case of the contested role that disclosure plays in the case of the US government's computer network operations shows, human agency and efforts at timing are not the only factors that shape the symbolic or practical parameters of disclosure. How do we make sense of technological vulnerabilities, and of state secrecy practices that they are imbricated in, in ways that can help us move away from essentialized understandings of technological determinism, and away from framings (of temporal urgency) that suggest states must undertake particular (secrecy) practices because the technologies or external causative factors demand it? Rather than intentional timing efforts alone, it is also important to study how secrecy and disclosure practices (and the analytical approaches that study them) may be exceeding these linear conceptions of time and cause and effect. While building on the burgeoning literature in critical secrecy studies that has fruitfully demonstrated secrecy's productive effects, and moved us beyond understanding secrecy and disclosure practices in terms of cybernetic models of information transfer and anti-epistemology (Galison 2004), there is still more to be said about the concept of disclosure in itself. This is the contribution this paper seeks to make.

Rather than conceptualizing disclosure in terms of managing the visibility of self-evident data that speaks for itself, instead this paper will argue two things: firstly, rather than acting as passive substrates or overdetermining structures, technologies *mediate* the concept and practice of "disclosure," and secondly, that disclosure is a concept and practice that exceeds unified institutional (state or human) agency. While elements of secrecy and disclosure practices can certainly be described in terms of strategic agency on the part of state actors, this paper will also show how such practices are emergent at the point of relations with the structuring (but not over-determining) temporalities and affordances of various technologies. As this paper will show, what disclosure *means*, what it *does*, how it *works*, is a product – and productive – of the technologies and the temporalities that mediate its practice. Instead of a standalone moment, or a linear transformation of information from one state to another, disclosure can take place in more complex and partial ways. Disclosures are a process, not an event, knowledge processes that require effort and maintenance.

More than just the procedural containment of information in which time and technologies feature as passive substrates then, or as the result of instrumental and conscious decisions to make strategic disclosures that lead to predictable effects, the paper that follows will present an argument to help scholars conceptualize the ways that time

DOI: 10.55917/2377-6188.1072

and technologies actively mediate the production of secrecy, disclosure and knowledge.

To set the scene for this two-part argument, the paper will first theorize disclosure in more detail. Next, the paper will draw out in more detail the difference that technics and temporalities make to disclosure, both as a concept and as a practice. Finally, through a critical analysis of the United States government's disclosure practices in the context of their discourse around the cybersecurity "Vulnerabilities Equities Process" (VEP), the main section of the paper will demonstrate how in the context of computer network operations conducted by state agencies, disclosure as a concept and practice has changed over time. As well as showing how government secrecy can be understood as a form of (agential) timing, orientation and control (Hom 2018), time and technologies have simultaneously mediated how disclosure works, often as a result of the negotiations of people and groups.

Therefore, rather than considering secrecy solely as the "intentional concealment of information" (Bok 1982, 5), considering secrecy and disclosures in terms of processual flows allows a shift away from what tend to be agential or unitary actor-centered approaches to secrecy. Instead, the approach outlined here means to show how attending to different temporalities, and shifting away from conceptions

of secrecy-as-containment, has utility. By showing how government actors have struggled to demarcate those bugs and flaws in code as uniquely governmental, as property, and that they have had to adapt and adopt their approaches in light of external criticisms as much as the "leakiness" of the code, such an approach shows how hegemonic discourses of technological determinism, urgency, and state power, no longer look so certain.

Theorizing Disclosure

As a concept that is often twinned with secrecy, even in literature that views the two as mutually enhancing, constraining or stimulating each other (Birchall 2021), disclosures by state agencies are generally seen as intentional and instrumental. This may be as a means of visibility management (Flyverbom, et al. 2016), or of forestalling diplomatic or foreign policy matters (Carson 2015; Carnegie 2021; Aldrich and Moran 2018), where information is declassified or deliberately shared for strategic purposes. However, the trouble with these approaches is that they see information as synonymous with understanding. As Mark Fenster (2012, 757) incisively points out:

> such assumptions about information's essential, predictable effects rely on a mistaken understanding of what is a complicated administrative, political, and communicative process. Government information frequently has no obvious meaning. Its significance often creates significant political and social contest.

> It is sometimes misinterpreted; it is often ignored by all but a small minority of interested groups and individuals.

As a point that we shall return to shortly in more detail, all kinds of factors affect the reception of such information amongst different audiences. These factors are often well beyond the intentions of the authors of the disclosure or the authors of the original source material being disclosed, even at times containing "no obvious meaning" outside of the interpretive processes that must follow. As well as the "strategic proliferation of leaks, the announced use of covert and special ops, the use of 'preventive revelations'" described by Bratich (2006, 45), there is also work that has investigated the role of disclosures in terms of whistle-blowing and leaks beyond the strategic intentions of state actors (Ku 1998; Mistry and Gurman 2020; Coleman 2014; Gros et. al 2017).

More than simply critiquing some gap between the rhetoric and reality of transparency projects, work by scholars such as Birchall (2021), Bratich, and others has increasingly shown how treating secrecy in informational terms risks fetishizing transparency and disclosure effects (Fluck and McCarthy 2019), belying its situated and processual tendencies. As a means of moving beyond this informational tendency, recent work on government secrecy has emphasized the ways that secrecy should be seen as a productive and

dynamic set of practices and social relations (Maret 2016; Walters 2021; Kearns 2017; van Veeren 2019; de Goede and Wesseling 2017; Birchall 2021; Kearns 2021). Work by Bratich (2006) in particular calls on us to recognize the ways in which revelation is not necessarily the end of secrecy, but rather contributes to secrecy's displacement or proliferation through what he calls "spectacular secrecy." Here, disclosure is part of secrecy's continuation: although disclosure may be promoted as an act of greater government openness and is a feature of an "unprecedented visibility of secrecy," offers of disclosure instead obscure more than they reveal, making a spectacle of the secrecy without fundamentally addressing it (Bratich 2006: 495). Indeed, Bratich (2006, 493) suggests that in this contemporary moment, "disclosure might be part of secrecy's game, not an end to it." Revelation, or disclosures, are thus not mutually exclusive from secrecy, but are mutually constituted (Anaïs and Walby 2016).

However, disclosure in itself has been less explicitly theorized in this literature, except in its relations to secrecy and other concepts such as transparency and surveillance. In the context of the use of torture during the US' and its allies' "War on Terror" is Lisa Stampnitzky's (2020) important intervention that clarifies the conceptual and the political differences between exposure and revelation. By drawing from approaches critical of conceptions of

information and knowledge as synonymous, where meaning is supposed to be self-evident, a critique of approaches that imagine that truth simply exists "out there" (Stampnitzky 2020, 5), she is able to show the collective sense-making and recognition that are needed before an *exposure* of information becomes a politically salient *revelation* that leads to action or even accountability. Though information may be disclosed, she shows how informational models cannot explain why those disclosures do not have the intended effects, either for increased accountability under transparency ideals or at times for those strategically disclosing.

There are other, more undertheorized reasons, why disclosure may not have the predicted or intended effects, or why it may exceed the intentions of those acting in the name of disclosure. Controlling information and being able to make functional distinctions between "secret" and "disclosed" are based upon a widespread organizational culture within national security circles, especially in the US, which share the presumption that "secrets produce security" (Dean 2004). However, building upon critiques like Dean's, this article contends that it is not such a simple (or linear) relationship between secrecy and security. Rather than taking the claims of security imperatives stemming from fast-moving technological frontiers, or self-evident threats, for granted, a more explicit theorization of temporality

provides researchers of government secrecy (and security) some fruitful analytical purchase.

