Privacy and Cybersecurity Research Briefing

Networked Policy Series

Translating Research for Action: Ideas and Examples for Informing Digital Policy

September 2016

Privacy and Cybersecurity

Research Briefing

David R. O'Brien, Ryan Budish, Rob Faris, Urs Gasser, and Tiffany Lin

for more from this series visit
cyber.harvard.edu

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

BERKMAN KLEIN CENTER

FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

Privacy and Cybersecurity

Research Briefing

David R. O'Brien, Ryan Budish, Rob Faris, Urs Gasser, and Tiffany Lin

Suggested citation: O'Brien, David, Budish, Ryan, Faris, Robert, Gasser, Urs and Lin, Tiffany, Privacy and Cybersecurity Research Briefing (September 26, 2016). Networked Policy Series, Berkman Klein Center Research Publication No. 2016-17. Available at SSRN: http://ssrn.com/abstract=2842801

23 Everett Street | Second floor | Cambridge, Massachusetts 02138
+1 617.495.7547 | +1 617.495.7641 (fax) | http://cyber.harvard.edu
press@cyber.harvard.edu

"From buying products to running businesses to finding directions to communicating with the people we love, an online world has fundamentally reshaped our daily lives. But just as the continually evolving digital age presents boundless opportunities for our economy, our businesses, and our people, it also presents a new generation of threats that we must adapt to meet. Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person. As more and more sensitive data is stored online, the consequences of those attacks grow more significant each year. . . . [W]ith each new story of a high-profile company hacked or a neighbor defrauded, more . . . wonder whether technology's benefits could risk being outpaced by its costs."[1]

Overview

The Berkman Klein Center for Internet & Society at Harvard University ("BKCIS") has prepared this research briefing on privacy and cybersecurity for use by decision-makers in the private and public sectors who must balance the numerous tensions inherent in securing products and services, keeping users safe, and maintaining a vibrant and innovative ecosystem that supports the continued development of new products. In this briefing, the BKCIS team builds on a series of bilateral and multilateral consultations[2] and seeks to summarize and translate selected findings from privacy and cybersecurity research into practical considerations and takeaways that might be helpful to non-academic stakeholders. This document and much of the underlying research is enabled by generous support by the Ford Foundation.

Part I of this briefing is an **ecosystem map**, i.e., a high-level survey of the following features of the cybersecurity ecosystem:

- Tectonic shifts – the fundamental forces in technology, business, and markets that have a significant impact on cybersecurity threats and policy.
- Landscape Snapshot – a survey of the cybersecurity environment and the challenges affecting stakeholders.
- Tensions – the considerations and competing values that make it difficult for decision-makers to effectively craft cybersecurity policies.

Part II of this briefing is an **action map**, which offers a high-level overview of several current approaches aimed at addressing cybersecurity challenges. It highlights how these approaches operate, provides some examples of these approaches in action, identifies the underlying values that these approaches represent, and raises guiding questions.

Part III of this briefing is a **navigation tool**, i.e., that looks ahead to emerging cybersecurity challenges in order to guide decision-makers. It identifies opportunities for collaborative approaches that will help prepare decision-makers for addressing the next generation of pressing cybersecurity issues concerning companies, legislatures, and law enforcement agencies worldwide.

---

1 The White House, "Cybersecurity National Action Plan," February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

2 For previous BKCIS work in the privacy and cybersecurity space, please visit https://cyber.law.harvard.edu/research/cybersecurity; World Economic Forum, "Global Agenda Council on Cybersecurity," 2016, http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf.

I. Ecosystem Map: Tectonic Shifts, Challenges, and Tensions

1. Tectonic Shifts

Across the Internet, tectonic shifts are taking place, fundamentally changing the way personal data is collected, stored, and transferred, disrupting technological paradigms and markets. On the scale of decades, the costs of producing hardware and software have plunged, and the computational capacity, throughput, and bandwidth of Internet infrastructure has drastically increased.

Cloud Computing Models. Fueled by these changes, cloud computing – which provides computational resources, software, and infrastructure as an on-demand service over the Internet – have become a common feature of the current landscape. Numerous products and services used by consumers are built on or integrate with cloud computing platforms. By extending software "into the cloud," today's products and services can offer consumers functionality and conveniences that were not possible fifteen years ago. For example, users are no longer limited by the amount of storage capacity on a device's hard drive; a user can, practically speaking, store an infinite amount of data through a cloud storage service and access it from anywhere over the Internet. Through an Internet connection, mobile and wearable devices with low-powered microprocessors can leverage the power of thousands of servers, neural networks, and machine learning algorithms to perform complex calculations. These features are often seamlessly integrated into a plethora of products and services, and the average consumer may not be aware of the mechanical underpinnings – they "just work."

