doi:10.1017/aju.2017.4

SYMPOSIUM ON CYBERSECURITY AND THE CHANGING INTERNATIONAL LAW OF DATA

NATIONAL SECURITY OR PRIVACY: A SECOND THOUGHT ON THE DNC HACK

*Sung-In Jun**

Introduction

The recent U.S. Democratic National Committee (DNC) hack raises several difficult questions in the fields of cybersecurity and privacy. Obviously, this was first and foremost a matter of *security* in that the hack likely involved a foreign government attempting to intervene in a presidential election process with the possible motive of influencing its outcome.[1] From another perspective, however, the incident was also a matter of *privacy*, in that the fundamental motive of the DNC hack was to reveal "information that the victim wants to keep private" and to influence its future decision through the compromise of privacy.

If we accept the proposition that there are two questions related to the recent DNC hack, then the impulse to view such incidents as predominantly a security issue could potentially skew the discussion, overlooking concerns regarding privacy. Considering the process that links the hack to the leak, perhaps the harm done to the victim's privacy deserves equal, if not more, attention than the compromised system itself. We need to examine the episode with due proportionality and proper attention to the entire context.

Protecting privacy in cyberspace is a tricky task that requires both maintaining an appropriate distance from the government and enhancing the duties of the relevant parties. While formal support from the government is necessary, we must also be aware that the individual and the government may sometimes have conflicting incentives in protecting privacy. In addition, we need to consider creating a form of discipline akin to a fiduciary duty on those who deal with private information.

This short essay discusses issues related to the protection of privacy triggered by the DNC hack. In particular, the essay discusses why the DNC hack should be viewed differently from other typical cyberbreaches, why viewing some breaches only as a matter of national security could skew the discussion, and what various pitfalls and obstacles exist in protecting privacy as well as their possible solutions.

* *Professor of Economics at Hongik University.*

[1] It was alleged that the CIA concluded that the Russian government was behind the DNC hack. *See* Adam Entous et al., *Secret CIA assessment says Russia was trying to help Trump win White House*, WASH. POST (Dec. 9, 2016).

American Society of International Law and Sung-In Jun © 2017. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/aju.2017.4 Published online by Cambridge University Press

A Different Context of Stealing

Steal in order to reveal rather than to keep

The purpose of a hack could be manifold. In the simplest dimension, it is executed to exfiltrate some valuable information or to disrupt the computer system or network itself. The assessment of this kind of cyberactivity is straightforward, since the traditional standard that we apply to our everyday offline life can easily be transplanted. We consider the activity inappropriate since it is either a theft or an attack.

The hack acquires another layer when the ultimate purpose of a hack is to *reveal* the hacked information to the public. The DNC hack is a case in point. The hacked information, or rather a carefully selected subset of it, was revealed on WikiLeaks and other similar websites.[2] So the hacker in a way *shares* some if not all of the stolen information with the public. Then, the assessment gets complicated.

Is all revelation bad, if it is illegally obtained?

We all know that the end does not justify the means. Still, there is a sense of discomfort when we disregard the entire content of a revelation only because the underlying information is obtained illegally. One may think of a Robin Hood in cyberspace who steals information from the information-greedy collector to distribute it to the information-poor public.

The case of Edward Snowden is an uncomfortable example of someone who revealed that many states renowned for ethical conduct worked together to collect information in inappropriate ways, sometimes even going so far as to tap the phone of another state's leader. It is not easy to tell who the bad guy is here, the collector or the revealer. Especially if the revelation is somehow connected to freedom of speech, and the content of the revelation is the possible wrongdoing of established authorities, the sense of discomfort increases when we try to silence the whistleblower.

Whose property is stolen here?

Sometimes the property right associated with the stolen information may not be firmly established. The DNC hack differs from the Snowden revelation in this respect. The stolen information stored on the DNC server was private property, produced or collected in a legitimate way, and can be claimed as such in court. Regardless of the motivation, the act of stealing information in this case can hardly be justified.

Can the same be said of the release of the NSA's information obtained by wiretapping a foreign leader? Certainly not in the ethical sense, and probably not in the legal sense either.[3] If the information is not the lawful property of the NSA in the first place, is it appropriate to punish the hacker for stealing it? Of course we can always incriminate the hacker by arguing that his use of the network was unauthorized and so on. We all know, however, that this skirts the main issue.

[2] For example, on October 6, 2016, DC Leaks released a set of emails from Hillary Clinton insider Capricia Marshall after an initial email leak posted on WikiLeaks in July. *See* Michael Sainato, *DC Leaks Exposes Clinton Insider's Elitist Embarrassing Emails*, OBSERVER (Oct. 7, 2016, 10:07 AM).