In many of the works cited so far, time and temporality are obvious and quantified externalities to the dynamics of secrecy and disclosure. For the most part to date, secrecy studies' treatment of the temporal has been limited to understanding secrecy (contained information) and its relation to revelation (uncontained information) as linear (Stampnitzky 2020; Fan and Liu 2022). As one of the few scholars to do so, Stampnitzky's work on the dynamic relations between secrecy, exposure, transparency and accountability for example has highlighted the importance of incorporating the possibility of change into our accounts of the *effects* of secrecy and disclosure (Stampnitzky 2020). Meanwhile, Fan and Liu (2022) have recently investigated the temporal character of secrecy for organizations through the constitution of archival records. However, more than just the role that timing has on the *effects* of secrecy and disclosures, or for organizations, the role of temporality in secrecy and disclosure regimes play a significant but largely undertheorized role (see Van Veeren et al, forthcoming).

That said, insofar as work has addressed temporality and anticipation, secrecy regimes are an important part of "gaining time." In this sense, secrecy is about managing time's damaging effects, what

Hom identifies as a problem that requires a solution, the "transcultural symbol of time as a malevolent force confronting human affairs" (Hom 2020, 9). Here, secrecy and disclosures can be thought of as a form of *timing*, used as a way to make sense of world events, a way of ordering change processes so that they become legible, contextualizable, sensible, and as such a productive strategy for state actors. As Eva Horn (2011) described the arcanum, secrecy as the locking away of information was "first and foremost a form of political time management," a temporary withholding of communication to facilitate a head start for political or military actions, or as a way of keeping options open (Horn 2011, 108). This is an important temporal element implicit in logics of secrecy, what she described as "the conservative power of secrets and secrecy," namely the ability to preserve the status quo, and as such "it is a force directed toward the present and the future in that it keeps open future possibilities" and "secures the here and now of the state." (Horn 2011, 108). Beyond this section of her formative arguments though, little explicit attention is directed to the role that time and timing have for making sense of secrecy and disclosure, or conversely of the role that secrecy practices have in making sense of the past, present and future. While secrecy and disclosure practices may be an effect of timing efforts, less has been said about time's effects on disclosure and secrecy.

As the later discussion on the VEP will show, and as set out by the introductory article to this special issue, shifting our understanding of technologies away from viewing them as passive substrates, or as the things being contained, is necessary in order to account for secrecy and disclosure as processes in and through time, rather than as linear sequences of cause-and-effect. As we will see, technologies-as-mediators are an example of how temporalities structure and modulate secrecy and disclosure practices, whilst also being constituted in and through those secrecy and disclosure practices, in a codependent manner. Contrary to many security discourses that posit external technological and temporal exigencies *determining* the ensuing political responses, a more nuanced (and less determinist) account emerges.

In the rest of this paper, a critical discussion of the Vulnerabilities Equities Process (VEP) will show how in the context of computer network operations conducted by state agencies, disclosure as a concept and practice has changed over time. At the same time, time and technologies have mediated how disclosure works, often as a result of the negotiations of people and groups, but also in ways beyond those strategic intentions. In the first part of Part Three we will see how disclosure was used instrumentally, both as a concept and in practice, to set procedural and practical parameters on disclosure in order to protect the autonomy of government agencies to look for and

to use vulnerabilities in networked computer systems. We will also see how disclosure as a signifier and as a practice was used differently as the basis for claims to legitimacy by different communities. As a result of contestations between representatives of state agencies on the one hand, and cybersecurity practitioners and civil rights advocates on the other, the second part will then show how federal actors have worked to constitute "disclosure" in particular ways. Beyond the strategic and instrumental action of state and non-state actors and their competing articulations of disclosure though, the second half of Part Three will show how technological vulnerabilities and the networked systems of which they are a part play an important structuring, though not overdetermining, temporal effect on secrecy and disclosure practices. This is important because by working to *translate* vulnerabilities into quantifiable entities that can be deliberated, rationalized and putatively unbiased, and by gradually constituting disclosure as a transitory concept rather than a binary state, this paper finds that these debates and their interplay through and with technologies have worked to redraw the political and procedural parameters of disclosure over time, as we shall now see.

The VEP and Contesting Disclosures

In response to Heartbleed[5] and WannaCry,[6] government representatives over the course of two administrations would use "disclosure" to articulate a vision of insecurity in which the use of vulnerabilities was in the name of "national security" and would not undermine broader conceptualizations of "cybersecurity." In 2014, the White House Cybersecurity Coordinator Michael Daniel took the unusual step of publishing a blog post to address the allegations. He set out the stakes of government involvement in exploiting vulnerabilities by articulating a boundary between the government's institutionalized use of such vulnerabilities and their use by adversaries. On the one hand, he argued that such vulnerabilities could be used as tools "…to collect crucial intelligence that could thwart a terrorist attack, stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks" (Daniel 2014).

5 "The Heartbleed bug [of 2014] allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users" (Synopsys 2020).

6 "WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computer, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them" (Fruhlinger, 2022)

Vulnerabilities in the hands of "hackers or other adversaries" were thus "more dangerous vulnerabilities" than the ones being used by the government. On the other hand, he recognized that retaining "a huge stockpile of undisclosed vulnerabilities" would leave the "Internet vulnerable and the American people unprotected" (Daniel 2014).

This was one of the most explicit acknowledgments that the government had made to date of its institutionalized uses of vulnerabilities during its lawful intelligence and law enforcement activities. While hyperbolic, by describing the whole internet as being vulnerable, and making references to stockpiles, Daniel was working to invoke historically resonant conceptions of the state's role as security provider. According to this logic, the government was historically responsible for protecting the American people, and managing vulnerabilities was to be an important component in that role. By articulating their traditional roles in this way, the administration was working instrumentally and strategically to buy time for their agencies to use these vulnerabilities.

Government actors would also use national security rationales to make the case for limiting the role of disclosures. Although "responsibly disclosing a newly discovered vulnerability is clearly in the national interest," Daniel (2014) highlighted how instrumental "this tool [was] as a way to conduct intelligence collection, and better

protect our country in the long-run." Hailing the use of vulnerabilities by federal agencies as like "so many national security issues," Daniel (2014) was conveying how they thought that this was a matter that the government had unique normative authority to act as an adjudicator for, suggesting that while "the answer may seem clear to some," the "reality is much more complicated." By invoking national security prerogatives, the implication here was that though "some" might disagree, the government were working to demarcate the legitimacy of using such vulnerabilities during their intelligence and law enforcement activities.

The administration thus drew a boundary between two positions: on the one hand was the government's commitment to the security of cyberspace more broadly – cybersecurity – and on the other were their national security prerogatives. Here, there was to be a "trade-off" (Daniel 2014) between disclosure of vulnerabilities and national security missions. Echoing Michael Daniel's depiction of the trade-off between cybersecurity and national security, Daniel's successor in the role of White House Cybersecurity Coordinator, Rob Joyce (2017) published a blog post that made the government's rationales for *limiting* disclosure explicit:

> Our adversaries, both criminal and nation state, are unencumbered by concerns about transparency and responsible disclosure and will certainly not end their own programs to discover and exploit vulnerabilities. Although I don't believe

> withholding all vulnerabilities for operations is a responsible position, we see many nations choose it. I also know of no nation that has chosen to disclose every vulnerability it discovers.

Despite the government's commitment "to promote resilience in the digital systems architecture," immediate or total disclosure was thus argued to be at the expense of pursuing adversaries who were unencumbered by such limitations (Joyce 2017). Joyce, like Daniel in the Administration before him, was here setting the parameters of disclosure in normatively laden and historically resonant terms of transparency and responsibility, so that national security was hailed as setting limits on requirements for limited and responsible disclosure, even if it was in the name of cybersecurity.

