Cybersecurity Research:
Addressing the Legal Barriers and Disincentives

Report of a Workshop convened by the Berkeley Center for Law & Technology, the UC Berkeley School of Information and the International Computer Science Institute under a grant from the National Science Foundation

Award No. (FAIN): 1541803

NSF Program Solicitation: 14-599, Secure and Trustworthy Cyberspace (SaTC)[*]

September 28, 2015

Background

It is blindingly clear that corporate, governmental and non-profit computer systems are vulnerable to attack. These vulnerabilities expose personal information,[1] strategic government assets,[2] corporate secrets, and personal safety to unacceptable levels of risk.[3] There is an urgent need to improve the security of these systems, and cybersecurity research is essential to these improvements. However, inquiry into vulnerabilities and threats remains hampered by fears of legal liability arising under multiple U.S. laws and is further chilled by private ordering—contracts and other forms of soft and hard restrictions that arise in the shadow of the law—that deters research. Researchers fear that their work could put them in personal legal jeopardy. Universities and other research institutions are concerned with potential liability, as well as reputational damage. Institutional structures such as human subjects review boards, conference committees, and journal boards raise concerns about work that treads too close to ethical and legal lines. Thus those who do undertake

[*] The workshop was supported by National Science Foundation grant (FAIN): 1541803. This report was drafted by Deirdre Mulligan, Nick Doty, and Jim Dempsey, with input from Pam Samuelson, Stefan Savage, Vern Paxson, and Joseph Lorenzo Hall.

[1] See, for example, Elizabeth A. Harris, Nicole Perlroth, Nathaniel Popper and Hilary Stout, "A Sneaky Path Into Target Customers' Wallets," New York Times, January 17, 2014 (reporting on theft of 40 million customers' credit card information).

[2] See, for example, Michael Riley and Jordan Robertson, "China-Tied Hackers That Hit U.S. Said to Breach United Airlines," Bloomberg Business, July 29, 2015 (the compromised data included records of passengers origins and destinations that could provide travel details on many government employees and could be aggregated with data from the OPM and other breaches, providing China with a growing database on US defense and intelligence officials); and Cory Bennett, "Lynch: OPM hack could out secret agents," The Hill, July 28, 2015 (reporting loss of 21.5 million individuals' security clearance information in hack of OPM database).

[3] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired, July 21, 2015 (reporting on researchers' ability to remotely seize control of a moving vehicle, and crash it, through the entertainment system's wi-fi connection).

research find it difficult to publish their work at conferences and journals, due to concerns over research methods, findings, potential consequences of disclosure, or a mix of the three.

The problem of liability risks associated with cybersecurity research is widely recognized within the computer science and related legal community. However, there has been little progress made in addressing these concerns. The uncertainty level and the consequent self-censorship remain high; uncertainty alone makes researchers steer away from valuable lines of inquiry.

While the issue has become acute, there are opportunities for progress. The Copyright Office's triennial review of exemptions in the Digital Millennium Copyright Act (DMCA) is underway, and it specifically includes a proposed set of exemptions for cybersecurity, offering one key venue for clarifying the scope of that law.[4] The Administration's recent legislative proposal to amend the cybercrime laws set off another round of concern,[5] but the prospect of legislative action on cybercrime also opens the possibility of clarifying amendments to the Computer Fraud and Abuse Act or the electronic communications privacy laws (the Wiretap Act, the Pen/Trap Statute, and the Electronic Communications Privacy Act (ECPA)). Perhaps most importantly, the recall of 1.4 million vehicles by Chrysler in the wake of a demonstrated over-the-air hack by two researchers that enabled them to control the steering, acceleration, braking, and other functions of a vehicle through its entertainment system—and the agency and congressional activity it triggered—suggests that there is an opportunity for a larger conversation about how to support and encourage a robust cybersecurity vulnerability research ecosystem.

Supported by the National Science Foundation, researchers associated with the Berkeley Center for Law and Technology, the UC Berkeley School of Information and School of Law, and the International Computer Science Institute (ICSI) convened on April 9 and 10, 2015, a workshop of leading computer scientists and lawyers, from academia, civil society, and industry, to map out the problem and propose a set of concrete solutions. A list of participants is attached as Appendix 1. The agenda for the workshop is attached as Appendix 2.

The goals of the workshop ran along three axes:

- Understand and document research that has not been undertaken because of fears of legal liability, identify other real-world examples of adverse impact of the laws or of the uncertainty surrounding those laws on research, and, if possible, quantify or otherwise effectively convey the cost of this chilling effect on research.
- Identify and/or develop reasonable norms, standards or best practices for the conduct of cybersecurity research that could be used to protect responsible research and provide guidance to policymakers to reduce the impact of existing statutes on cybersecurity research through the use or creation of exemptions or other appropriate mechanisms.
- Outline larger reforms to existing laws or other policy clarifications, such as DMCA exemptions, that would reduce risks of liability for the conduct and dissemination of cybersecurity research and additional research that might inform their creation.

[4] See http://copyright.gov/fedreg/2014/79fr73856.pdf and http://copyright.gov/1201/ .

[5] See Jen Ellis, "Will the President's Cybersecurity Proposal Make Us More Secure?" (Jan. 23, 2015) https://community.rapid7.com/community/infosec/blog/2015/01/23/will-the-president-s-cybersecurity-proposal-make-us-more-secure

The Value of Cybersecurity Research

Cybersecurity is an urgent national priority. Vulnerabilities in a wide range of digital devices, systems, and products, including critical infrastructure, can and have been exploited to undermine national security, economic prosperity, and personal privacy. The rapid emergence of the Internet of Things heightens the risk, as consumer products widely used in daily life, ranging from automobiles to medical devices to thermostats and home appliances, become connected to the Internet and thus vulnerable to remote manipulation, exploitation, and attack. The growing complexity and interdependencies among devices and networks compounds the risks, making it increasingly important to assess, and address, vulnerabilities in technically and socially complex real world settings.

In this environment, cybersecurity research is vital. Security by obscurity—the notion that vulnerabilities can be kept hidden from adversaries and remain unexploited—has failed in the past and is particularly poorly suited to today's interconnected environment that is replete with wily, malicious, and increasingly better funded adversaries.

Corporate, governmental, academic, and independent cybersecurity researchers all contribute to identifying and remediating cybersecurity vulnerabilities. Cybersecurity research has advanced the security, trustworthiness, and resilience of systems ranging from cyberphysical systems, to voting systems, to medical devices. It has benefited human health and safety, protected democratic self-governance, and shored up systems essential to the economic and physical wellbeing of the nation. Much further positive work could be done if the legal barriers to research were lowered.