Consumer Data Held by Vendors and Service Providers. Another consequence of the shift towards cloud computing is that Internet companies are increasingly the caretakers and stewards of consumer data.[3] This happens in a few ways. As individuals and organizations use cloud computing services, their personal digital byproducts, such as old emails, messages, photos, and documents, are redundantly stored on vendor-owned infrastructure for indefinite periods of time. Not only is this convenient for consumers, but data has also become a commodity for Internet businesses as they mine and monetize large quantities of data about individuals. In these arrangements, online services may be offered for no cost to the user and subsidized entirely by revenue from advertising. Some of this data is biographic and transactional, including information like first and last names, email addresses, postal addresses, phone numbers, business records, and other information. However, an increasing amount of it could be described as behavioral and inference-based, such as a user's social graph and relations, their interests, personal preferences, browsing history, clickstream, geolocation, the probability they will fall ill[4] or are pregnant,[5] and much more. Needless to say, such data can be very personal and potentially sensitive.

---

3 See Bruce Schneier, Feudal Security," December 3, 2012, https://www.schneier.com/blog/archives/2012/12/feudal_sec.html.

4 See, e.g., Shannon Pettypiece, "Hospitals Are Mining Patients' Credit Card Data to Predict Who Will Get Sick," Bloomberg, July 3, 2014, http://www.bloomberg.com/news/articles/2014-07-03/hospitals-are-mining-patients-credit-card-data-to-predict-who-will-get-sick.

5 See Charles Duhigg, "How Companies Learn Your Secrets," The New York Times, February 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Internet of Things. Everyday consumer products, public infrastructure, and industrial processes are increasingly controlled by computers and networked together. Fifteen years ago, Internet-connected toothbrushes, streetlights, power plants, and vehicles may have seemed an unnecessary luxury; today, this is a financially and technologically feasible proposition that lays a foundation for unpredictable utility and innovation. Powerful sensors can be embedded into small form-factors, augmenting devices to be more controllable, autonomous, cyberphysical, and environmentally aware. For example, a number of major companies have developed vehicles that can operate autonomously and more accurately than a human driver. Networked thermostats use an array of onboard sensors and data from the Internet to optimize heating and cooling cycles for power consumption and comfort. This movement has been referred to as the "Internet of Things" (IoT), and it is projected to be a major area of growth in the coming years. Some estimates predict 21 billion new "things" will be connected and in use by 2020.[6]

1. Snapshot of Today's Cybersecurity and Privacy Landscape

Over the last two decades, cybersecurity has evolved into a pressing issue. It sits near the top of government policy and boardroom agendas as the prevalence and severity of incidents continue to increase.

* Cybersecurity incidents of all stripes have become the norm. Thousands of data breaches are reported each year in the private sector, affecting nearly every industry sector and exposing the information of millions of individuals.[7] More are believed to occur but go unreported or unnoticed by the victims. Consumers unwittingly fall prey to individually-targeted schemes that compromise their online accounts, privacy, and personal computers.[8] Repressive governments are known to exploit software to target and surveil political dissidents.[9] Numerous corporations have had their intellectual assets stolen and networks dismantled in high profile incidents, including some believed to be the work of sophisticated government-sponsored hackers, cyber vigilantes, or hacktivists.[10] Federal and state government and political orga-

6 Gartner, "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015," November 10, 2015, http://www.gartner.com/newsroom/id/3165317.

7 See, e.g., Symantec, "Internet Security Threat Report," April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf; Verizon, "2016 Data Breach Investigations Report," http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

8 See, e.g., Brian Krebs, "Ransomware getting more targeted, expensive," Krebs on Security, September 16, 2016, http://krebsonsecurity.com/2016/09/ransomware-getting-more-targeted-expensive/; Benjamin Wittes, et al., "Sextortion: Cybersecurity, teenagers, and remote sexual assault," Brookings Institution, May 11, 2016, https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/.

9 Targets UAE Dissidents," May 29, 2016, https://citizenlab.org/2016/05/stealth-falcon/; John Scott-Railton, et al., "Packrat: Seven Years of a South American Threat Actor," December 8, 2015, https://citizenlab.org/2015/12/packrat-report/.