However, for commentators challenging the government's use of vulnerabilities and the deployment of disclosure as a concept to rationalize their use, disclosure was similarly used as a symbolic resource, but to contest the government's credibility and legitimacy. These were fundamentally opposing visions of what disclosure *meant*, what it *is* – whether it meant to patch, or to spy, based on either a technical conception of cybersecurity to secure cyberspace by fixing vulnerabilities, or on a political conception of cybersecurity to secure cyberspace by utilizing vulnerabilities for wider strategic ends (Nissenbaum 2005). For those self-described in the technical community concerned about the government's exploitation of

vulnerabilities in widely used systems, disclosure for patching was meant to be a constitutive part of cybersecurity. As one prominent security expert in this debate, Bruce Schneier (2012), had described the role of disclosure as "regardless of the motivations," the role of disclosure was to facilitate patching. This was because it was an important constituent to security more broadly: "…a disclosed vulnerability is one that - at least in most cases - is patched. And a patched vulnerability makes us all more secure." It was therefore on the grounds of disclosure's role that in 2012 the civil liberties non-profit group the Electronic Frontier Foundation (EFF) questioned the government's commitment to cybersecurity more broadly, stating that,

> If the U.S. government is serious about securing the Internet, any bill, directive, or policy related to cybersecurity should work toward ensuring that vulnerabilities are fixed, and explicitly disallow any clandestine operations within the government that do not further this goal. (Hofmann and Timm 2012)

In other words, the EFF was arguing that fixing vulnerabilities would be a key indicator of the government's commitment to cybersecurity more broadly. As Bruce Schneier (2016) later summarized, "[p]retty much uniformly, security experts believe we ought to disclose and fix vulnerabilities." By invoking a consensus of "we" amongst this technical community, and citing the expertise of this community of security professionals, Schneier was constructing boundaries around disclosure on the basis of the credentials of the

"experts" on the one hand, disputing the government's credentials on the other. As far as this security, privacy and policy advice community were concerned, they were arguing that the use of vulnerabilities for clandestine operations by government agencies would undermine the credibility and capability of the government's broader cybersecurity efforts, because *disclosure* was synonymous with *security*. The meaning of disclosure in itself, what it could *do*, was thus a site of contention.

For those challenging the government's uses of vulnerabilities for hacking, drawing the bounds of disclosure in the ways articulated by government actors was thought to be particularly challenging in this technologically mediated context. Harvard Law Professor Jack Goldsmith reflected on the difficulty of segregating and compartmentalizing the use of vulnerabilities when he observed that "every offensive weapon is a (potential) chink in our defense - and vice versa." Similarly, in response to WannaCry and Joyce's blog posts, a former principal technologist at the American Civil Liberties Union was reported as highlighting the risks that all users endure from unpatched vulnerabilities given that, "…[w]e all use the same technology. We all use the same laptops, we all use the same web browsers, we all use the same word processing programs" (Soghoian, quoted in Hopper and Waldman 2017). These observations were not restricted to those

outside of government: as the ranking Democrat on the House Intelligence Committee pointed out in the context of the NSA's use of vulnerabilities, cybersecurity was particularly challenging because "…[w]hen it comes to cyber in particular, the line between collection capabilities and our own vulnerabilities … is virtually non-existent" (Schiff, quoted in Nakashima 2016).

The technological and social challenge posed by government computer network operations was thus that they take advantage of software and hardware vulnerabilities that domestic civilians and organizations may also use: Schiff's argument was that government actors cannot so easily segregate or compartmentalize their actions in space or time as they might in other classified contexts. Statements such as these were each challenging the sources and criteria of the authority conferred by the Administration's claims to disclosure in the name of "national security." They challenged the argument that Federal government agencies were uniquely qualified to manage the knowledge of these vulnerabilities as though they had direct equivalence with conventional weaponry and other matters of national security. Furthermore, government agencies did not have a monopoly on these secrets or their disclosure.

As we shall see in the next section's discussion of the ways that disclosure practices were mediated by and through these technologies,

government agency uses of zero-day vulnerabilities were not so easy to segregate from the security interests of wider technology users. The networked characteristics of the ecosystem which made hacking and exploitation possible and attractive by being so widely used around the world, were simultaneously the characteristics which meant government actors would continually struggle to compartmentalize and segregate vulnerabilities in a manner the state secrecy machinery could process with extant bureaucratic procedures, leading to the development (and the publicity) of the VEP.

Disclosure as Deliberative

Looking at the wording and the documents released through FOIA requests shows how the VEP set the parameters for the debate amongst multiple government departments internally and externally negotiating their competing mission interests, or "equities." Facilitating the process, the "National Security Agency/Information Assurance Directorate" would serve as the Executive Secretariat, and they would document, host, and maintain the regular meetings. The "Equities Review Board" was made up of representatives from several agencies who had submitted a vulnerability to the process or might have an interest in the vulnerability. The Points of Contact were tasked with "ensuring the applicable … equities of their organization" were

"appropriately represented in the process", which included cybersecurity, intelligence, counterintelligence and law enforcement equities amongst other listed mission interests (U.S. National Security Council 2010b, 5). Several agencies would have been involved in the process beyond the NSA, but aside from a redacted section describing the agencies involved, the unredacted agencies were described in more tentative terms in the 2010 policy document with the phrase "other participants may include" U.S. Departments of State, Justice, Homeland Security, Treasury, Commerce and Energy. This procedure was designed to be "…a comprehensive common policy and systematic process for handling the problem across the USG" (U.S. National Security Council 2010b, 2). By hosting regular meetings, turning the complexity and organizational breadth of these competing interests into a formalized procedure was therefore meant to impose some boundaries on the problem of vulnerability use and to set procedural parameters on who would be involved and when.

The procedure also set boundaries on disclosure by seeking to draw a symbolic as well as procedural line between dissemination and retention so that consensus was a simplified matter. To begin with, the purpose of the procedure was to build consensus amongst the range of government agencies. At this stage, the procedure was primarily concerned with setting parameters upon internal interagency

deliberations, but a by-product of these negotiations was what they called the decision "…to disseminate information pertaining to the vulnerability" (U.S. National Security Council 2010b, 8). At this stage in the procedure's existence, disclosure was not its main focus. The procedure was instead more concerned with institutionalizing a forum that would broaden deliberations to involve government agencies involved in vulnerability questions beyond the NSA. It was also to act as a formalized mechanism that would set the terms of those deliberations, and the 2010 VEP policy document spent the most time outlining those terms. The focus in the VEP policy was on procedural matters – who should attend, what kinds of clearances they must have, what the hierarchy of decisions were, the step-by-step process for electing vulnerabilities to the process, and the process for contesting decisions. In other words, deliberations were concerned first and foremost with assessing the internal equities of the different agencies and providing a platform for them to communicate information about vulnerabilities amongst themselves.

With a procedural focus on classified and uniquely governmental knowledge of vulnerabilities, this procedure was oriented around when to communicate *within* the U.S. government. As time passed though, and in response to the allegations (discussed above) that the government's actions were making cyberspace less secure, the

procedure would become more concerned with questions of when and why agencies should disseminate information to those *outside* the government.

To begin with, the procedure established parameters of dissemination in binary terms. According to the official guidelines in the 2010 policy, the Equities Review Board would reach a decision to disseminate, or to not disseminate. To the extent that the policy document stipulated what the ERB should consider as dissemination, the document contained an appendix of terms, where "external dissemination" (as opposed to dissemination amongst government agencies) was described as the "sharing or release of vulnerability information to entities external to the USG" (U.S. National Security Council 2010b, 12). Unlike later incarnations of the VEP, at this stage, there was no indication of temporary restrictions, or of a range of possible measures in between "disclosure" or retention. Depending upon the vulnerability in question, information about it would be disseminated to relevant cyber centers tasked with incident response or defensive network security, according to the sector in question. Even the terms used – dissemination, rather than disclosure as would be used later[7] – suggested a cybernetic model of information transfer,

7 According to *Collins American English Dictionary* "to disseminate information or knowledge means to distribute it so that it reaches many people or organizations"; to disclose means "to bring into view; uncover"; in insurance, "if you disclose

of senders actively distributing information rather than passively uncovering it or it needing interpretation (Stampnitzky 2020; Fenster 2015). The redacted information in the policy document may have indicated a more detailed range of vulnerability dissemination options to those "external to the USG" (U.S. National Security Council 2010a, 2010b), but given that the sections that remained redacted after review by the Office of the Director of National Intelligence in 2015 and 2016 were based on the government's desire to withhold information about offensive capabilities rather than defensive equities and the procedural parameters of dissemination (Hudson 2015, 2016; U.S. National Security Council 2010a), a more nuanced account of dissemination options is unlikely to have been in the redactions of this document.