Three examples highlight the value of cybersecurity research:

- **Automobile safety and security**: Modern automobiles are becoming increasingly computerized — with many components controlled partially or entirely by computers and networked both internally and externally. While this architecture provides many benefits, the risks have not been carefully considered or addressed by the automotive industry. University researchers and others have begun to examine these risks, yielding important findings. They have showed that existing automobiles are extremely fragile to attack and that a range of vectors (including dealership shop tools, media players, Bluetooth and cellular telematics connections) all can be used to compromise even safety critical components (e.g., remotely disabling the brakes).[6] This was research that was not being pursued by the automotive industry, involved extensive reverse engineering of automotive systems, and has had major positive concrete impacts for the public. The visible side effects of this work include the establishment of a new cybersecurity standards effort undertaken by the Society of Automotive Engineers, a cyber security testing and evaluation capability being created by the Department of Transportation's National Highway and Traffic Safety Administration (NHTSA), a $60M research program created by DARPA (HACMS) to develop new technologies to increase vehicle security, the introduction of a Senate bill that would regulate

[6] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX Security, August 2011, available at http://www.autosec.org/publications.html.

automotive cybersecurity,[7] and significant automotive industry investment in cybersecurity. (For example, Eric Gassenfeit, OnStar's chief information security officer, has been publicly quoted as saying that his team has had its resources and staff grow "by an order of magnitude" in the period after the publication of cybersecurity research undertaken by academic researchers.[8]) All of these benefits accrued only because the researchers took risks that they should not have had to take.

- **Voting machine security and accuracy:** Research on voting machines identified significant vulnerabilities in the technical systems upon which the most fundamental act of our democracy relies. Election officials lacked the expertise to analyze these systems, and federal and state standards failed to deliver sound security, yet researcher access was limited by contracts that prohibited most forms of testing as well as reverse engineering. But for cybersecurity researchers willing to take risks, the investment of the National Science Foundation and several private foundations, the diligence of a handful of Secretaries of State, and the relentless activity of non-profits, the public would have remained unaware of the vulnerabilities in these systems, and election officials would have been unable to seek fixes to mitigate risks of election fraud and failure.[9] The majority of voting system vendors were hostile to independent security analysis of their systems and went to great lengths to prevent election officials and researchers from independently examining them. The work of security researchers led to the decertification of insecure voting systems, the adoption of new policies, procedures, and technologies, new methods of oversight and certification of machines, and improved training for election workers. Internet voting, which is now being promoted, deserves similar security research, but that research may be impeded by the laws mentioned above.

- **Medical device security:** Security researchers have uncovered fundamental flaws in devices such as pharmaceutical drug compounders, automated external defibrillators, ventilators, drug infusion pumps, and implantable medical devices.[10] Very few medical device companies have security engineering teams. Independent security researchers have taken the risk to publish security flaws in the public interest. In general, medical device engineers sincerely care about helping patients live longer and healthier lives. The devices save countless lives. However, the majority of medical device manufacturers lack the level of cybersecurity engineering maturity found in the information technology and finance sectors. Thus, medical device manufacturers often respond with hostility during a first encounter with a security researcher. The existing laws give companies unnecessary means of recourse that do not

[7] The Security and Privacy in Your Car Act of 2015, S. 1806, introduced July 21, 2015, https://www.congress.gov/bill/114th-congress/senate-bill/1806/all-info.

[8] Keith Barry, "Can Your Car be Hacked?" Car and Driver (July 2011) http://www.caranddriver.com/features/can-your-car-be-hacked-feature.

[9] See generally, D.W. Jones and Barbara Simons, BROKEN BALLOTS, Center for the Study of Language and Information (Stanford), 2012.

[10] Shane S. Clark and Kevin Fu, "Recent Results in Computer Security for Medical Devices," (2011) https://spqr.eecs.umich.edu/papers/clark-mobihealth11.pdf.

> protect patients from the most prevalent cybersecurity threats; the laws serve to chill research on medical device security.

The benefit of independent cybersecurity research is further underscored by the emergence of vulnerability rewards programs (VRPs), commonly known as "bug bounty" programs, developed by leading Internet companies to encourage adversarial research on their systems. These programs incentivize the reporting of information to software vendors and online service providers so that patches can be created to prevent exploitation. The programs are designed to promote disclosure to those in the position to patch them before discovered—but unreported—vulnerabilities can be sold on the black market as zero-day exploits. Not all vendors utilize VRPs, but those that do offer varying participation guidelines and incentive structures often including monetary rewards, recognition, or both.[11] At times, third party security vendors will set up VRPs for companies that do not independently offer incentives to report vulnerability information. For instance, in 2007 VeriSign offered monetary rewards for exploits found in the newly released Windows Vista operating system.[12] More recently, independent platforms like Bugcrowd,[13] HackerOne,[14] and Cobalt[15] bring together skilled and vetted security experts along with organizational resources so that a company of any size—not just those with enough resources to run their own independent bug bounties or hire their own team of security researchers—may run a comprehensive security audit, set up a VRP, and create responsible disclosure programs so that researchers may securely report vulnerabilities to the company. These platforms allow flexibility for vendors by allowing different incentive options including fixed pricing, pay-per-bug, and/or acknowledgements. The variety in available programs allows companies to make their programs and systems available to researchers so that they may pay or otherwise incentivize them to identify vulnerabilities, because those companies view external testing by security experts as essential to maintaining a strong security posture.

The Legal Landscape

Despite its importance to the development of safe, secure, trustworthy, and private systems, legal barriers to cybersecurity research are increasing. The legal impediments to cybersecurity research arise from various sources, including the Computer Fraud and Abuse Act, section 1201 of the Digital Millennium Copyright Act, and the wiretap laws.[16] Impediments also arise from contracts and

[11] *An empirical study of vulnerability rewards programs*, Proc. 22nd USENIX Secur. Symp. 273–289 (2013), https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf.

[12] "A Lively Market, Legal and Not, for Software Bugs," New York Times, 2007, http://www.nytimes.com/2007/01/30/technology/30bugs.html?=&_r=0.

[13] "Bugcrowd: Some Questions," 2015, https://bugcrowd.com/faq#faq-programs.

[14] "HackerOne: About," 2015, https://hackerone.com/product.

[15] "Cobalt: How it works,"2015, https://cobalt.io/how.

terms-of-service (the breach of which may expose one to criminal liability) that broadly prohibit modifications of devices or collections of data.[17] As the urgency of the cybersecurity threat has grown to affect more types of products and services, the inhibiting effect of these laws has spread. Meanwhile, contractual prohibitions on reverse engineering have proliferated. New categories—such as "sensitive security information"—have entered the legal lexicon,[18] statutes have been broadly interpreted, and technical protections have been added to an array of consumer products to limit tinkering and modification. While there are arguments that the laws at issue would not be used to actually prosecute legitimate cybersecurity research, the laws are ambiguous and can be broadly interpreted, generating uncertainty that has a wide chilling effect.

The chilling effect of these barriers takes many forms: Academic and other research institutions can be risk-averse, advising faculty and students to steer clear of research with unclear liability; faculty may advise students to work in areas less fraught with potential legal and public-relations challenges; and peer review may look unfavorably upon researchers whose work treads too closely to legal lines.[19] Funders may be reluctant to support certain kinds of research. Academic publication venues are forced to wrestle with questions regarding the legality of research, despite its public value. Papers have been both delayed and outright pulled due to court intervention, threats of suit by research subjects, and program committee concerns with potential liability exposure for the committee, the institution, or the venue.[20] Independent researchers face an outsized threat of criminal prosecution and civil litigation. Researchers at corporations face a chill as well, because the questionable legality of certain security research may raise an appearance of impropriety if another company's technology is the subject of analysis.

[16] Aaron J. Burstein, "Amending the ECPA to Enable a Culture of Cybersecurity Research," 22 Harv. J. Law & Tech. 167 (2008), http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech167.pdf (describing the impact of the wiretap laws).