10 See, e.g., "China's Cyber-Theft Jet Fighter," The Wall Street Journal, November 12, 2014, http://www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777; Devlin Barrett, "FBI Says North Korea Behind Sony Hack," The Wall Street Journal, December 19, 2014, http://www.wsj.com/articles/fbi-says-north-korea-behind-sony-hack-1419008924; Tony Cappacio, David Lerman, and Chris Strohm, "Iran Behind Cyber Attack on Adelson's Sands Corp., Clapper Says," Bloomberg, February 26, 2015, http://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says; JM Porup, "How Hacking Team got hacked," Ars Technica, April 16, 2016, http://arstechnica.com/security/2016/04/how-hacking-team-got-hacked-phineas-phisher/.

nizations, too, have reported serious breaches of the most sensitive employee information.[11] The motivations behind these incidents is varied, spanning espionage, surveillance, law enforcement, warfare and armed conflict, civil disobedience, geopolitics, and fraud.[12]

Case Example: Sony Pictures

In 2014, Sony Pictures was the victim of a devastating security incident, which took offline more than half of Sony's global network and erased the data stored on thousands of workstations and servers. Over a period of several weeks, confidential information, unfinished movie scripts, unreleased films, email spools with candid correspondence between senior executives and celebrity, employee social security numbers, salary information, and more were dumped onto public websites by the hackers for the world to see.[13] The attack is believed to have been carried out on behalf of the North Korean government, which was upset over The Interview, a comedy film being produced by Sony Pictures that depicted an assassination attempt on a North Korean dictator.[14] In the aftermath, stories emerged about how the company's lax information security practices may have contributed to the incident.[15]

* Despite government and private sector efforts in the past decade to promote trustworthy and secure computing, many cybersecurity issues only seem to get worse.[16] Vulnerabilities – design and implementation defects – plague software, and adversaries can exploit them to gain access to computers and networks to exfiltrate data, gain control of critical systems, and disrupt services. Software developers and vendors try to combat such threats by building in and bolting on security countermeasures and releasing "patches," which mitigate and eliminate some threats through software updates. However, many vendors and distributors do not issue updates expediently, if at all, and many users do not apply updates when they are issued. Some vendors and service providers have offered greater security by encrypting user data stored on devices and in transit across their networks; however, enabling encryption by default has proven to be somewhat controversial.[17]

* Beyond the prevalence of vulnerabilities, other key aspects of the problem can be traced to human error, a lack of standards, and weak adherence to the standards that do exist. Many security risks are well known and could be avoided by following basic "cyber hygiene," but or-

11 See Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," The New York Times, July 9, 2015, http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.htm; David Sanger and Nick Corasaniti, "DNC Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump," The New York Times, June 14, 2016, http://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html.

12 Although none of the incidents we cite in this section are known to constitute acts of war in a legal sense, many recent incidents carried out or commissioned by government actors have raised questions about where such lines are drawn in the cyber domain. Perhaps the leading example of this is the Stuxnet worm, discovered in 2010, which was believed to be a joint US and Israeli cyber campaign to sabotage a uranium enrichment facility in Iran. See Ellen Nakashima and Joby Warrick, "Stuxnet was work of US and Israeli experts, officials say," The Washington Post, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

13 See Peter Elkind, "Inside the Hack of the Century: Part 1: Who was manning the raparts at Sony Pictures", Fortune, June 25, 2015, http://fortune.com/sony-hack-part-1/; Amanda Hess, "Inside the Sony Hack", Slate, November 22, 2015, http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

14 Devlin Barrett, "FBI Says North Korea Behind Sony Hack," The Wall Street Journal, December 19, 2014, http://www.wsj.com/articles/fbi-says-north-korea-behind-sony-hack-1419008924

15 See Bruce Schneier, "Sony Made It Easy, but Any of Us Could Get Hacked", The Wall Street Journal, December 19, 2014, http://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701.

16 See, e.g., Bill Gates, "Trustworthy Computing," WIRED, January 17, 2002, http://www.wired.com/2002/01/bill-gates-trustworthy-computing/; U.S. Department of Homeland Security, "Software Quality Assurance," https://www.dhs.gov/science-and-technology/csd-sqa.

17 James B. Comey, Federal Bureau of Investigation Director, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech delivered to Brookings Institution, October 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

ganizations and individuals often fail to take these steps.[18] For example, mistakes introduced by human error – e.g., misconfigurations of security settings – can inadvertently introduce vulnerabilities and weaknesses. Social engineering attacks in which adversaries deceive users into divulging account credentials also play a significant role in security incidents.[19] These types of attack are both highly effective and especially difficult to guard against.

