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

---

[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.

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 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

---

[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.

[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).

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 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

---

[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.

[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.

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.

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

---

[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.

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.