[17] Chris Grier, et al., "Barriers to Security and Privacy Research in the Web Era," http://www.inwyrd.com/blog/wp-content/uploads/2010/03/wecsr-submit.pdf (describing the impact of terms of service).

[18] Originally created to limit what TSA, airline and airport personnel could say about air travel security measures, the category "sensitive security information" has expanded in scope over time to cover virtually the entire transportation sector. Moreover, the restrictions can be triggered by a growing set of conditions, spread across different laws.

[19] Edward Felten, "The Chilling Effects of the DMCA," Slate (March 29, 2013) http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.html. See generally EFF, "Unintended Consequences: Twelve Years under the DMCA" (March 2010) https://www.eff.org/wp/unintended-consequences-under-dmca.

[20] See, for example, MBTA v. Anderson, where three students at MIT were sued by the Massachusetts Bay Transit Authority and forced to cancel a scheduled conference presentation. Court filings available at https://www.eff.org/cases/mbta-v-anderson.

-- Key Federal Statutes

Three federal laws pose potential barriers to cybersecurity research:

- The DMCA (Digital Millennium Copyright Act) – Section 1201 of the DMCA provides that "No person shall circumvent a technological measure that effectively controls access to a work protected" by the Copyright Act. While there is a strong legal argument and some court precedents that Section 1201 was not intended to prohibit conducting research on software vulnerabilities, highly publicized threats of legal actions and the actual takedown of research have had a strong chilling effect.[21]

- Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 – The CFAA prohibits a wide variety of conduct. Its broadest provision says that it is a crime to access a protected computer (essentially any computer connected to the Internet) "without authorization" or to "exceed authorized access" and "thereby obtain[]… information." Again, some courts have rejected broad readings of the "without authorization" or "exceeds authorization" language, but the threat of criminal or civil liability looms large.[22]

- Wiretap Act, Pen/Trap Statute and ECPA (specifically the Stored Communications Act) – The Federal Wiretap Act prohibits real-time interception of the content of electronic communications. The Pen/Trap Statue likewise prohibits real-time interception of the non-content portions of electronic communications. The Stored Communications Act prohibits entities providing service to the public from disclosing the contents of stored communications to anyone and transactional data to a governmental entity. All three have exceptions that permit service providers or other systems operators to intercept, record, and disclose communications on their own systems to the extent necessary to protect the "rights and property" of the system operator. These exceptions pretty clearly support monitoring and analysis by a provider (or its contractor) on the provider's own network, but they do not expressly permit research for general cybersecurity purposes or a provider's sharing of information with peers or with third party researchers.[23]

With all three laws, a key barrier to research is legal uncertainty. Legal ambiguity, combined with the discretion afforded to prosecutors and private litigants, deters research. Commenters in connection with the Copyright Office's current review of Section 1201 have cited specific, real-world examples of important security research that was not undertaken because of liability concerns under the

[21] See EFF, "Unintended Consequences: Fifteen Years Under the DMCA."

[22] See David B. Thaw, "Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement," 103 J. Crim. L. & Criminology 907 (2013); Orin Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," (Symposium: Cyberspace & the Law: Privacy, Property and Crime in the Virtual Frontier) 94 Minn. L. Rev. 1561 (2010).

[23] See Aaron J. Burstein, "Amending the ECPA to Enable a Culture of Cybersecurity Research," 22 Harv. J. Law & Tech. 167 (2008); http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech167.pdf.

DMCA.[24] While the chilling effect of the DMCA has been described in public proceedings, there is relatively little public discussion of the barriers to research presented by these other laws. Proposals currently before Congress and federal agencies—for example, reforms to the CFAA and amendments to the Wassenaar Agreement—if enacted, will create new risks, further discouraging cybersecurity research.

-- Additional Constraints

Workshop participants identified additional constraints that, in conjunction with the legal framework, inhibit research in the university setting, including:

- university contracts with vendors that limit testing, reverse engineering, and other research enabling activities;
- general risk aversion of university counsel coupled with complicated legal frameworks that require expert analysis;
- problematic terms in mass market form contracts and licenses on consumer goods and services;
- relationships with corporate donors and potential donors, and relationships with corporate collaborators;
- liability concerns of funders;
- risk aversion and lack of expertise in institutional review boards;
- colleagues' concerns about blowback from vulnerability research; and,
- ethical and legal concerns of conference and publication sponsors and organizers.

Researchers unaffiliated with academic institutions do not face these organizationally specific barriers, but face greater risk of personal liability and reputational damage that can exert a similar effect.

-- Research Limitations Arising from Private Ordering

The federal statutes are viewed as significant impediments to cybersecurity research. However, workshop participants discussed the importance of understanding how this network of statutes, case law, and regulations interacts with private contracts and terms of use restrictions to constrain research. Restrictions on cybersecurity research can arise from university agreements with vendors. They can also result from consumer-facing click or shrink-wrap contracts and terms of service that prohibit reverse engineering, benchmarking, and other activities required for research. For example, one academic researcher at the workshop discussed the impact of mass-market contract terms on

[24] Relevant comments and reply comments (particularly those filed under Classes 22 and 25) in the proceeding can be retrieved here: http://copyright.gov/1201/2015/comments-020615/; http://copyright.gov/1201/2015/comments-032715/; and http://copyright.gov/1201/2015/reply-comments-050115/. Initial petitions for exemptions can be retrieved here: http://copyright.gov/1201/2014/petitions/.
Relevant ones include: Bellovin et al. [Computer Programs – Malfunctions and Security Flaws]; Berkman Center for Internet & Society [Computer Programs – Medical Devices]; Electronic Frontier Foundation 3 [Vehicle Software – Safety Research]; Green, Dr. Matthew D. [Computer Programs – Applied Cryptography, Security and Reverse Engineering Research].

that researcher's ability to explore mobile malware issues. This research requires downloading applications and performing static or dynamic analysis. Scraping an application store requires researchers to misrepresent themselves as an Android device and often requires researchers to violate mobile applications' terms of service.

Workshop Outcomes: The Chilling Effect on Research

Participants highlighted the interplay between legal ambiguity and the likely target of a suit, explaining that the chilling effect was different depending upon the context. For example, junior faculty, post-docs, and students, particularly those who are foreign nationals, are likely to experience a heightened level of chill. Similarly, independent researchers may be easier targets, due to their lack of institutional affiliation, and the associated pedigree, privilege, and access to resources, and therefore be more hesitant to take research risks.

One participant gave another real-world example illustrating the problems around disclosure to vendors: A research firm was engaged under contract to perform penetration testing for a large retailer. The researchers found a point-of-sale (POS) system vulnerability but the retailer told them that the researchers could not disclose the vulnerability to the vendor of that POS system. The retailer argued that disclosure to the vendor would put the retailer at greater risk of exploitation. The researchers argued that failing to disclose to the vendor meant they would be leaving vulnerable every other retailer that had this particular POS system. The research firm eventually convinced the retailer to disclose the vulnerability to the vendor but it was a challenge. Since then, the research firm has changed its policy to make it clear that it will disclose vulnerabilities to both the client that has engaged the firm and the vendor of the vulnerable product.