* The existence of software and human vulnerabilities are not new security challenges, but they are exacerbated by the tectonic shifts in the landscape. For example, as more connected devices and services are coming online, such as IoT products, the "attack surface" – the vectors through which adversaries can exploit systems – is increasing at a similar rate (or greater). An exploitable vulnerability in one system can be a vulnerability in all systems networked with it. Moreover, as software and systems become more complex, it also becomes commensurately more difficult to anticipate security and privacy risks.

* Meanwhile, adversaries are growing more sophisticated and the targets more attractive. Gray and black markets make it easy to acquire hacking tools, software vulnerabilities, and exploits. With more tools available, cyber criminals have evolved from individual actors into a highly-networked system of criminal enterprises around the globe.[20] We have also seen the emergence of the so-called "advanced persistent threats" – well-resourced and highly-skilled groups of adversaries believed to be backed by governments, which penetrate private and public sector organizations. The targets of these threats are evolving too. A handful of large companies in particular are becoming stewards of large amounts of data as they increasingly become centralized platforms on which many other services and Internet-connected products rely, making them tempting targets for malicious actors. And, the proliferation of cloud-based services and the sensors and networked components of the IoT, such as microphones, cameras, and industrial control systems, to name but a few, presents new opportunities for surveillance and privacy incursions on an unprecedented scale.[21]

Case Example: Targeting Political Dissidents

A number of reports have emerged in recent years documenting attempts to identify and monitor political dissidents, journalists, activists, and others in sophisticated hacking and social engineering operations. In some cases, attacks on dissidents intend to cause physical damage to computer systems or data, and manipulate the availability or integrity of content published online.[22] Such incidents take place around the world, and are often thought to be led by governmental and state sponsored organizations.[23]

---

18 *See e.g.*, World Economic Forum, "Global Agenda Council on Cybersecurity," 2016, http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf.

19 *See* Alex Stamos, "Addressing Security Blindspots through Culture," August 1, 2016, https://www.facebook.com/notes/alex-stamos/addressing-security-blindspots-through-culture/10154390896047929.

20 *See, e.g.*, Ponemon Institute, "Flipping the Economics of Attacks," January 2016, http://media.paloaltonetworks.com/lp/ponemon/report.html; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," *RAND*, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

21 *See* Urs Gasser et al., Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Research Publication 2016-2 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/.

22 "A Human Rights Response to Government Hacking," Access Now, September 2016, https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf;

23 See, e.g., Bill Marczak and John Scott-Railton, "Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents," May 29, 2016, https://citizenlab.org/2016/05/stealth-falcon/; John Scott-Railton, et al., "Packrat: Seven Years of a South American Threat Actor," December 8, 2015, https://citizenlab.org/2015/12/packrat-report/.

* Stakeholders disagree about the best solutions to solve the many problems. For example, some have advocated for creating new government regulations and liability, while others think the private sector is better suited to create solutions free of regulations. Although this debate has yet to be resolved, stakeholders are not standing still. Both domestic government and private sector organizations have pursued new initiatives. For example, legislation was introduced in 2016 in the U.S. to facilitate threat information sharing between stakeholders, and the U.S. National Institute of Standards and Technology (NIST) has collaborated with the private sector to develop new standards frameworks.[24] Unilateral efforts are insufficient as the issues are increasingly international in nature: the victims as well as the adversaries responsible for attacks are located around the world. Policy debates reflect this trend, particularly around contentious issues such as encryption, international law enforcement requests for data, and data localization efforts. Fragmentation across national and supranational boundaries also continues to be a challenge for multinational companies as they navigate a diverse set of standards, laws, and policies worldwide, while trying to ensure the preservation and security of users' data.

Tensions, Tradeoffs, and Other Considerations

Beneath the surface are numerous tensions and tradeoffs that compound cybersecurity and privacy issues. They help answer the question of how we arrived at this point. They also punctuate the complexity of the issues and explain why satisfactory solutions are elusive. In this section, we explore a selection of these tensions and tradeoffs in rapid succession, highlighting those most emblematic of the status quo and the stakeholder groups they affect.

Consumers (including individual users and organizations)

- **Loss of Control.** Consumers have become reliant on vendors to provide security and privacy. Many vendors can be more effective at securing systems than the average consumer. However, consumers are ill-equipped to verify the claims of vendors. Moreover, a lack secure alternatives and high switching costs limit the viability of substitutes.
- **Demand for Security and Privacy.** Recent polls on privacy and security suggest an increasing number of consumers care deeply about privacy and security issues,[25] however this does not seem to be reflected in purchasing habits and security practices. One explanation is that other factors, like price and convenience, are more determinative; another is that consumers lack the knowledge and information to adequately make decisions based on security and privacy.[26]

---

24 U.S. National Institute of Standards & Technology, "Cybersecurity Framework for Improving Critical Infrastructure," Version 1.0, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

25 *See, e.g.,* Mary Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," *Pew Research Center,* May 20, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

26 *See, e.g.,* Joel Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (New York: Penguin, 2010); J. Alex Halderman, "To Strengthen Security, Change Developers' Incentives," *IEEE Security and Privacy* (March/April 2010): 79-82.