By the time that Daniel made the blogpost in 2014, the language he used indicated a shift in how the procedure was constituting disclosure. There was now a more nuanced expression of the bounds of disclosure. In referencing this "…debate about whether the federal government should ever withhold knowledge of a computer vulnerability from the public," Daniel made reference to the *timing* of disclosure as a way of moderating the either-or position instituted in

information to an insurer, you provide information about a risk that may be relevant" – an interesting analogy given the VEP's later focus on categorizing and quantifying risks posed by government discovery and uses of vulnerabilities.

the early VEP-as-procedure. Describing the procedure itself as "…a disciplined, rigorous and high-level decision-making process for vulnerability disclosure," this interagency forum was concerned about when to "…*temporarily* withhold[..] knowledge of a vulnerability" and suggesting that there were "no hard and fast rules" for making these judgments (Daniel 2014, emphasis added).

While the *organization* of the Equities Review Board was instituted and disciplined in a rigorous way, the vulnerabilities themselves were more loosely bound in this procedure. Disclosure could be temporarily delayed, and categorizing the vulnerabilities was more done more flexibly than being subject to "hard and fast rules." Unlike the 2010 policy document, Daniel's 2014 blogpost also outlined the range of considerations that the review board subjected vulnerabilities to, including asking the question of whether they "… could … utilize the vulnerability for a short period of time before" it was disclosed – it could be temporarily exploited, and nor did disclosure prevent it from being exploited while patches were developed or as long as patches remained uninstalled on targeted systems (Hennessey 2016). The procedure's rationale was now beginning to reflect a more expansive range of what constituted disclosure.

The VEP is demonstrative of some of the unique challenges that government actors have articulated in bounding disclosure, in this

instance the distinctive problems of managing interfaces between "network" time and "bureaucratic" or "political" rhythms and time. Government actors and the VEP work to articulate the distinctive time pressures of maintaining secrets during cyberspace operations. In 2017 government actors acknowledged that the vulnerabilities cannot or will not remain secret forever, despite the government's best intentions or wishes. Rather than aiming to totally restrict knowledge of specific vulnerabilities that government agencies may discover, they inserted a new temporal element:

> …the VEP balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to *temporarily restrict* the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes. (White House 2017, 1 emphasis added)

Typical of this framing was Admiral Rogers' responses to advanced questions for his confirmation hearings as head of the NSA and CYBERCOM, where he told congress that "transparency can be ensured by establishing procedures" in "real-time," that leveraged "…technology that enables a transparent, policy-based, *machine-speed infrastructure*" (Rogers 2014a, 527, emphasis added). Here, "machine speeds" apparently stood in tension with the "political speeds" of interagency government processes, and the desire to pause or control the flow of knowledge for tactical or strategic reasons, even

temporarily. Disclosing and sharing information in "…a space this transformative and this disruptive" would challenge institutionalized practices that took place at political-speed (Rogers 2017, 2). This was expressed in the VEP as an articulation of distinctive time pressures of the role that disclosure played, where:

> …the VEP balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to *temporarily restrict the knowledge* of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes." (U.S. National Security Council 2017, 1, emphasis added)

By temporarily restricting knowledge, the VEP was intended to give the government a time advantage. As Michael Daniel had phrased the matter, "…the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences" (Daniel 2014). The "significant consequences" here hinged upon the matter of *timing* the disclosures: keeping the vulnerability secret would give government actors a functional advantage, enabling them to take advantage of the knowledge before the vulnerability was detected or patched. The VEP is thus one of the most visible elements of the government's efforts at producing and negotiating an interface between these different tempos, whereby disclosure is a process emerging as a product of

negotiations between intentional strategic action and the material affordances of the technologies with which actors are working.

With each iteration of the VEP, disclosure would become more wide-ranging in scope, with actors increasingly emphasizing the fuzzy edges of what constituted disclosure. By the time of Rob Joyce's blogposts in 2017 in response to the Shadow Brokers and WannaCry incidents, the VEP was enacting "disclosure" as a *spectrum* of possible outcomes. Building on the VEP's broadening of "disclosure" highlighted by Daniel in 2014, the spectrum that disclosure operated along was made explicit by the 2017 procedure, and it is worth quoting the 2017 Policy Charter at length:

> The U.S. Government's determination as to whether to disseminate or restrict a vulnerability *is only one element* of the vulnerability equities evaluation process and is *not always a binary determination***.** Other options that can be considered include disseminating mitigation information to certain entities without disclosing the particular vulnerability, limiting use of the vulnerability by the USG in some way, informing U.S. and allied government entities of the vulnerability at a classified level, and using indirect means to inform the vendor of the vulnerability. All of these determinations must be informed by the understanding of risks of dissemination, the potential benefits of government use of the vulnerabilities, and the risks and benefits of *all options in between.* (U.S. National Security Council 2017, 1, emphasis added)

Pointing to a more complex range of disclosure "options" in this way was working to make disclosure a more transitory state than set out when discussing vulnerabilities in terms of "dissemination." The

publication of this unclassified VEP Charter was the most detailed account of the VEP's functioning to date, indicating that the public controversy discussed in earlier had not been settled by official statements during the Obama Administration and was further aggravated by high profile incidents like WannaCry. Here, the VEP Charter was releasing more details of the procedure's range of considerations, and underscoring "disclosure" as a spectrum meant that reaching unconditional limits or thresholds was not the goal. As a former deputy director of the National Security Agency Rick Ledgett wrote in a personal op-ed following WannaCry, disclosure and patching were not a panacea:

> …WannaCry […] exploited flaws in software that had either been corrected or superseded, on networks that had not been patched or updated, by actors operating illegally. The idea that these problems would be solved by the U.S. government disclosing any vulnerabilities in its possession is at best naive and at worst dangerous. (Ledgett 2017)

While this was a confrontational articulation of the possible bounds of disclosure and its role in cybersecurity, instituting a spectrum of disclosure was in support of this general sense that it was not a binary state or an unmediated good. This meant that government actors would be less likely to "fail" in reaching publicly acceptable thresholds for disclosure, that they would be less likely to face criticism, if the VEP had already established that those thresholds were

contingent or mutable. Whilst the VEP had set parameters on disclosure by drawing different agencies together and making it a deliberative procedure rather than a distributed and messy problem, it had also expanded disclosure's possible permutations.

Disclosure as Rational

In contrast to the 2010 procedure, the way that disclosure was constituted by the VEP following Heartbleed in 2014 was thus beginning to shift. Rather than a procedural focus on when to *disseminate* knowledge of vulnerabilities amongst government agencies, the shift in approach was now specifically orienting the VEP around *disclosure*. The whole of Daniel's 2014 blogpost was describing the VEP in terms of its focus on when to disclose vulnerabilities to those outside the government. Repeatedly, government officials would emphasize that the VEP was weighted towards disclosure, on disclosure as the norm rather than the exception. As the head of NSA had described the process within the VEP, "…by orders of magnitude, the greatest numbers of vulnerabilities we find, we share" (Rogers 2014a). This phrasing was echoed by Daniel in an interview, who stated that the procedure was working on the assumption that "…the overwhelming majority of those that we find we do disclose. The idea that we have these vast stockpiles of vulnerabilities stored up - you know, Raiders of the Lost Ark style - is just not accurate" (Daniel,

quoted in Zetter 2014). The implication here was that the VEP was not designed to withhold information on vulnerabilities (or metaphorically store vulnerabilities like stacks of mysterious crates) but was an institutionalized and rigorous manifestation of disclosure in action.