An academic researcher added that political pressure can sometimes have a larger effect than the threat of lawsuits. The researcher shared his experience where there were numerous calls to his university president, dean, and trustees alleging that his research had broken the law. The researcher stated that in that kind of situation the merits of the legal arguments matter less than the threats themselves.

One academic researcher commented that other academic researchers he knows are afraid to even discuss what areas they are *not* researching for fear of revealing the legal stance taken by their academic institution on such matters. This workshop participant also commented that there was a need for the cybersecurity research community to create a chilling effects database of legal threats against security researchers. Another participant said that www.attrition.org/errata/legal_threats has a small collection of these. There were also comments that this kind of database might consist of examples of research that individuals did not do, but putting together a database of examples of the kind of research individuals *have* done would be more difficult because researchers might not want to disclose for fear of exposing them to the very risks the database was intended to document.

-- Risk Adversity in the Shadow of Legal Ambiguity

Workshop participants described several ways that legal ambiguity stymied research. One academic researcher shared a project on automobile security research that illustrated the complicated legal terrain created by the interaction of the DMCA, CFAA, and EPCA. The researcher discussed the onboard diagnostic ports that enable communication with almost every component in an automobile. Both automakers and third parties are exploring and bringing to market uses of these ports for a wide range of purposes (thereby creating the connected vehicle). For example, the insurance industry offers devices that track driving habits in return for discounts for safe driving. In investigating and identifying vulnerabilities in these devices, the researcher's group encountered a range of legal challenges. Among these were contractual anti-reverse engineering provisions associated with the purchase of the device and potential liability under the DMCA (anti-circumvention) and CFAA (when the device was part of a service offering and not a product offering). As well, monitoring or engaging in communications with the Internet-based servers that these devices communicate with raised additional issues including about the scope of "authorized access" under the CFAA and ambiguity in ECPA (and state wiretap restrictions) about how to interpret multi-party consent between computers. More generally, workshop participants noted that the move to software as a service (SaaS) pervasively expands what used to be primarily DMCA issues into potential CFAA issues as well.

Workshop Outcomes: Mitigation Strategies

Workshop participants have adopted multiple strategies to reduce their risk. These include: 1) conducting this kind of research at a high profile university, 2) releasing their final reports to regulators or other policy makers first, which may provide additional protection against efforts to limit the dissemination of research findings under what are know as anti-SLAPP[25] laws, which protect the flow of information about important public issues; 3) fostering positive relationships with law enforcement and relevant regulatory agencies; 4) vetting factual claims with other researchers to double check claims before disclosing them; and 5) partnering with the media to conduct certain sorts of research, which has proven useful in the privacy context. Working with regulators, securing press coverage, and enlisting colleagues to vet factual claims and research findings (to the extent possible) were viewed as good protection against vendor pushback on findings and retaliatory suits.

Workshop Conclusions and Action Items

-- Immediate Policy Interventions

At the conclusion of the workshop participants agreed upon two immediate policy interventions:

- A public statement of the value of cybersecurity research, the impediments created by existing laws, and the negative impact of legal barriers to improving the state of security; and,
- Participation in the Copyright Office DMCA review and other venues where it is important to make the case for limiting barriers to cybersecurity research in order to better realize its value.

Quick action was taken on both items:

- Workshop organizers and key participants drafted a Statement on Legal Impediments to Cybersecurity Research, which was released on May 1, 2015. (Attached as Appendix 3.) It was signed by many of the workshop participants, as well as other cybersecurity researchers.

[25] Strategic Lawsuits Against Public Policy are filed to squelch public discussion and debate.

It remains open to signature and continues to draw attention. It was referenced by several participants in comments filed with the Copyright Office in the DMCA review.

- Several workshop participants, including the organizers, submitted comments to the Copyright Office in connection with the DMCA review, explaining the value of cybersecurity research and arguing that opposition to cybersecurity research exemptions from industrial copyright owners should be dismissed because the objections did not stem from copyright-related concerns.[26] These comments emphasized that concerns raised by opponents to the exemption were about public safety, battery life, and supply chain integrity—issues that lie outside the DMCA and the expertise of the Copyright Office, are better addressed in other venues and through other regulatory regimes, and are in fact advanced by cybersecurity research. The Statement on Legal Impediments to Cybersecurity Research was attached to these comments.

Additionally, workshop participants from civil society organizations submitted comments on the Wassenaar export control rules put forward by the US Department of Commerce's Bureau of Industry and Security (BIS). The Wassenaar Arrangement is a multilateral policy agreement under which member states including the United States agree to place limits on the export of certain technologies used in offensive weapons. BIS had put out proposed rules for public comment meant to control certain "cybersecurity items." From the perspective of the commenters, the limits would seriously affect the use of common security testing tools and curtail communications about security vulnerabilities necessary to protect systems. The organizations submitted extensive comments arguing that the rules were poorly formed and over inclusive—covering far more than necessary to control software that may be weaponized and used in violation of human rights treaties.[27]

-- Areas for Further Research

The workshop identified five additional areas of potential research, collaboration, and action:

1. documenting the "cost" of the chilling effect on research—both research projects forgone and real-world negative consequences of research undertaken;
2. guidance on application of existing legal authorities;
3. clarifying that following good practices signifies good intent, regardless of researchers' institutional pedigree or affiliations;
4. vulnerability reporting processes; and,
5. educating policymakers and the public.

[26] Reply Comments of the Center for Democracy and Technology et. al., In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. §1201 Docket No. RM 2014-07, May 5, 2015.

[27] Access, The Center for Democracy & Technology, Collin Anderson, The Electronic Frontier Foundation, The Open Technology Institute, and Human Rights Watch, "Comments to the U.S. Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements," RIN 0694-AG49, July 20, 2015, *available at:* https://cdt.org/files/2015/07/JointWassenaarComments-FINAL.pdf.

1. Further documenting the "cost" of the chilling effect on research—both research projects forgone and real-world negative consequences of research undertaken

Workshop participants agreed that additional facts about the cost imposed by today's legal environment on cybersecurity research and the downstream impact of foregone research on cybersecurity in commercial and government systems is necessary to build understanding and support for reform among policymakers and the public. Given the risks to public safety and health from insecure devices, participants viewed documentation and research in this area as a top priority.

Participants agreed that a collaboratively-sourced compendium of research that has been chilled would be a useful starting point. There was a suggestion to improve on the current collection of publicly reported incidents of legal threats, prosecutions, and civil suits.[28] However, while reports from the field were viewed as useful, workshop participants noted that they fail to capture the myriad ways research is chilled.

Moreover, compendiums of chilled research are likely to underrepresent the scope of the problem, as individuals may be reluctant to share information about research they've avoided or abandoned. Reluctance to share information about abandoned and avoided research stems from a fear that acknowledging it or speaking about it may bolster claims that such research—if undertaken by that researcher or others—is illegal, or it may draw exceptional scrutiny by vendors, complicating future research. More importantly, as participants noted throughout the workshop, the legal climate deters and shapes cybersecurity research long before research or publication.