- **Convenience, Usability, and Autonomy.** Software products and services that are more secure are often more difficult to engineer and use. A product that is difficult to use may not be viable in the marketplace. Similarly, onerous security policies can push end users to circumvent security controls for the sake of convenience.
- **Security and Privacy as Premium Products.** While some companies offer products with security features enabled by default, many do not. Those that do are typically higher-cost, premium products and services, such as Apple's iPhone. In contrast, low cost devices tend to have more security vulnerabilities that are less frequently patched by vendors. This creates the risk of a segregated society that offers additional security and privacy only to those who can afford it.[27]

Producers (including software developers, vendors, and service providers)

- **Competition and Market Forces.** To keep pace with the competitive global marketplace for software goods and services, many producers have shifted toward rapid software development lifecycles, often trading security for speedy development. For example, it is common for new products and services to ship with known vulnerabilities or without undergoing a thorough security review.
- **Allocation of Resources and Knowledge Within Organizations.** Money, time, and personnel are finite resources for producers that must be justified as they are invested and allocated. Security is costly, and is often viewed as an expense rather than an investment – on a balance sheet, security does not add revenue even when it is effective.[28] The lack of liability has also minimized the costs of security incidents, which can make it difficult to justify allocations for preventative security and support for older products. Security knowledge, expertise, and talent are frequently cited as lacking across organizations. The emerging cyber insurance industry has also struggled to quantify risks and encourage producers to adhere to a common set of best practices.
- **Silos and Information Sharing.** Concerns about leaks, antitrust violations, and regulatory scrutiny have constrained information flows between the public and private sectors. As a result, information silos within governments and companies make it difficult to share information about vulnerabilities and security threats.
- **Independent Security Research and Vulnerability Disclosures.** Although "bug bounty" programs in which companies award independent security researchers for discovering and disclosing vulnerabilities have been successful, not all software vendors offer them. A large number of researchers have reported that companies and vendors have threatened them with lawsuits and criminal actions over their

27 See, e.g., Tom Simonite, "Why Google Trailing Apple on Encryption Support is a Human Rights Issue", MIT Technology Review, November 3, 2015, https://www.technologyreview.com/s/543161/why-google-trailing-apple-on-encryption-support-is-a-human-rights-issue/.

28 See Bruce Schneier, "Security ROI: Fact or Fiction?," CSO Online, September 2, 2008, http://www.csoonline.com/article/2123096/metrics-budgets/security-roi--fact-or-fiction-.html.

research, chilling further research.[29] Instead of disclosing vulnerabilities to vendors, security researchers can be lured by lucrative black and gray markets in which buyers – including military, intelligence, law enforcement, and hackers – pay top dollar.

- **Regulatory and Legal Systems.** Software developers, vendors, and service providers are generally not held liable for damages that stem from latent and known vulnerabilities in products and services. The exceptions lie within regulated industrial and critical infrastructure sectors, such as transportation, energy, finance, and healthcare. Even so, it is rare for consumers to recover the full costs of harms from cybersecurity incidents, making it less likely for companies to take into account the societal costs.

Government Organizations (including policy-makers, regulators, law enforcement, and military)

- **Public-Private Trust Deficits.** Since the Snowden revelations in 2013, trust between the US government and private sectors has been especially low.[30] Many multinational technology companies have taken steps to distance themselves from the government.
- **Government Roles and Regulatory Policy.** The legal and regulatory system is slowly and cautiously evolving in response to the tectonic shifts. The U.S. government, for instance, has opted to eschew regulating and mandating software security standards, due to lack of expertise and to avoid impeding economic growth. Instead, the U.S. government often operates as a facilitator and convener of bottom-up efforts, by rallying producers around standards and self-regulation, and educating consumers about best practices.
- **Civil Liberties, National Security, and Foreign Policy.** Security and privacy protecting technologies, such as encryption, can be useful tools for countering many of the cybersecurity threats we face. At the same time, these same tools can be used by malicious actors to hinder law enforcement surveillance and prosecution. This raises difficult questions about how such conflicts should be reconciled with other priorities like national security and the promotion of democratic values through foreign policy.
- **Government Exploitation of Vulnerabilities in Commercial Software.** Military, intelligence, and law enforcement agencies discover, acquire, exploit, and stockpile software vulnerabilities in commercial, off-the-shelf software for use in offensive operations and investigations. Some commentators have warned that such practices could potentially endanger the public should an adversary exploit vulnerabilities in commercial software undisclosed by the government. This raises difficult questions about the degree to which the public's interests would be better served by policies that prioritize disclosure over stockpiling.