Despite the VEP working to concretize disclosure practices as a spectrum, rather than an either-or, and thus broadening the boundaries of disclosure as a concept in political terms, in other ways it was institutionalizing a set of categorical parameters. Specifically, it did this by demarcating "repeatable methodologies" for quantifying risk:

> To the extent possible and practical, determinations to disclose or restrict will be based on repeatable techniques or methodologies that enable benefits and risks to be objectively evaluated by VEP participants. This process employs techniques that include assessment factors such as prevalence, reliance, and severity. (U.S. National Security Council 2017, 7)

Categorizing risk was to be a formative element of the VEP: "understanding risk was critical" to "ensure an equitable review of vulnerability information," and that the VEP did so by making "consistent, informed determinations" (U.S. National Security Council 2017, 8). All of the equity considerations listed in Annex A of the 2017 VEP Charter document are a long form attempt to assess "likelihood," "impact" and "harm," measures traditionally associated with risk assessments (U.S. National Security Council 2017, 13–14). In other words, "…[d]efense risk equations […] account for a threat multiplied

by one's vulnerability to that threat multiplied, in turn, by the consequences of that threat's exploitation." (Hennessey 2016). As the former legal counsel to the NSA, Hennessey was here articulating the NSA's rationale for deciding on the risks posed by vulnerabilities. The implication here was that if they could be quantified and rationalized, then vulnerabilities could be made amenable to clear methodologies that in turn set parameters on their disclosure.

This was a response to the difficulties that government agencies and actors were having in implementing containment imaginaries of secrecy in the face of mutable and mobile technological affordances in networked computer systems. Even when acknowledging that vulnerabilities may be retained according to the government's rationales, WannaCry and a series of other breaches and leaks of classified information meant that government agencies' ability to control and compartmentalize vulnerabilities had become a matter of contention in defending the credibility of their imaginaries for cybersecurity. For technology companies such as Microsoft, this was "an emerging pattern in 2017," where repeatedly, "…exploits in the hands of governments have leaked into the public domain and caused widespread damage" (Smith 2017). Even the former senior director for cybersecurity at the U.S. National Security Council admitted that

> …[i]n the current environment, government-held vulnerabilities are going to leak. Governments should not expect that they can

> hold on to vulnerabilities as long as they used to and we have to come up with coping mechanisms for it. (Schwartz, quoted in Carberry 2017)

At the heart of many similar such articulations of "the current environment" was an essentialized view of vulnerabilities' characteristics, that they were something that could be "held on to" and that the government could have a unique (if temporary) hold of. Underlying this understanding is a linear conception of cause-and-effect, a logic of if/then: *if* government actors can keep vulnerabilities segregated, secret, *then* security will follow. The problem with this informational view of vulnerabilities is that it belies a particularly static conception of them, rather than recognizing their emergent and mobile tendencies.

Those in the technical community would contest the government's account as a way to challenge the credibility of their claims that the federal agencies could manage such information, arguing that such an approach belied a technically illiterate understanding of vulnerabilities as something that could "held on to." As one former NSA hacker described the matter:

> …it is obvious to the technical community (although not to lawyers and policy makers) that 0days are not a simple commodity like grain or oil, but often are highly correlated, composed of smaller parts and techniques, and *uniquely non-fungible***.** (Aitel 2016, emphasis added)

In distinction to those outside this self-described community, such as lawyers and policy makers, to this "technical community" in the know, such non-fungible and hard-to-categorize matters meant that the VEP could only bound vulnerabilities and disclosure in limited ways. Their tendencies towards being transitory, leaky and moveable, emergent properties of the vicissitudes of execution (Chun 2008) meant that state articulations of the need for secrecy were being challenged by the very tempos and rhythms that they had initially proclaimed as justifications for their secrecy practices. Vulnerabilities and their associated exploits were not so neatly amenable to efforts at itemization and containment, which meant that over the course of its development, the VEP would make its methodological and rational parameters more explicit.

Rather than repeating the technologically determinist arguments discussed earlier in the article that the technologies were overdetermining the governments secrecy responses, we can see instead how disclosure would gradually shift in its meaning and practice, in effect adapting to the *timescapes* of networked technologies. On technical grounds, given the "non-fungible" characteristics of vulnerabilities and exploits discussed earlier, attempts to develop "repeatable techniques and methodologies" reflected a rationalist desire to impose prescriptive models of risks and

their relationship to people (Wynne 1996, 57). The VEP was a manifestation of this desire to quantify and therefore regularize or standardize the decision to disclose.

The 2010 VEP contained tacit criteria for the Equities Review Board to make its determinations based on determinations of its subject matter experts of what their respective agencies' interests would be. Despite the VEP having been established as a procedure in 2010, it emerged that it "…had not been implemented to the full degree that it should have been," with the result that the administration had "…re-invigorated our efforts to implement existing policy with respect to disclosing vulnerabilities," (Daniel, cited in Zetter 2014 n.p). Earlier incarnations of the VEP had set bounds too constrictively upon disclosure as a binary state, and while the VEP had been instigated, not all the agencies were communicating as consistently or in as coordinated a fashion as the policy called for (Daniel, cited in Zetter 2014). The "reinvigorated" VEP thus made the parameters of disclosure more explicit by incorporating more questions and more explicit thresholds for disclosure over time (Daniel 2014), whilst also broadening disclosure's parameters by expanding its possible permutations into a transitory and non-binary state.

DOI: 10.55917/2377-6188.1072

Disclosure as Quantifiable

The WannaCry incident in 2017 would again trigger administration officials to further advocate for the VEP's putatively impartial features. This was due in large part to Congressional lawmakers introducing a bicameral and bipartisan bill in Congress called the Protecting our Ability To Counter Hacking (PATCH) Act. The PATCH Act was described as intending to add "transparency and accountability to the U.S. government process for retaining or disclosing vulnerabilities" because the government's current decision-making process was "…opaque, unaccountable to Congress, and unestablished in law or Executive Order." (Schatz 2017) According to the sponsors of the Act, this was something that undermined "…trust with the American people and private sector and potentially jeopardize[d] our nation's cybersecurity" (Schatz 2017). The decision to disclose was about nothing less the trust of the American people and the nation's cybersecurity, illustrating the extent to which wider debates (discussed earlier) were shaping the conceptual and political importance of disclosure for constituting cybersecurity.

Despite the Obama administration's claims to the VEP's objectivity, Congressional and thinktank pressure to codify the VEP into law would be suffused with assumptions about law's capability to make the procedure more formalized and therefore more objective. For a

former Director for Cybersecurity Policy at the White House National Security Council, moving "…from what is an interagency agreement to substantiate VEP into law" would be an important step for improving accountability, given that there were "no penalties for individuals to hold back information" from the VEP (Knake, quoted in Spring 2017). A desire to impose a "legal framework around this process" indicated the extent to which speakers outside of the government felt there was still too much ambiguity around what constituted disclosure (Knake, quoted in Spring 2017). Putting legal parameters upon the VEP was intended to codify and regularize the process and was presumed to add an extra layer of rigor and impartiality. As a case in point, the statements in support of the PATCH Act from the Open Technology Institute described how legislation like the PATCH Act was "crucial in establishing confidence and trust" in the VEP process and "…would codify what the White House claims it has had all along: a rigorous process" (Bankston and Wilson 2017). Putting legal parameters on disclosure was intended to impose a framework, or set the bounds, of government disclosure practices. While the PATCH Act failed to progress beyond first reading, Congressional efforts to regulate the government's uses of vulnerabilities and to legally constitute their own readings of disclosure in its importance for ensuring national

cybersecurity led the White House to release the VEP Charter later that year.