In light of these constraints, workshop participants suggested that qualitative and quantitative social science research interviewing and surveying computer science researchers, research institutions, conference committees, and publishers on the opportunity cost of the current laws would more fully and systematically document the scope and impact of the problem. To bolster reporting, survey responses could be anonymous and interviews designed to protect confidentiality. Protecting the identity of research subjects *might* diminish the utility of the results in the public policy context, but participants thought it was likely necessary to encourage participation

Participants emphasized the importance of documenting the downstream health and safety implications of foregone research. The recent voluntary recall[29] of millions of Chryslers and Fiats, due to public safety risks caused by vulnerabilities in the onboard Uconnect entertainment system, provides a compelling example of the consequences of cybersecurity vulnerabilities that could be identified through independent research. Researchers had identified this risk and notified the companies long before disclosing it to the public. Similar vulnerabilities in the Prius software stack, which allowed a remote attack on a physically tampered vehicle to cause acceleration, as well as

[28] Including those compiled by the Electronic Frontier Foundation, *Unintended Consequences: Sixteen Years under the DMCA*, September 2014 https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf: and, Attrition, *Legal Threats Against Security Researchers: How vendors try to save face by stifling legitimate research*, http://attrition.org/errata/legal_threats/.

[29] While technically voluntary, NHTSA exerted pressure on Fiat and has commenced an investigation into the hack and the patch. See, David Shepardson, *Fiat Chrysler will recall vehicles over hacking worries*, Detroit News, July 24, 2015.

research on medical devices that revealed security vulnerabilities that could lead to loss of life, further illustrate the health and safety costs of software vulnerabilities. In these particular cases, intrepid researchers forged ahead despite the risks of legal liability, relying on some of the mitigation strategies discussed above. Similar research is needed on many other types of devices. The rise in the number and diversity of embedded and networked devices increases the importance of this research. Given the accelerated pace of embedded software, workshop participants believe it is imperative that policy makers are aware of the role research plays in building more trustworthy and secure devices and systems.

2. Guidance on application of existing legal authorities

The climate for cybersecurity research could be improved by reliable guidance on the interpretation of existing legal authorities and in particular guidance on how the Department of Justice (DOJ) intends to navigate its discretion in gray areas. One participant noted, however, that DOJ guidance, because it can be ignored in specific cases or changed anytime in the future, would not fully assuage the concerns of researchers.

Another participant commented that amendment to ECPA and the associated wiretap and pen/trap statutes would be desirable. The participant recommended three specific changes: 1) to amend the definition of governmental entity in the Stored Communications Act to clarify it doesn't apply to public universities engaged in research (for purposes of permitting disclosures of non-content); 2) to amend the Wiretap Act to allow service providers, under the exception for security, to disclose customer communications to security researchers under the condition that the data be protected under a non-disclosure agreement; and 3) to amend the Pen Register/Trap and Trace Statute to allow providers to give researchers access to communications metadata. The participant noted that these recommendations had been proposed in 2010 but that they had not gone anywhere. The same participant noted that amending the CFAA to address the concerns of workshop participants was not politically tenable at this time.

In response to whether the CFAA reform known as "Aaron's law" was a good proposal, one corporate participant said that many companies would not support it because they rely on the CFAA to deter the insider threat problem (by insisting that it is a crime under the CFAA for employees to access corporate data they are not authorized to access). One academic researcher said that, in regards to the CFAA, most of the research community does not have a problem with the "unauthorized access" prong of the statute. Rather, the main issue with the CFAA is in connection with the "exceeding authorized access" prong. Another participant noted that the CFAA could be amended to resolve these issues without touching on the insider threat problem.

3. Clarifying that following good practices signifies good intent, regardless of researchers' institutional pedigree or affiliations

Workshop participants were skeptical of efforts to define "appropriate" or "legitimate" research or to define the group of individuals eligible for protection under existing or future security research exemptions. Participants noted that efforts to limit who is covered by exemptions is problematic for reasons similar to those that led courts and policymakers to reject efforts to limit who was considered a reporter for purpose of reporters' shield laws. Like reporters, researchers are increasingly not affiliated with the institutions that historically housed cybersecurity research (for example, universities), but rather are operating independently or in businesses that, while specializing in research, may be for-profit and unaffiliated with universities. Attempting to limit who can claim a research exemption based on characteristics of educational degree, title, or institutional affiliation would discourage very valuable models for organizing and conducting cybersecurity research.

The alternative, allowing all those engaged in security research to enjoy protection, is more protective of research and more likely to ensure that ongoing security advancements reach the public. However, some individuals engaged in security research are doing so to profit from discovered vulnerabilities—directly, or indirectly. For this reason, while participants were adamant that efforts to define "legitimate" research were untenable and risked discouraging beneficial research, there was some interest in identifying patterns or paths of behavior that signal white-hat status. This interest, however, was coupled with some skepticism about the scope of this problem—the inability to discern non-malicious actors. Many of the known instances of chilled research involve researchers whose track record of scientific contributions, institutional affiliations, and behavior in conducting, disclosing, presenting, and publishing research has definitively signaled their productive and positive motivation and the research's contribution to science and improved security, without the need for some agreed-upon set of standards.

Participants observed that researchers have varying interests, sensitivities, and ethical constraints that define the scope of research palatable in their community. Community norms influencing research take many forms, including program committees (ad-hoc communities of relevant researcher peers that select papers for presentation and publication, providing peer review, an essential component of sound science) that at times reject papers due to legal and ethical concerns, and Institutional Review Boards (IRBs) that interpret the Federal ethical framework for human subjects research and which increasingly review research on cyber systems and electronic devices due to their tighter coupling to individuals. In areas such as automobiles and health devices, researchers face additional constraints due to the more direct connection to health and safety and the thicket of legal protections that, while often not explicitly constraining them, inform how they scope and conduct their research. While not all researchers experience these constraints, for a substantial number of participants they inform decision-making about research ethics and legality. As discussed below, participants believe that these institutions—program committees, IRBs—along with other actors such as university counsel, are generally overly risk averse and in need of additional guidance. However, if appropriately informed and resourced, participants believed these institutions could play an important role in protecting the security research ecosystem.

4. Vulnerability reporting processes

Researchers' conduct around the disclosure of discovered vulnerabilities is influenced by an additional set of forces. There are multiple, sometimes competing, standards and best practices for vulnerability disclosure. Workshop participants noted the importance of distinguishing between vulnerability coordination and disclosures *to vendors* and disclosures *to the public*. "Vendor" in this context was defined broadly as whomever is responsible for maintaining the software, hardware, or deployment and can remediate the problem. Participants believed that following existing best practices around disclosures procedures[30] was a useful indication of good intent, but cautioned that

[30] Several participants are working on a review of vulnerability disclosure frameworks, but for now this older technical report provides a review of many vulnerability disclosure frameworks: Andrew Cencini, Kevin Yu, Tony Chan, "Software Vulnerabilities: Full, Responsible, and Non-Disclosure," Technical Report, 2005, *available at:*

the inverse was not true—the failure to follow best practices did not necessarily indicate malicious intent, but could stem from lack of knowledge, inexperience, and frustration with a poor response by a vendor.

-- Best Practices for Vendors

Participants noted that legal threats often come from inexperienced vendors. Participants agreed that guidance to vendors on how to receive and respond to vulnerability reports would make a valuable contribution to improving the climate for security research.

There was consensus that creating a safe harbor for researchers who use an established procedure provided by the vendor would ease the chill on white-hat researchers and reduce tensions between researchers and vendors. While participants noted that it would be hard to get all vendors to agree on a single safe harbor, it seemed feasible that vendors would agree to a safe harbor that was defined by use of their own process for working with vulnerabilities.