---

29 See, e.g., Malena Carollo, "Influencers: Lawsuits to prevent reporting vulnerabilities will chill research," CSM Passcode, http://passcode.csmonitor.com/influencers-research.

30 See Ellen Nakashima, "NSA tries to regain industry's trust to work cooperatively against cyber-threats," The Washington Post, October 10, 2013, https://www.washingtonpost.com/world/national-security/nsa-tries-to-regain-industrys-trust-to-work-cooperatively-against-cyber-threats/2013/10/09/93015af0-2561-11e3-b3e9-d97fb087acd6_story.html.

Case Example: Encryption, "Going Dark," and Apple v. FBI

For the last several years, officials from the Federal Bureau of Investigation in the U.S. and other law enforcement entities abroad have raised alarms over what they see is a concerning trend: communications are "going dark." That is, major technology companies – including Apple, Google, and WhatsApp – are implementing security features, such as end-to-end encryption and disk encryption schemes, in their communications products and services in a way that puts user data beyond the investigative reach of the government, even in circumstances when the law would otherwise permit government access. Many within governments fear this will make it far more difficult to conduct investigations, prevent terrorist attacks, and enforce national security interests. One manifestation of the debate transpired during a legal fight in early 2016 in which the FBI asked a federal court to compel Apple to unlock an iPhone used by a perpetrator in the San Bernardino mass shooting. On the other hand, the companies implementing these features believe these stronger measures are needed to mitigate the growing number of security threats and to protect the privacy interests of individuals. And, as noted in a February 2016 Berkman Center report, *Don't Panic: Making Progress on the 'Going Dark' Debate*, questions remain about the degree of "darkness" in the future landscape given the emergence of the Internet of Things, a desire to monetize user data, and other forces that will influence the trajectory.

II. Action Map

In addressing the range of challenges described above, a wide range of governance mechanisms have been identified, discussed, and implemented as solutions. To give but a few examples:

- The implementation of open, well-documented standards could substantially boost the security of certain products or services.
- New regulations could require that vendors adhere to a particular standard of design, or that they practice a degree of openness around their security and privacy practices.
- Safe harbor laws could enable public and private sector entities to share with each other information about threats, incidents, and vulnerabilities without fear of repercussions.
- Bolstering the quality of cyber insurance offerings may help companies more accurately allocate costs in proportion to risk.

* Such interventions could be implemented in a number of ways and in various combinations, which makes it difficult to describe all the possibilities on the pareto frontier. For instance, in some cases, government actors or industry leaders are best positioned to push these interventions from the top down. In other cases, a diverse collaboration of actors from industry, civil society, and academia are best positioned to build support for change from the bottom up. Interventions can also vary in scope, with some targeting a specific ill, others addressing the whole of the ecosystem directly, and others indirectly reaching objectives through first and second order effects.

The action map that follows provides a high-level sampling of different possibilities for governance mechanisms, including current representative uses and proposals, organized by modality: technology, market, norms-based, law, and blended governance approaches. This is not to say any of these are the best, the most effective, or the only choices – the pathways forward are uncertain and rife with tradeoffs, and many unlisted ideas deserve more study.