Institutionalizing the bounds of disclosure through law as advocated by Congress and civil society was a step too far for those in the intelligence community. The 2017 VEP Charter was therefore an effort to preserve the autonomy of federal agencies to arbitrate their use, independently of this kind of external interference. Building on the reorientation of the VEP outlined by Daniel in 2014, the VEP shifted the emphasis in leadership of the process from the NSA as in 2010, to an increased role for a "VEP Director" based within the National Security Council, overseeing the NSA's role as Executive Secretariat (White House 2017, 4). The 2017 Charter even echoed the phrasing of the 2010 document when it stated that "Executive Secretariat function will be executed so as to remain neutral and independent" (White House 2017, 4). The 2017 VEP and its associated public statements were intended to head off congressional efforts at regulation and law, with the aim of preserving the autonomy of these agencies to make their own deliberations. In this sense, the VEP was intended to grant government agencies more latitude in the decision-making process, as legal requirements would have enforced oversight and reporting commitments. In effect, disclosures would have been recorded, and thus frozen in time and in records, made intelligible for larger potential

audiences in Congress and beyond. Instead, the 2017 VEP sought to limit those efforts at enumerating disclosures, to instead keep them as a more liminal, transitory (as well as symbolic) process that could be deniable too.

While keeping the VEP from being regulated in law was an important element in enabling the Executive Secretariat more latitude and freedom in deciding the bounds of disclosure, at the same time the VEP would also work to set limits upon disclosure's scope. Unlike the 2010 VEP policy that was so oriented around establishing interagency lines of communication, the 2017 Charter consistently articulated its rationale in terms of external interests. Thus, the 2017 incarnation of the VEP signified an even more explicit shift of disclosure in the name of "public interests." Accordingly, the 2017 VEP described "the primary focus of this policy" being to:

> …prioritize the public's interest in cybersecurity and to protect core Internet infrastructure … absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes. (National Security Council 2017, 1)

Demarcating between "national security" and "the public's interest in cybersecurity" was thus intended to set procedural and political limits upon the role of disclosure in constituting cybersecurity. In other words, by making these distinctions, the VEP Charter was setting limits on how far and how much disclosure would produce

cybersecurity, in effect setting limits on cybersecurity's otherwise all-encompassing scope. Joyce made such a distinction explicit when he rationalized that:

> What we're trying to carefully weigh is having those capabilities, to be able to use them for national security, while at the same time making sure that it's not a major liability for our economy, for the international community, for our national security." (Joyce, quoted in Bing 2017)

Disclosure was important for cybersecurity, but there would be limits to its scope in the name of "our national security." Through the VEP, disclosure would not be immediate in the temporal sense then, but neither would it be immediate (self-evident) in the political or democratic sense. With each iteration of the VEP, the arguments of those in the private sector and policy advocacy communities about the importance of "disclosure" for constituting disclosure were increasingly accommodated into federal initiatives, shaping their imaginaries and the ways that they were actualized through initiatives such as the VEP. The VEP was intended to allay some of those criticisms. At the same time however, the VEP would build into its process a broader spectrum of what would count as disclosure by institutionalizing exceptions. In 2014, Michael Daniel was reported as implying that the VEP would put vulnerabilities that had been discovered by contractors through the

process (Zetter 2014). However, the 2017 Charter made a certain range of exceptions explicit when it stated that:

> The USG's decision to disclose or restrict vulnerability information could be subject to restrictions by foreign or private sector partners of the USG, such as Non-Disclosure Agreements, Memoranda of Understanding, or other agreements that constrain USG options for disclosing vulnerability information. (National Security Council 2017, 9)

This distinction is important, because in working to constitute disclosure as a spectrum of possible variations rather than a binary state, the VEP here was also circumscribing the immediacy of the government's responsibility to disclose in instances where they paid for the vulnerability but did not see it themselves, such as through the use of contractors and proxies. Without concretized thresholds for what counts as disclosure, agencies would thus have more room for autonomy. By making the parameters of disclosure more liminal in this way, government actors were able to reassure outsiders by hailing disclosure-as-transparency, but without setting strict thresholds for agencies to be held accountable to by outsiders.

The VEP was an institutionalization of strategic practical action that sought to emphasize disclosure's ambiguity more as time passed, though this was always filtered or mediated through experiments (and leaks and controversies) with operational experiences with the technologies. Thus, the sense of external time pressures, of

imperatives stemming from a fast-moving technological frontier, were implicit throughout the VEP and its accompanying justifications. In this vein, Rob Joyce reflected on the tensions that cybersecurity's "imperatives" for patching posed with the instrumental withholding of information from vendors, given that the "…reasons you want to patch, you want to disclose are because our society has grown intertwined with our IT technology, so if there's a flaw in those systems there is an imperative to close that hole and make sure it's not exploited" (Joyce, quoted in Newman 2017).

The VEP was thus suffused with references to timing and urgency. The implication here was that if American society was intertwined with information technologies, then they were also intertwined with technological vulnerabilities. As a result, the VEP was intended to act as a means to temporarily set their use apart and to functionally demarcate vulnerabilities from a society "intertwined" with them. As Rob Joyce later defended the VEP at a public event, it was "…just a fact that the government is going to work to develop vulnerabilities and find them for operations. The ecosystem continues to find new and innovative ways to exploit." (Joyce, cited in Newman 2017). Implied here was that government actors were responding to external pressures of "the ecosystem" changing and innovating. Similarly, the NSA general counsel described how,

> Physically, and logically, the domain is in *a state of perpetual transformation*. It enables the transmission of data across international boundaries in nanoseconds—controlled much more by individuals or even machines than by governments... (Ney 2020, emphasis added)

In the face of the kinds of criticisms discussed earlier, processes taking place in nanoseconds and through claimed machine speeds would prompt novel questions for state actors trying to both articulate and justify the role of vulnerabilities in their cyberspace operations. As systems evolved, the assumption was that discovery, exploitation and patching would also speed up, lending an urgency to government actions.

As with many matters of risk assessment, different communities expressed competing (and subjective) expressions of the risks calculated by the VEP. Summarizing a principle from the technical security community, one security researcher stated that:

> *It is a well-known fact* that security vulnerabilities are not purely technical problems. They usually arise as a result of the interaction of several components, including technical issues, processes, management, and human errors. (Civaner 2020, emphasis added)

One of the problems with vulnerabilities is that they do not speak for themselves: they are not self-evident or fungible objects in a familiar sense and are social and organizational entities as much as they are technical. Schemes for evaluating and rating risks posed by

vulnerabilities have been a matter of debate even within the de facto industry standard for assessing the severity of vulnerabilities (Taylor 2015). Here, the security researcher community has highlighted the limitations of categorizing vulnerabilities and their risks as quantifiable entities (Robinson 2019; Ross 2019). While technical and operational programs may be in place to share information, like government secrecy and disclosures in other contexts (Stampnitzky 2020), information still requires political context and human actions to translate it into *cybersecurity* measures.

Over time, the VEP has thus sought to reconfigure the bounds of disclosure in order to accommodate both the federal visions of cybersecurity as well as some of the dissenting narratives discussed earlier. Disclosure as both concept and practice has emerged at the point of experiences with and through technologies, including the technologies of the VEP procedure itself, as much as strategic intentional action on the part of state actors. The contestation between different articulations of what disclosure *means*, what it *does*, has also fed into this gradual modulation of disclosure practices. With each iteration of the VEP, and with each round of debate with those outside of government, vulnerability disclosure as a practice and concept became an increasingly important symbol and resource for government actors to draw upon as a means of highlighting their cybersecurity

credentials. Disclosures about the VEP procedure meanwhile were a means for the Administration to keep the American people minimally informed of its activities, and to characterize these activities in ways intended to solicit public support by invoking normatively laden ideals of transparency, accountability and responsibility (Pozen 2013). At the same time, the VEP worked to avoid any substantive alternatives to government actions by keeping details of vulnerabilities from being made public. Normatively and procedurally, revealing the VEP under the guise of transparency was a strategic effort at legitimizing the government's actions. Although it is dressed up as transparency for democratic accountability, it sought to focus attention on the processes, rather than questioning why this process was necessary in the first place. It also helped to show that government agencies possess these offensive capabilities (perhaps as a form of deterrence signaling), but without really addressing the contents of the disclosure. Those vulnerabilities that government actors did reveal, and by extension the hacking capabilities of state agencies, still required interpretation and translation into something politically meaningful.