Participants generally agreed that vendors and other entities in a position to correct cybersecurity vulnerabilities should adopt procedures to receive and respond to reports of vulnerabilities. Some advocated the adoption of the current ISO standard; however, many objected to its proprietary nature. Participants agreed that the ISO standards are not well known as they are somewhat new and not publicly available, and therefore vendor adoption of practices informed by them required outreach and education. Regardless, participants agreed that adoption of a process for receiving and responding to vulnerability reports was an essential component of the solution. Allowing vendors to choose among standards allows some flexibility, but also could create some common processes to ease researchers' interactions with vendors.

The activities of the Securities and Exchange Commission (SEC), the National Highway Traffic Safety Administration (NHTSA), and other agencies that frame security as part of a company's fiduciary duty and regulatory responsibility were viewed as supporting the adoption of processes for handling the receipt and response to vulnerabilities. Participants suggested that they might provide leverage within the commercial vendor community.

-- Varying Practices for Researchers

Participants objected to a model of imposing best practices on researchers. The diversity of research, the different implications of vulnerabilities, the differing fields, all argue against a single set of practices. The need for variation and responsiveness to address risks from research, disclosures, and most importantly the vulnerabilities themselves counsel against both single and fixed practices.

http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf. There are two proprietary, non-public International Standards Organization (ISO) standards that have been developed for receiving vulnerability disclosures (often called "vulnerability handling processes): ISO/IEC 29147 Vulnerability Disclosure, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170, and ISO/IEC 30111 Vulnerability Handling Processes, http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231.

5. Educating policymakers and the public

There was broad concern that some policymakers don't understand the importance of, and technical issues associated with, security research and vulnerability disclosure. There was wide support from all participants for educating policymakers and relevant stakeholders about why security research is needed and how it is being hindered by the current legal landscape. There was support in principle for outlining a larger set of reforms to existing laws, along with other policy clarifications (such as DMCA exemptions) that would reduce risks of liability for the conduct and dissemination of cybersecurity research.

-- Materials for University Counsels, Computer Science Deans, and Institutional Review Boards

University policymakers were identified as a particular target for education. An academic researcher noted that it was not just policymakers who needed to be educated, but also leadership in the university hierarchy. The participant shared an experience where they were forced to cancel a research project because they did not feel they had the support of the institution. In terms of materials for universities, participants noted that materials for IRBs would be useful. Currently participants noted there is great variation in how IRBs assess the research that falls within their purview and set standards for its review, coupled with a general lack of technical proficiency, this variation creates uncertainty for researchers. There were also comments from participants regarding a knowledge gap among general counsels at universities and the fact that they would need any guidance on the legal landscape to come from someone they trust (practical, neutral advice). One participant mentioned the "Legal Guide to Botnet Research" and the "Legal Guide to Cybersecurity Research"[31] as potential resources.

-- Resource for students

One participant suggested that university students would benefit from a simple web resource that outlined the issues and described potential mitigation strategies. The participant clarified that this would not require the general counsel to advise students, just a way to support the students.

-- Whitepaper on legal barriers

Participants agreed that the research community needed a forward-looking policy agenda that would advance the climate for security research. They believed that the research on chill and impact, as well as the educational documents for policymakers, were necessary to set the stage for such an effort. The agenda would outline reforms to existing laws and policy clarifications, such as DMCA exemptions, that would reduce risks of liability for the conduct and dissemination of cybersecurity research.

[31] Jody R. Westby, *Legal Guide to Cybersecurity Research,* ABA Book Publishing, 2013, http://shop.americanbar.org/eBus/Store/ProductDetails.aspx?productId=215455; Jody R. Westby, *Legal Guide to Botnet Research,* ABA Book Publishing, 2013, http://shop.americanbar.org/eBus/Store/ProductDetails.aspx?productId=215452.

-- Public education on the benefits of cybersecurity research

Educating the public about the connection between security research and safe and secure consumer products was viewed as vitally important. Public awareness of the benefits of cybersecurity research will improve policy decisions, by providing a more balanced understanding of researchers' contributions to safety and security improvements. Participants recommended that op-ed pieces in widely read publications, building off high profile events, be used to inform the general public about these issues.

Appendix 1

Participants
Workshop Held at the University of California Berkeley
April 9-10, 2015

Kevin Bankston, Policy Director, New America's Open Technology Institute

Jim Dempsey, Executive Director, Berkeley Center for Law & Technology, University of California, Berkeley School of Law

Timothy Edgar, Visiting Fellow, Watson Institute, Brown University

Jen Ellis, Rapid 7

Jeremy Epstein, National Science Foundation

Ed Felten, Professor, Computer Science and Public Affairs, Princeton

Kevin Fu, Associate Professor, Electrical Engineering and Computer Science, University of Michigan

Dipayan Ghosh, Office of Science and Technology Policy, Executive Office of the President

Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society

Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology

Chris Hoofnagle, Lecturer in Residence, University of California, Berkeley School of Law

Harri Hursti, Independent Security Expert

Richard Kemmerer, Professor, Computer Science, University of California, Santa Barbara

Erin E. Kenneally, Center for Applied Internet Data Analysis, University of California San Diego)

Art Manion, CERT

Bill Marczak, PhD candidate, Computer Science, University of California, Berkeley

Andrea Matwyshyn, Microsoft Visiting Professor, Center for Information Technology Policy, Princeton

Jonathan Mayer, PhD candidate, Computer Science, Stanford University

Kate Moussouris, HackerOne

Deirdre Mulligan, Professor, School of Information, University of California, Berkeley

Kurt Opsahl, Electronic Frontier Foundation

Vern Paxson, Professor, Electrical Engineering and Computer Sciences, University of California, Berkeley

Audrey Plonk, Intel

Jay Radcliffe, Rapid 7

Larry Rohrbough, UC Berkeley, TRUST

Pamela Samuelson, Richard M. Sherman Distinguished Professor of Law, University of California, Berkeley

Stefan Savage, Professor, Computer Science, University of California, San Diego

Barbara Simons, IBM Research, Retired, and Board Chair, Verified Voting

Abigail Slater, Internet Association

Bill Smith, Paypal

Erik Stallman, Director of the Open Internet Project and General Counsel, Center for Democracy & Technology

Andy Steingruebl, Paypal

Eli Sugarman, Hewlett Foundation

David Thaw, Assistant Professor of Law and Information Sciences, University of Pittsburgh, Affiliated Fellow, Information Society Project, Yale Law School

Kit Walsh, Electronic Frontier Foundation

Jody Westby, Global Cyber Risk

Appendix 2

Workshop Agenda
April 9-10, 2015

Thursday April 9 – Dean's Seminar Room, Boalt Hall, UC Berkeley Law School

1:00 Welcome
Deirdre Mulligan, UC Berkeley
Jeremy Epstein, National Science Foundation

1:15 Introductions

1:30 Overview of Agenda and Discussion of Desired Outcomes
Jim Dempsey, UC Berkeley
Questions for discussion:
What would a better research environment look like?
What product or products might we develop to promote that environment?
What are the audiences for our outputs?