Action Map

	Tech-based	Market-based	Human-centered	Law	Blended
Approaches	Initiatives aimed at new or existing technologies that enhance privacy and security in networked environments	Mechanisms that act through market incentives to influence individual and organizational behaviors around privacy and security	Mechanisms that target the behaviors of individuals	Addition of new or reform of existing laws, regulations, and policies to address security and privacy challenges	Interrelated use of more than one of the tech, market, human, and law-based mechanisms to address multi-dimensional security and privacy problems
Examples	**NIST Cybersecurity Standards:** A voluntary set of cybersecurity standards and best practices to help organizations manage cybersecurity risks.[31] **The Tor Project and Community:** A project that develops open software protects privacy of Internet traffic. **AI2:** A collaboration between MIT's CSAIL and PatternEx, a cybersecurity startup, which developed a system for detecting, preventing, and stopping cyberattacks using artificial intelligence.[32]	**DHS Innovation Call:** A government-led program to fund startup companies developing solutions for securing commercial and governmental IoT environments.[33] **Bug Bounty Programs:** Initiatives in which companies reward developers for the discovery and responsible disclosure of software vulnerabilities.[34]	**Stop.Think.Connect:** A national public awareness campaign to increase the public's understanding of cybersecurity threats.[35] **National Cybersecurity Workforce Framework:** An initiative aimed at equipping and encouraging individuals to pursue careers in the cybersecurity.[36] **Berkman Klein Assembly:** An exploratory BKCIS program aimed at bringing together developers and other technology professionals to develop collaborative solutions to vexing cybersecurity problems.	**Cybersecurity Information Sharing Act:** Passed in 2015, this law aims to facilitate the sharing of information about threats between public and private sector organizations through liability safe harbors. **State Breach Notice Laws:** 48 states have enacted laws that require holders of personal information to notify consumer when their personal information has been compromised in a security incident.	**Cyber Independent Testing Laboratory:** A new, non-profit company funded by DARPA that will test and issue consumer reports about the security of off-the-shelf commercial software to educate consumers about risky software and incentivize companies to avoid common security mistakes as the develop products.
Values	Preservation of the open and generative Internet; protection of individual privacy	Promotion of the autonomy of market actors; inclusion and promotion of diversity in solution space	Promotion of consumer agency and autonomy through the fostering of a more well-informed user base	Preservation of public and individual safety through laws and regulations; promotion of transparency and accountability	Inclusion of multi-stakeholder models; promotion of diversity in perspectives and approaches
Sample Questions	What tools and guidance are needed to improve the overall state of security in software and hardware that preserve the open, generative nature of the internet?	How can the market forces be supplemented to encourage organizations and individuals to ensure a vibrant marketplace of products that offer strong security for those that use them?	What interventions at the individual level are effective in promoting a robust cyber workforce and consumer populations that take measure to mitigate risks?	What changes should be made to the law in response to the new security and privacy challenges we are likely to face in the future?	Can multiple approaches be used to address the issues from different angles?

31 NIST, "Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0," February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

32 Adam Conner-Simons, "System predicts 85 percent of cyber-attacks using input from human experts," MIT News, April 18, 2016, http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418.

33 U.S. Department of Homeland Security, "DHS S&T Releases Innovation Call Aimed at Startups," December 11, 2015, https://www.dhs.gov/news/2015/12/11/dhs-st-releases-innovation-call-aimed-startups.

34 See, e.g., HackerOne, a bug bounty platform for sharing vulnerabilities and coordination. https://hackerone.com/.

35 U.S. Department of Homeland Security, "Stop.Think.Connect. Toolkit," last published September 8, 2016, https://www.dhs.gov/stopthinkconnect-toolkit.

36 U.S. Department of Homeland Security, "Cybersecurity Education & Career Development," last published April 13, 2016, https://www.dhs.gov/topic/cybersecurity-education-career-development.

III. Navigation Aid (Identification of Key Opportunities)

As we look beyond the current challenges and interventions, we recognize that this complex ecosystem will continue to evolve. It is important for decision-makers to anticipate and prepare for the next generation of cybersecurity and privacy challenges.

Given the numerous complexities and tensions in play, the emerging challenges and interventions are not obvious. However, what is clear is that stakeholders, including government, private sector, civil society, and academia, must work collaboratively to address the emerging challenges and find solutions that overcome many of the current obstacles to successfully mitigating cybersecurity risk. With this in mind, we identify four broad categories of opportunities for collaborative approaches:

1. **Information sharing and horizon scanning** – opportunities for identifying and responding to upcoming technological and policy shifts;
2. **Impact assessments** – opportunities for assessing the impact of regulation and other interventions;
3. **Transparency and education** – opportunities for improving communications with consumers about cybersecurity issues; and
4. **Accountability and liability** – opportunities to change how the costs of cybersecurity failures are internalized and improve how the public and private sectors allocate cybersecurity risks.

Below are some examples of – and by no means the only – opportunities within each category.

- **Information Sharing and Horizon Scanning:** decision-makers could engage in collaborative, multistakeholder horizon scanning exercises to better anticipate how technological and policy developments are shaping this quickly evolving ecosystem.