Policies in the name of "cybersecurity" like the VEP are an example of government actors reimagining established secrecy and security practices in the face of ubiquitous computing. While my empirics focus on the US, this paper has relevance for more general

conceptualizations of official secrecy in the age of digital networks and technologically-mediated security contexts. Countries all over the world are pursuing and developing these capabilities through the global internet and the VEP is demonstrative of government actors trying to make sense of ongoing change-processes in the world. Through a critical discussion of the US government's secrecy practices in this context, I suggest that it is possible to see some common themes, behaviors, assumptions and technologies that can shed light on wider global patterns (Marx 2007).

Conclusion

At first reading, it appears that the story of the VEP fits the standard conceptualization of disclosure as instrumental, undertaken strategically to manage PR, to manage expectations, to allay fears in the public that the government is undermining its own transparency and accountability ideals. There is certainly an element of what Bratich would call *spectacular secrecy* here.

But in a second reading, we can see how practices and conceptualizations of disclosure have emerged and iterated. Attending to time and technologies has allowed us to shift away from linear conceptions of cause and effect, to more processual and therefore contingent arrangements of structures and agents. The secrecy

practices that governmental actors are seeking to rationalize here are not about the closing off or concealment of knowledge that the government already possesses, but about a speculative secrecy that anticipates the need to claim as-yet undiscovered vulnerabilities in the future for national security purposes. Disclosure does not operate solely in the past (as a reference to historic entities or information already discovered), or in the present (as the simple revelation of these entities). Indeed, in the case of entities like vulnerabilities that are emergent properties rather than informational "nuggets," such a linear and informational model of the relationships between secrecy and revelation have been the very thing that government actors have struggled to transpose.

At the same time, we can see not only how vulnerabilities and internet technologies pose particular challenges to government actors seeking to claim a monopoly on secrecy, we can also see how these technologies and political processes have given rise to new interpretations of the concept of disclosure itself, moving beyond regular conceptions of disclosure as a binary state, or even as a spectrum, to a mutable or transitory process. Disclosure also produces opportunities for strategic maneuver in the future, a concept mediated by its interactions with networked technologies, an artifact of the non-fungible qualities of the technological vulnerabilities and capabilities in

question. Technologies, and their times, have served to mediate disclosure in particular ways in this particular set of circumstances.

The paper has sought to show how attending to different temporalities, and shifting away from conceptions of secrecy-as-containment or linear relations between secrecy-and-disclosure, has utility for future work on state secrecy. In this instance, it has shown how government actors have struggled to demarcate those bugs and flaws in code as uniquely governmental, as property, and that they have had to adapt and adopt their approaches in light of external criticisms as much as the "leakiness" of the code and its own secrecy practices. Hegemonic discourses of technological determinism, security and state power, no longer look so certain.

References

Aitel, Dave. 2016. "The Value of an 0day Stockpile to the Country versus the Value of Feeling Self-Righteous." *CyberSecPolitics*, February 12. https://perma.cc/KT8L-AEHK

Aldrich, Richard J., and Christopher R. Moran. 2018. "'Delayed Disclosure': National Security, Whistle-Blowers and the Nature of Secrecy." *Political Studies* 67(2)*, 291–306*. https://doi.org/10.1177/0032321718764990

Anaïs, Seantel, and Kevin Walby. 2016. "Secrecy, Publicity, and the Bomb: Nuclear Publics and Objects of the Nevada Test Site, 1951–1992." *Cultural Studies* 30(6): 949–68. https://doi.org/10.1080/09502386.2015.1113553

Bankston, Kevin, and Andi Wilson. 2017. *OTI Applauds Introduction of the PATCH Act.* Open Technology Institute, New America. https://perma.cc/Y63Q-RGVN

Beyes, Timon, Wendy Hui Kyong Chun, Jean Clarke, Mikkel Flyverbom, and Robin Holt. 2022. "Ten Theses on Technology and Organization: Introduction to the Special Issue." *Organization Studies* 43(7), 1001–1018. https://doi.org/10.1177/01708406221100028

Bing, Chris. 2017. "Trump Administration Will Shine Light on Vulnerability Disclosure with Public Charter." *CyberScoop*, October 4. https://cyberscoop.com/vep-public-charter-rob-joyce-cybersecurity/

Birchall, Clare. 2021. *Radical Secrecy: The Ends of Transparency in Datafied America*. Minneapolis, MN: Minnesota University Press.

Bok, Sissela. 1982. *Secrets: On the Ethics of Concealment and Revelation*. Oxford: Oxford University Press.

Bratich, Jack. 2006. "Public Secrecy and Immanent Security: A Strategic Analysis." *Cultural Studies* 20 (4–5): 493–511. https://doi.org/10.1080/09502380600708937

Carberry, Sean D. 2017. "Why Disclosure Rules Didn't Prevent the WannaCry Attack." *FCW*, May 15. https://perma.cc/A6G9-7BWV

Carnegie, Allison. 2021. "Secrecy in International Relations and Foreign Policy." *Annual Review of Political Science* 24(1): 213-233. https://doi.org/10.1146/annurev-polisci-041719-102430

Carson, Austin. 2015. "Facing off and Saving Face: Covert Intervention and Escalation Management in the Korean War." *International Organization* 70(1): 103–31.

Chun, Wendy Hui Kyong. 2008. "On 'Sourcery,' or Code as Fetish." *Configurations* 16(3): 299–324.

Civaner, Fırat. 2020. "Real-Life Software Security Vulnerabilities and What You Can Do to Stay Safe." *HackerNoon*, January 22. https://perma.cc/F7G9-GHMA

Coleman, G. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous.* London, New York: Verso Books.

Daniel, Michael. 2014. *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities.* The White House. April 28. https://perma.cc/HG36-JGNW

Dean, Jodi. 2004. "Secrecy Since September 11." *Interventions* 6(3): 362–80. https://doi.org/10.1080/1369801042000280023

De Goede, Marieke, and Mara Wesseling. 2017. "Secrecy and Security in Transatlantic Terrorism Finance Tracking." *Journal of European Integration* 39(3): 253–69. https://doi.org/10.1080/07036337.2016.1263624

Fan, Ziyun, and Yihan Liu. 2022. "Decoding Secrecy as Multiple Temporal Processes: Co-Constitution of Concealment and Revelation in Archival Stories." *Human Relations* 75(6): 1028–52. https://doi.org/10.1177/0018726721998743

Fenster, Mark. 2012. "Disclosure's Effects: WikiLeaks and Transparency." *Iowa Law Review* 97: 753–806. https://doi.org/10.3868/s050-004-015-0003-8

_____.2015. "Transparency in Search of a Theory." *European Journal of Social Theory* 18(2): 150–67.

Fluck, Matthew, and Daniel R. McCarthy. 2019. "Information Is Power? Transparency and Fetishism in International Relations." *Globalizations* 16(1): 1–16. https://doi.org/10.1080/14747731.2018.1507698

Flyverbom, Mikkel, Paul M. Leonardi, Cynthia Stohl, and Michael Stohl. 2016. "The Management of Visibilities in the Digital Age." *International Journal of Communication* 10(1): 98–109.

Fruhlinger, Josh. 2022. "WannaCry Explained: A Perfect Ransomware Storm." *CSO Online,* August 24. https://perma.cc/LF85-KSME

Galison, Peter. 2004. "Removing Knowledge." *Critical Inquiry* 31: 229–43. https://doi.org/10.1086/427309

Gros, Valentin, Marieke de Goede, and Beste İşleyen. 2017. "The Snowden Files Made Public: A Material Politics of Contesting Surveillance." *International Political Sociology* 11(1): 73–89.