2:00 Current landscape of uncertainty – real-world scenarios where research has been chilled – security research concerns
Chris Hoofnagle, UC Berkeley
Jonathan Mayer, Stanford

3:00 Industry (manufacturer/developer) concerns
Jen Ellis & Jay Radcliffe, Rapdi7

3:30 Break

4:00 Legal Framework
Kit Walsh, EFF – DMCA
Erik Stallman, CDT – ECPA/CFAA/CPNI

5:00 Workshop Concludes for Thursday

Friday April 10th – Bancroft Hotel (2680 Bancroft Way)

9:00 Convergence of impediments – contract, DMCA, CFAA, and ECPA all in one case
Stefan Savage, UC San Diego

9:30 DMCA – The triennial review – overview of exemptions and comments
Pam Samuelson, UC Berkeley
Erik Stallman, CDT

10:30 Break

11:00 ECPA and CFAA exceptions for security research

11:30 Current best practices and standards for security research and voluntary disclosure
Jody Westby, Global Security Risk
Erin Kenneally, CAIDA
Katie Moussouris, HackerOne

12:30-1:30 Break for Lunch – Bancroft Hotel

1:30 Afternoon workshop begins: Towards acceptance of best practices – and alternatives

For disclosure by security researchers
For company processes to interact with researchers

3:00 Outcomes, next steps and possible follow-up

4:00 Workshop concludes

Appendix 3

Statement on Legal Impediments to Cybersecurity Research
May 1, 2015 (updated May 21, 2015)

Cybersecurity is an urgent national priority. Vulnerabilities in a wide range of digital devices, systems, and products, including critical infrastructures, can and have been exploited to undermine national security, economic prosperity, and personal privacy. The rapid emergence of the Internet of Things heightens the risk, as consumer products widely used in daily life, ranging from automobiles to medical devices to thermostats and home appliances, become connected to the Internet and thus vulnerable to remote manipulation, exploitation, and attack. The growing complexity and interdependencies among devices and networks compounds the risks, making it increasingly important to assess, and address, vulnerabilities in technically and socially complex real world settings.

In this environment, cybersecurity research is vital. Security by obscurity – the notion that vulnerabilities can be kept hidden from adversaries – has failed in the past and is particularly poorly suited to today's interconnected environment.

Corporate, governmental, academic, and independent cybersecurity researchers all contribute to identifying and remediating cybersecurity vulnerabilities. However, there are serious legal impediments today to cybersecurity research. The Digital Millennium Copyright Act, the Computer Fraud and Abuse Act, and the web of statutes amended by the Electronic Communications Privacy Act all impose uncertain and potentially catastrophic liability on good-faith security research and the disclosure of security vulnerabilities. We, the undersigned, warn of the negative impact of these impediments, and we urge policymakers to address and mitigate them.

Even in the face of these barriers, cybersecurity research has advanced the security, trustworthiness, and resilience of systems ranging from cyberphysical, to voting systems, to medical devices. It has benefited human health and safety, protected democratic self-governance, and shored up systems essential to the economic and physical wellbeing of the nation. Much further positive work could be done if the legal barriers to research were lowered.

Three examples highlight the value of research conducted under the cloud of legal uncertainty:

Research on automobiles: Modern automobiles are becoming increasingly computerized — with many components controlled partially or entirely by computers and networked both internally and externally. While this architecture provides many benefits, the risks have not been carefully considered or addressed by the automotive industry. University researchers and others have begun to examine these risks, yielding important findings. They have showed that existing automobiles are extremely fragile to attack and empirically demonstrating that a range of vectors (including dealership shop tools, media players, Bluetooth and cellular telematics connections) all can be used to compromise even safety critical components (e.g., remotely disabling the brakes).[1] This was research that was not being pursued by the automotive industry, involved extensive reverse engineering of automotive systems and has had major positive concrete impacts for the public. Among the visible side effects of this work include the establishment of a new cybersecurity standards effort undertaken by the Society of Automotive Engineers, a cyber security testing and evaluation capability being created by the Department of Transportation's National Highway and Traffic Safety Administration (NHTSA), a $60M research program created by DARPA (HACMS) to develop new technologies to increase vehicle security, a pending Senate bill soon to be introduced regulating automotive cybersecurity and significant automotive industry investment in cybersecurity. (For example, Eric Gassenfeit, OnStar's chief information security officer, has been publicly quoted as saying that his team has had its resources and staff grow "by an order of magnitude" in the period after the publication of this research.[2]) All of these benefits accrued only because the researchers took risks that they should not have to take.

Research on voting machines identified significant vulnerabilities in the technical systems upon which the most fundamental act of our democracy relies. Election officials lack the expertise to analyze these systems, federal and state standards failed to deliver sound security, and yet, researcher access was limited by contracts that prohibited most forms of testing, as well as reverse engineering. But for cybersecurity researchers willing to take risks, the investment of the National Science Foundation, and the diligence of a handful of Secretaries of State, the public would have remained unaware of the vulnerabilities in these systems, and election officials would have been unable to seek fixes to mitigate risks of election fraud and failure.[3] The majority of voting system vendors were hostile to independent security analysis of their systems, and went to great lengths to prevent election officials and researchers from independently examining them. The work of security researchers led to the decertification of insecure voting systems, the adoption of new policies, procedures, and technologies, new methods of oversight and certification of machines, and improved training for election workers. Internet voting, which is now being promoted, deserves similar security research, but that research may be impeded by the laws mentioned above.

Medical device security researchers have uncovered fundamental flaws in devices such as pharmaceutical drug compounders, automated external defibrillators, ventilators, drug infusion pumps, and implantable medical devices.[4] Very few medical device companies have

[1] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX Security, August 2011, available at http://www.autosec.org/publications.html.

[2] Keith Barry, "Can Your Car be Hacked?" Car and Driver (July 2011) http://www.caranddriver.com/features/can-your-car-be-hacked-feature.

[3] See Virginia Information Technologies Agency, "Security Assessment of WinVote Voting Equipment for Department of Elections," April 14, 2015, http://elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf; Ariel J. Feldman, et al., "Security Analysis of the Diebold AccuVote-TS Voting Machine," Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (August 2007) https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman_html/index.html.

[4] Shane S. Clark and Kevin Fu, "Recent Results in Computer Security for Medical Devices," (2011) https://spqr.eecs.umich.edu/papers/clark-mobihealth11.pdf.

security engineering teams. Independent security researchers have taken the risk to publish security flaws in the public interest. In general, medical device engineers sincerely care about helping patients live longer and healthier lives. The devices save countless lives. However, the majority of medical device manufacturers lack the level of cybersecurity engineering maturity found in the information technology and finance sectors. Thus, medical device manufacturers often respond with hostility during a first encounter with a security researcher. The existing laws give companies unnecessary means of recourse that do not protect patients from the most prevalent cybersecurity threats; the laws only serve to chill research on medical device security.

In other sectors as well, multiple security advancements in the marketplace are the product of, or informed by, cybersecurity research. The benefit of independent cybersecurity research is also underscored by the fact that numerous companies have started their own or joined collaborative "bug bounty" programs aimed at fueling adversarial research on their systems. These programs literally pay researchers to hack into systems and identify vulnerabilities, because companies view external testing by security experts as essential to maintaining a strong security posture.