    - » Decision-makers could convene stakeholders to engage in information sharing and discuss emerging threats and approaches in cybersecurity, and exchange actionable informatOion. These conversations should aim to break down private-to-private and public-private information silos, leveraging a diversity of perspectives to help highlight trends as they emerge to ensure that decision-makers fully understand the current cybersecurity landscape and its trajectory in the future. Such convenings could also serve as early-warning mechanisms to help stakeholders identify potentially divergent interests.
    - » Decision-makers could develop exchange programs in which employees from one organization spend time at another as a means of sharing information, expertise, and to experience the challenges from another perspective. For example, government employees of one agency could be temporarily assigned to another government agency. Likewise, a private sector employee or member of academia could temporarily work for a government agency in an advisory role, which has worked well in the past for organizations like the U.S. Federal Trade Commission.[37]

37 See, e.g., U.S. Federal Trade Commission, "FTC Names Edward W. Felten as Agency's Chief Technologist; Eileen Harrington as Executive Director," November 4, 2010, https://www.ftc.gov/news-events/press-releases/2010/11/ftc-names-edward-w-felten-agencys-chief-technologist-eileen.

- **Impact Assessments:** decision-makers could benefit from a more accurate understanding of the tensions in the ecosystem as well as the likely effectiveness and the tradeoffs of potential solutions, including new regulations, industry-led efforts, and other interventions.

    » Decision-makers could convene stakeholders from industry and government to discuss and catalog potential interventions, like regulation or a tort regime for software development, while debating and sharing the potential impacts that might affect various stakeholder.

    » Decision-makers could support additional research on the economic impact of inventions by examining other, historically comparable and analogous regulated industries in order to develop testable hypotheses for measuring the impact of various interventions in the cybersecurity ecosystem.

- **Transparency and Education:** decision-makers could foster a series of educational reforms and transparency initiatives to help consumers understand the impact of cybersecurity and take steps to better protect themselves. But for such interventions to be effective, additional research may be required. For example, what are the most impactful methods for communicating to consumers about the cybersecurity of products and services? How would disclosures likely impact consumer purchasing decisions? How can decision-makers ensure that private entities provide fair, truthful, and actionable information to consumers? What is the optimal balance of regulatory disclosure requirements, spanning a spectrum from simply encouraging voluntary disclosures, to mandated self-reporting (e.g., nutrition label-like approaches), to third-party disclosures (e.g., government or independent testing laboratories conducting tests and providing the disclosures)?

    » Decision-makers could work with stakeholders from across industry and government to discuss potential methods and approaches for measuring and communicating about cybersecurity practices.
    » Decision-makers could support the development of prototype disclosures and test them with small samples of consumers. After testing and iterating on draft disclosures, decision-makers should publish the draft standard in order to further advance the debate about transparency.
    » Decision-makers could also collaborate with cybersecurity testing laboratories to support their efforts to measure and improve the effectiveness of their transparency efforts.

- **Allocation of Risks and Decision-making:** decision-makers could develop a collective understanding of the private and societal costs of allocating risk and the necessity of responsible decision-making, particularly around the proliferation of insecure software and poor cyber hygiene. These efforts could help identify the practices that undermine our broad interests in maintaining a secure and trustworthy software ecosystem as well as those that would strengthen them.

» Decision-makers could work with other stakeholders to understand how their interests affect decision-making, with an eye towards developing firm-level decisions that critically affect the ecosystem as a whole. This could inform the creation of voluntary best practices to aid software developers and vendors as they make business decisions that implicate privacy and cybersecurity interests.
» Decision-makers could work with key stakeholders, including software developers and vendors, and insurance companies, to discuss new governance mechanisms that would help all parties best internalize the costs of cybersecurity risks.

About the Authors

Ryan Budish is a Senior Researcher at BKCIS, and a lawyer. In his time at Berkman, Ryan has contributed policy and legal analysis to a number of projects and reports, and he has led several significant initiatives relating to cybersecurity, Internet censorship, corporate transparency about government surveillance, and multistakeholder governance mechanisms.

Rob Faris is the Research Director of BKCIS at Harvard University. His recent research includes Internet content regulation, state censorship and surveillance practices, broadband and infrastructure policy, and the interaction of new media, online speech, government regulation of the Internet and political processes.

Urs Gasser is the Executive Director of BKCIS and a Professor of Practice at Harvard Law School. He is a visiting professor at the University of St. Gallen (Switzerland) and at KEIO University (Japan), and he teaches at Fudan University School of Management (China).

Tiffany Lin is a Research Associate at BKCIS. She supports research and activities for the Center's cybersecurity and open data projects, including the Berklett Cybersecurity project and the Assembly program.

David R. O'Brien is a Senior Researcher at BKCIS, and a lawyer. He leads research efforts at BKCIS related to privacy and cybersecurity, including the Berklett Cybersecurity project and Privacy Tools for Sharing Research Data project.

This paper and the other briefings included as part of the Networked Policy Series are generously supported by the Ford Foundation and the John D. and Catherine T. MacArthur Foundation.