Hennessey, Susan. 2016. "Good Defense Is Good Offense: NSA Myths and the Merger." *Lawfare,* Feb 9. https://perma.cc/GP8B-TY5P

Hofmann, Marcia, and Trevor Timm. 2012. "Zero-Day" Exploit Sales Should Be Key Point in Cybersecurity Debate. *Electronic Frontier Foundation*, March 29. https://perma.cc/ZPV9-LUUA

Hom, Andrew. 2020. *International Relations and the Problem of Time*. Oxford: Oxford University Press.

Hopper, Darby, and Dan Waldman. 2017. "How Washington Evaluates Software Vulnerabilities." *Christian Science Monitor, March 22.* https://perma.cc/3TNW-XAPY

Horn, Eva. 2011. "Logics of Political Secrecy." *Theory, Culture & Society* 28(8): 103–22.

Hudson, Jennifer L. 2015. *Declaration of Jennifer L. Hudson, Director, Information Management Division, Office of the Chief Information Officer.* Office of the Director of National Intelligence, October 30. United States District Court for the Northern District of California, San Francisco Division. https://www.eff.org/document/declaration-jennifer-l-hudson

Hudson, Jennifer L. 2016. *Declaration of Jennifer L. Hudson, Director, Information Management Division, Office of the Chief Information Officer.* Office of the Director of National Intelligence, January 14. United States District Court for the Northern District of California, San Francisco Division. https://www.eff.org/document/vep-foia-second-hudson-declaration

Joyce, Rob. 2017. *Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do*. The White House. https://perma.cc/7ANC-PB2Z

Kearns, Oliver. 2017. "Secrecy and Absence in the Residue of Covert Drone Strikes." *Political Geography* 57: 13–23. https://doi.org/10.1016/j.polgeo.2016.11.005

Kearns, Oliver. 2021. "Beyond Enclosure: Military Bases and the Spatial Dynamics of Secrecy." *Geoforum* 127: 12–22.

Ku, Agnes S. 1998. "Boundary Politics in the Public Sphere: Openness, Secrecy, and Leak." *Sociological Theory* 16(2): 172–92.

Ledgett, Rick. 2017. "No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession." *Lawfare*, August 7. https://www.lawfareblog.com/no-us-government-should-not-disclose-all-vulnerabilities-its-possession

Maret, Susan. 2016. "The Charm of Secrecy: Secrecy and Society as Secrecy Studies." *Secrecy and Society* 1(1). DOI: https://doi.org/10.31979/2377-6188.2016.010101

Manach, Jean Marc. 2018. "NSA Deletes "Honesty" and "Openness" from Core Values." *The Intercept,* January 24.

https://theintercept.com/2018/01/24/nsa-core-values-honesty-deleted/

Marx, Gary T. 2007. "Rocky Bottoms: Techno-Fallacies of an Age of Information." *International Political Sociology* 1(1): 83–110.

Mistry, Kaeten, and Hannah Gurman. 2020. *Whistleblowing Nation: The History of National Security Disclosures and the Cult of State Secrecy*. New York: Columbia University Press.

Nakashima, Ellen. 2016. "National Security Agency Plans Major Reorganization." *Washington Post,* February 2. https://www.washingtonpost.com/world/national-security/national-security-agency-plans-major-reorganization/2016/02/02/2a66555e-c960-11e5-a7b2-5a2f824b02c9_story.html

Newman, Lily Hay. 2017. "Feds Explain Their Software Bug Stash - But Don't Erase Concerns." *Wired,* November 15. https://perma.cc/PAZ3-XX3D

Ney, Paul C. 2020. *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*. March 2. https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7(2): 61–73.

Pozen, David E. 2013. "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information." *Harvard Law Review*, 127: 512.

Rapid7. 2022. *Vulnerabilities, Exploits, and Threats at a Glance*. https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Robinson, Christopher. 2019. *Why CVSS Does Not Equal Risk: How to Think about Risk in Your Environment*. Red Hat Blog, July 10. https://perma.cc/V7MN-GKYP

Rogers, Adm. Michael. 2014a. *Transcript of Admiral Michael S. Rogers Address to Stanford University at the Freeman Spogli Institute for International Studies.* November 3. Speeches and Congressional Testimonies, NSA. https://perma.cc/M6U3-ZKV4

Rogers, Adm. Michael. 2014b. *Nominations Before The Senate Armed Services Committee*. 113th Congress, 2nd Sess., S. HRG. 113-611. https://perma.cc/X29H-LWSK

Rogers, Adm. Michael. 2017. *Maximizing the Value of Cyber Threat Information Sharing.* Subcommittee on Cybersecurity and Infrastructure Protection of the Committee on Homeland Security. 115th Congress, 1st Sess., H.Rep. 115-39. https://perma.cc/K4VH-DFAJ

Ross, Abby. 2019. "Calling Into Question the CVSS." *Security Intelligence,*February 20. https://perma.cc/4A75-AXAE

Schatz, Brian. 2017. *Bipartisan, Bicameral Lawmakers Introduce Bill To Enhance Cybersecurity, Promote Transparency* (*Protecting Our Ability to Counter Hacking "PATCH" Act of 2017).* May 17. https://perma.cc/3DNC-NKBA

Schneier, Bruce. 2012. "The Vulnerabilities Market and the Future of Security*." Schneier on Security,* May 30. https://perma.cc/S8E7-A7PX

Schneier, Bruce. 2016. "The NSA Is Hoarding Vulnerabilities." August 26. *Schneier on Security,* August 27. https://perma.cc/U2J5-7MDS

Smith, Brad. 2017. "The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack." *The Official Microsoft Blog*, May 14. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Spring, Tom. 2017. "Policy Experts Push To Make Vulnerability Equities Process Law." *ThreatPost.com*,February 23. https://perma.cc/WV9L-X9UD

Stack Overflow. 2008. "Bugs Versus Vulnerabilities?" *StackOverflow Forum,*December 31. https://stackoverflow.com/questions/402936/bugs-versus-vulnerabilities

Stampnitzky, Lisa. 2020. "Truth and Consequences? Reconceptualizing the Politics of Exposure." *Security Dialogue,* 51(6), 597–613.

Synopsys. 2020. *The Heartbleed Bug*. https://heartbleed.com/

Taylor, Richard G. 2015. "Potential Problems with Information Security Risk Assessments." *Information Security Journal* 24 (4–6): 177–84.

U.S. National Security Agency. 2017. *Mission and Strategy*. https://web.archive.org/web/20171214073007/https://www.nsa.gov/about/mission-strategy/

U.S. National Security Council. 2010a. *Commercial and Government Information Technology and Industrial Control Product of System Vulnerabilities Equities and Process*. https://www.eff.org/document/vulnerabilities-equities-process-redactions

_____. 2010b. *Commercial and Government Information Technology and Industrial Control Product of System Vulnerabilities Equities and Process.* https://www.eff.org/document/vulnerabilities-equities-process-january-2016

Van Veeren, Elspeth. (2019). "Secrecy's Subjects: Special Operators in the US Shadow War." *European Journal of International Security* 4(3): 386-414. http://doi.org/10.1017/eis.2019.20

Van Veeren, Elspeth and Tim Duroux, Amaha Senu, and Clare Stevens. (Forthcoming). "Tunnels, Mazes, Layers: Secrecy and Security Beyond Containment." *European Journal of International Security*.

Walters, William. 2021. *State Secrecy and Security: Refiguring the Covert Imaginary*. Abingdon; New York: Routledge.

Wellerstein, Alex. 2021. *Restricted Data: The History of Nuclear Secrecy in the United States*. Chicago: University of Chicago Press.

White House, 2017. *Vulnerabilities Equities Policy and Process for the United States Government*. November 15. https://perma.cc/NS88-7F4U

Wynne, Brian. 1996. "A Reflexive View of the Expert-Lay Knowledge Divide." In *Risk, Environment and Modernity: Towards a New Ecology*, edited by Scott Lash, Bronislaw Szerszynski, and Brian Wynne, 44–83. London: Sage Publications.

Zetter, Kim. 2014. "U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies." *Wired*, November 17. https://perma.cc/4P7M-TTSQ