However, legal barriers remain and are even increasing. The legal impediments to cybersecurity research arise from various sources, including the Computer Fraud and Abuse Act, section 1201 of the Digital Millennium Copyright Act, and the wiretap laws.[5] The impediments also arise from contracts and terms-of-service (the breach of which may expose one to criminal liability) that broadly prohibit modifications of devices or collections of data.[6] As the urgency of the cybersecurity threat has grown, the inhibiting effect of these laws has also grown. Meanwhile, contractual prohibitions on reverse engineering have proliferated. New categories—such as "sensitive security information"—have entered the legal lexicon,[7] statutes have been broadly interpreted, and technical protections have been added to an array of consumer products to limit tinkering and modification. While there are arguments that the laws at issue would not be used to actually prosecute legitimate cybersecurity research, the laws are ambiguous and can be broadly interpreted, generating uncertainty that has a wide chilling effect.

The chilling effect of these barriers takes many forms: Academic and other research institutions can be risk-averse, advising faculty and students to steer clear of research with

[5] Aaron J. Burstein, Amending the ECPA to Enable a Culture of Cybersecurity Research," 22 Harv. J. Law & Tech. 167 (2008), http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech167.pdf (describing the impact of the wiretap laws).

[6] Chris Grier, et al., "Barriers to Security and Privacy Research in the Web Era," http://www.inwyrd.com/blog/wp-content/uploads/2010/03/wecsr-submit.pdf (describing the impact of terms of service).

[7] Originally created to limit what TSA, airline and airport personnel could say about air travel security measures, the category "sensitive security information" has expanded in scope over time to cover virtually the entire transportation sector and, moreover, there is an ever growing set of trigger conditions spread across many different laws that make one subject to restrictions applicable to it.

unclear liability; faculty advise students to work in areas less fraught with potential legal and public-relations challenges; and peer review may look unfavorably upon researchers whose work treads too closely to legal lines[8]. Funders may be reluctant to support certain kinds of research. Academic publication venues are forced to wrestle with questions regarding the legality of research, despite its public value. Papers have been both delayed and outright pulled due to court intervention, threats of suit by research subjects, and program committee concerns with potential liability exposure for the committee, the institution, or the venue.[9] Independent researchers face an outsized threat of criminal prosecution and civil litigation. Researchers at corporations face a chill as well, because the questionable legality of certain security research may raise an appearance of impropriety if another company's technology is the subject of analysis.

In light of these concerns, we recommend that:

- The Copyright Office should endorse the security research exemptions that have been proposed in the current triennial review.

- The US Department of Justice, in order to narrow the possibility of prosecution for cybersecurity research aimed at improving the security of devices or of our nation's Internet systems, should issue guidance clarifying the government's interest in promoting cybersecurity research and describing practices that will not be subject to prosecution.

- University general counsels and other university officials should defend cybersecurity research, including by assisting university researchers to thread their way through the maze of laws.

- Vendors and other entities in a position to correct cybersecurity vulnerabilities should adopt procedures, such as those recommended in ISO standards,[10] to receive and respond to reports of vulnerabilities.

- Congress should amend laws that impede cybersecurity research to make it clear that those laws do not prohibit research intended to improve the security of devices or of our nation's Internet systems and infrastructure.

[8] Edward Felten, "The Chilling Effects of the DMCA," Slate (March 29, 2013) http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.html. See generally EFF, "Unintended Consequences: Twelve Years under the DMCA" (March 2010) https://www.eff.org/wp/unintended-consequences-under-dmca.

[9] See, for example, MBTA v. Anderson, where three students at MIT were sued by the Massachusetts Bay Transit Authority and forced to cancel a scheduled conference presentation. Court filings available at https://www.eff.org/cases/mbta-v-anderson.

[10] ISO 29147: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170; ISO 30111: http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231.

Ben Adida, VP Engineering, Clever Inc.
Jacob Appelbaum, The Tor Project
Ruzena Bajcsy, NEC professor, Electrical Engineering and Computer Sciences, University of California, Berkeley
Kevin Bankston, Policy Director, New America's Open Technology Institute
Steven M. Bellovin, Professor, Computer Science, Columbia University
danah boyd, Founder, Data & Society
Sam Bowne, Instructor, Computer Networking and Information Technology, City College San Francisco
Eric Burger, Research Professor, Computer Science, Georgetown University
L. Jean Camp, Professor of Informatics, Indiana University
Stephen Checkoway, Assistant Research Professor, Computer Science, Johns Hopkins University
Ming Chow, Senior Lecturer, Department of Computer Science, Tufts University
Nicolas Christin, Assistant Research Professor, Electrical and Computer Engineering, Carnegie Mellon University
Donald E. Eastlake 3rd, network engineer
Timothy H. Edgar, Visiting Fellow, Watson Institute, Brown University
Casey Ellis, Co-founder and CEO, Bugcrowd Inc
David Evans, Professor, Computer Science, University of Virginia
Bryan Ford, Associate Professor, Computer Science, Yale University
Kevin Fu, Associate Professor, Electrical Engineering and Computer Science, University of Michigan
Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society
Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology
Nadia Heninger, Magerman Term Assistant Professor, Computer and Information Science, University of Pennsylvania
Harri Hursti, independent security expert
Richard Kemmerer, Professor, Computer Science, University of California, Santa Barbara
Erin E. Kenneally, Center for Applied Internet Data Analysis, University of California San Diego
Shriram Krishnamurthi, Professor of Computer Science, Brown University
Susan Landau, Professor of Cybersecurity Policy, Worcester Polytechnic Institute
Harlan Lieberman-Berg, Debian Maintainer, the Debian project
Sascha Meinrath, Director, X-Lab
Sigurd Meldal, Director, Silicon Valley Big Data and Cybersecurity Center, San José State University
Tyler Moore, Assistant Professor, Computer Science and Engineering, Southern Methodist University
Katie Moussouris, Chief Policy Officer, HackerOne
Deirdre K. Mulligan, Associate Professor, School of Information, University of California, Berkeley
Vern Paxson, Professor, Electrical Engineering and Computer Sciences, University of California, Berkeley
Ron Rivest, Vannevar Bush Professor, Massachusetts Institute of Technology
Avi Rubin, Professor, Computer Science, Technical Director, Information Security Institute, Johns Hopkins University
Pamela Samuelson, Richard M. Sherman Distinguished Professor of Law, University of

California, Berkeley
Stefan Savage, Professor, Computer Science, University of California, San Diego
John E. Savage, An Wang Professor of Computer Science, Brown University
Tim Sayre, co-founder, Kanawha IT Security Services
Bruce Schneier, Fellow, Berkman Center for Internet and Society, Harvard Law School
Micah Sherr, Assistant Professor, Computer Science, Georgetown University
Barbara Simons, IBM Research (retired)
Abigail Slater, Vice President, Internet Association
Jason Syversen, CEO, Siege Technologies
Janos Sztipanovits, E. Bronson Ingram Distinguished Professor of Engineering, Vanderbilt University
David Thaw, Assistant Professor of Law and Information Sciences, University of Pittsburgh, Affiliated Fellow, Information Society Project, Yale Law School
David Wagner, Professor of Computer Science, University of California, Berkeley
Nicholas Weaver, staff researcher, International Computer Science Institute, University of California, Berkeley
Stephen Wicker, Professor of Electrical and Computer Engineering, Cornell University

Affiliations for identification purposes only.