[3] Of course not all of the information stored on the NSA server was collected illegally. Allegedly, a significant part of data collected by the PRISM program was Internet communications data obtained from companies like Google Inc. This collection was legal, according to Section 702 of the FISA Amendments Act of 2008. *See* Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U. S. Internet companies in broad secret program*, WASH. POST (June 7, 2013).

https://doi.org/10.1017/aju.2017.4 Published online by Cambridge University Press

Protection of privacy: a clearer criterion

The analysis above shows that the proper regulation of a hack is more complicated than it first appears. Even if we all agree that there is ample reason to treat stealing information and gaining unauthorized access to systems and networks as illegal, there is a sense of mitigation, if not the realization of justice, when what the act purportedly reveals is evident wrongdoing by authorities.

This raises a series of complicated questions. When is a hacking incident justified, if only partially; who decides whether it is justified and based on what kind of criteria? Presumably the answer would vary from individual to individual and from one society to another. In short, this may not be the most practical way of framing the problem.

Where else should we look then? We might well begin by concentrating on a less controversial area, *privacy*. In this context, a hack is bad if it infringes the victim's privacy. This criterion is much clearer in establishing cybersecurity or in regulating hacking since the invasion of privacy is almost always and everywhere regarded as a reproachable act.

Admittedly, the criterion of privacy on its own is insufficient to judge the extent of illegality. For example, some exceptions must be made for emergencies. Moreover, the criterion of privacy does not provide definite answers with regard to hacks targeting governmental and quasi-governmental entities. And there are grey areas in the definition of privacy. Nonetheless, the privacy criterion provides a valuable cornerstone upon which to build a more sophisticated and realistic regulatory structure.

Obstacles to Enhancing the Protection of Privacy

Security from whom?

The invasion of privacy could originate from various angles, even if we restrict our attention to activities in cyberspace. The DNC hack insinuated that the threat could come from foreign governments, as well as from traditional sources such as insurance companies, credit rating agencies, and the marketing departments of supermarket chains. Social network services and email-servicing companies are also rapidly emerging as sources of potential trouble. Finally, we should not leave out the ultimate information guzzler, our own government. So protecting privacy means reasonable protection from all these potential intruders.[4]

Where could we turn, then, for help with the protection of privacy? The government usually handles such public functions. Unfortunately, this does not work well here. One notable difficulty in finding reasonable solutions for the protection of privacy is that the state or government, including all of its quasi-public subsidiaries, is both friend and foe. It could lend a helping hand with the protection of privacy, but it could also collect, indeed has often proved to be collecting, private information for its own purposes whether legally or illegally. So simply emphasizing the role of the government in the struggle against the invasion of privacy will not do the trick. Rather, reasonably good privacy may be achieved by maintaining a proper distance from the intervention of the state.

The DNC hack was again a case in point. Allegedly, the hack was done to reveal some critical *dishonorable* information about the presidential candidate, Hillary Clinton, or her surrounding supporters. The most probable motive for this kind of action was to arouse negative opinions of the target and influence the course of events *ex ante* or *ex post*. This is an irresistible temptation to which every government is prone. If a foreign government can do it, any government can do it. If any government can do it, some government will do it.

[4] One may argue that the collection of metadata does not necessarily invade privacy since each isolated piece of information does not mean much. The process of *matching* or *reidentification*, however, can link pieces of information to individual entities and hence reintroduce the privacy concern.

https://doi.org/10.1017/aju.2017.4 Published online by Cambridge University Press

Is a centralized fortress for storing private information a good idea?

How privacy can be protected is also a question in need of critical attention. Frightened by the ample possibilities for an invasion of privacy, we might imagine an *information fortress* with high and strong walls of several layers maintained by cybersecurity experts, where valuable information can be stored like precious belongings in the vault of a trusted bank.

The fable of a strong fortress where information can be stored may sound reassuring, but actually has the following critical problems:

First, the usefulness of information accelerates as the amount of information added to the analysis increases. So does the potential benefit from a hack. The cost advantage, however, is not obvious. Even if the average cost of storing information is likely to fall, the cost of monitoring data traffic could increase very quickly as everyone who needs to store or retrieve information has to access the highly guarded gates. So, the scale may weigh against the central management of private information.

Second, the central management of diverse information usually needs some kind of universal key, such as a Social Security Number (United States) or a Resident Registration Number (South Korea). The data structure used in this kind of universal identifier can be more or less known or easily guessed so that the encryption applied to this identifier could be very ineffective.[5]

Third, giving the control of valuable information to a handful of people is inherently a dangerous idea. If there is anything we learned from the cryptographic scheme of Bitcoin, it is that fooling many people at the same time or tampering with a decentralized system altogether is very hard. The idea of one big shining fortress has exactly the opposite structure. If you somehow obtain a universal key from the system operators, you can open any gate and access the entire database in the fortress.

Unsound motives of the government and the private sector

If centralized management of private information is not the way to go, the remaining option is to enhance the protective capability of individuals and other private entities. This is harder than it looks for the following reasons.

First, the state will often be motivated to ask for exceptions such as specially designed backdoors that will circumvent any protective scheme in one snap.[6] This was often justified as serving a public purpose, typically national security. Given that it is very hard for an ordinary individual to distinguish a matter of national security from the disguised desire to collect information about the governed, this request for backdoors always has the possibility of abuse. The response, then, must depend on how much social trust the government enjoys.

Second, the state may prevent the private sector from coming up with stronger information protection technology. The alleged reason is again the same, national security. When means of communication are too secure, it is hard for the government to collect valuable information about national security or organized crime.[7] Lowering the level of protection for the private sector makes that sector inherently vulnerable.

[5] Latanya Sweeney & Ji Su Yoo, *De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data*, TECH. SCI. (Sept. 29, 2015) showed that recovering the Resident Registration Numbers (RRNs) of all 23,163 Korean individuals in a given sample was easy and accurate. The study exploited the data structure of the RRNs which include date of birth, sex, place of birth, and the checksum.

[6] "But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone." *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016).

[7] In February 1993, Phil Zimmermann, the original inventor of Pretty Good Privacy, faced a formal criminal investigation initiated by the U.S. Government for "munitions export without a license." The Justice Department dropped the charges in 1996. *See* John Markoff, *Data-Secrecy Export Case Dropped by U.S.*, N.Y. TIMES (Jan. 12, 1996).

https://doi.org/10.1017/aju.2017.4 Published online by Cambridge University Press

Third, certain information-hungry business sectors tend to prefer lowering the level of privacy protection. Since the business sector's power of coercion is not comparable to the government's, it usually relies on loopholes or hoaxes that lead individuals to abandon their privacy voluntarily. For example, trading minimally deidentified sensitive data exploits loopholes in the current regulatory structure, while attracting consumers and effectively enticing them to give up their private information for a modicum of compensation without disclosing entire details of possible uses of collected information, is a frequently used tactic to enlarge their databases.[8]

Basic Directions for Solutions

Practical ways of enhancing the protection of privacy

Given that the private sector as well as the government lack an inherent incentive to support the strong protection of privacy, explicit checks by the legislative and judicial branches are needed. Specifically, there must be explicit guidelines as to what the government can and cannot do regarding the collection, the storage, and the usage of private information.

Moreover the current regulatory structure based on the prior consent of individual owners of information should be supplemented with one based on duty whereby anyone who deals with the private information of others bears a quasi-fiduciary duty. The data handler should be reasonably sure that the information is not misused, causing harm to the original owners of information. A duty-based regulatory structure becomes increasingly important as data collection without the information owner's explicit endorsement, such as the Internet of Things or CCTVs, becomes increasingly prevalent.

A minimum damage award is also necessary to deter information abuse effectively. It is usually very hard to prove the actual amount of damage when one's private information is abused. This is especially the case when the damage occurred as part of a mass leak of information. Thus, undercompensation is prevalent even if the leak itself is well established. A minimum damage award can help to close this loophole by allowing a court to award a predetermined amount for minimum damage once the leak itself is proved.

In the name of national security

Securing the safety of the homeland and preserving law and order are among the state's basic functions. Defending the homeland from malicious cyberattacks certainly falls squarely within them. So it is almost tautological that the state should have proper means to fulfill this mission. There are, however, some important restrictions on the *proper means*.

First, the means used by the state should not interfere with the protection of privacy except under very extreme circumstances. Under such circumstances, the state should bear the burden of proof and the extent of the invasion of privacy should be kept to a minimum. Without these restrictions, the protection of privacy could be in danger of continuous erosion.

Second, the preventive measures taken by the state against a possible wrongdoer should be kept to a minimum since they are essentially actions relating to a crime not yet committed. Even if we agree on the benefit of crime prevention and the irrevocable cost of information breach, the benefit of avoiding information leakage or the

[8] From 2011 to 2014, Homeplus, a supermarket chain in South Korea, collected private information from individuals in exchange for small presents and later sold the data to an insurance company. The District Court in Seoul found Homeplus not guilty of violating the Individual Information Protection Act, since the defendant provided the necessary disclosure even if in very fine print using 1mm fonts. Civil rights organizations delivered a protest letter to the Court written in 1mm fonts to mock the verdict. *See* *"판사님은 이 글씨가 보이십니까?"*, YTN (Jan. 13, 2016, 10:14 PM).

https://doi.org/10.1017/aju.2017.4 Published online by Cambridge University Press

breakdown of networks should be conservatively balanced against the possible violation of an inalienable human right.[9]

Concluding remarks

At first glance, the DNC hack may seem to be a national security concern rather than a matter of privacy. Overemphasizing national security, however, may obscure the other aspect of the incident, the invasion of privacy. The concern about privacy may be more important in that any government, or any organization with sufficient power and drive, can be tempted to act similarly. In this regard, seeking ways to enhance the protection of privacy may be the correct lesson to learn.

[9] The notion of *active defense*, as described in Center for Cyber & Homeland Security, *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats* (2016), is much more controversial in that it allows the defender to infiltrate the networks of potential wrongdoers and to alter the system so that it can no longer do harm to the defender. This idea comes dangerously close to the statement that the end justifies the means.

https://doi.org/10.1017/aju.2017.4 Published online by Cambridge University Press