August 1, 2013

Dear Congress and members of the Senate and House Committees on the Judiciary,

We are computer security experts who have dedicated our careers to maintaining the safety and integrity of information technology systems in the service of consumers, businesses, and governments worldwide. We are also coders, developers, engineers, explorers, and users of digital technologies who care deeply about protecting those who engage in computer security research and science. We write to urge you to support HR 2454: "Aaron's law." It's a new bipartisan bill by Representatives Zoe Lofgren and Jim Sensenbrenner and Senator Ron Wyden's aimed at reforming the Computer Fraud and Abuse Act ("CFAA"), 18 USC § 1030. The bill seeks to ensure that this work will continue to both help Americans be more secure and to ensure that American companies build better products.

While seldom heralded publicly, security researchers in academia, industry, public service, and independent practice work to identify serious security shortcomings in systems ranging from medical devices to voting machines to cloud services to critical national infrastructure. This research and investigation is especially urgent as we find ourselves integrating computers into our homes, vehicles—even our bodies. The security research community stands ready to meet that technical challenge, but we need Congress to clear legal hurdles out of our way.

We recognize that there are bad actors in the world; individuals, groups, corporations, and nations that wish to use technology to manipulate, lie, cheat, and steal. We have no desire to eliminate the ability for real crimes to be investigated and criminals judged with due process. Yet while the CFAA has a core purpose of criminalizing harmful computer intrusions that we strongly support, the law has lost its way. It now poses an increasing threat to security research. In short, applied computer security research requires experimenting with computer systems. The CFAA, due to outdated wording, makes it unlawful to access a computer system "without authorization" or "in excess of authorization." This vague wording, while not misused in the early days of the statute, has recently allowed the Department of Justice and companies litigating under the civil enforcement provision of the law to push an expansive definition that, if applied, would make much of the best work in computer security research a serious federal crime, along with criminalizing ordinary behavior like violating terms of service.

For decades now, independent security research involving computer systems has slowly pushed the world's technology providers to build more trustworthy products. Some examples:

ELECTRONIC VOTING: A number of computer scientists, including Princeton professor and former FTC Chief Technologist Ed Felten and Johns Hopkins University professor Avi Rubin, have tested the security of electronic voting systems, again generally without authorization, and discovered critical flaws that would make it possible for wrongdoers to rig elections and for votes to be lost through malfunctions and misconfigurations. This research led many jurisdictions across the country to abandon paperless

voting machines and begin to put real auditing processes into place. It also initiated a national dialogue and created an informed open debate about how and when digital technologies and networked machines should be used in voting.

SAFE DRIVING: Computer scientists, including professor Stefan Savage at the University of California San Diego, are documenting security vulnerabilities in computer systems in cars, like tampering with the cars' brakes. These flaws could make it possible for malicious hackers to interfere with car systems in a way that would make the vehicle less safe to drive. Without the work of these researchers, the public wouldn't know about these flaws, and car manufacturers wouldn't have critical feedback on how to build more secure computer systems for cars.

CONSUMER PRIVACY: Computer scientists are studying how advertisers and other companies track consumers' activities online and report web browsing details back to entities interested in knowing such information. This information helps inform the citizenry about the sometimes hidden business models behind many new technologies, including social networks and other online services. It has also spurred actions by the FTC and state legislatures to try to build useful tools and rules for these tracking activities.

PUBLIC HEALTH: Several academic and independent security researchers, including computer science professor Tadayoshi Kohno at the University of Washington, have revealed security flaws in medical devices like insulin pumps and pacemakers that put the privacy and physical safety of patients at risk. As a result of this important research, done largely without the authorization of the medical devicemakers who were initially resistant, the Government Accountability Office has now recommended that the FDA devise a plan to keep tabs on the security risks of implantable medical devices.

As you know, the *very purpose* of federal computer crime law is to promote computer security by punishing those who break into computers and cause harm. Yet paradoxically, the CFAA currently threatens and chills valuable research in the field by reaching mere violations of terms of use and other acts, such as security research, which cause no real harm and indeed make the public safer. Many of our colleagues, and many of us, have directly experienced the chilling effects of the CFAA. Actual litigation or prosecution of security researchers is, to be sure, quite rare. But that's because the mere risk of litigation or a federal prosecution is frequently sufficient to induce a researcher (or their educational or other institution) to abandon or change a useful project. Some of us have jettisoned work due to legal threats or fears.

HR 2454, the bipartisan CFAA reform bill called Aaron's Law, includes a provision that would eliminate the possibility that terms of service violations or other contractual "duty" can constitute an offense. The bill also adjusts the CFAA penalty scheme to ensure that actions that do no harm are not heavily penalized. This bill is an important first step in protecting the work of security researchers, as well as the general public, and we stand ready to assist as the legislative process progresses. We urge you to support this bill, to take immediate action and help to reform the CFAA so that the future vitality of responsible computer security research, and all of us who are protected by it, is ensured.

Sincerely,

Alex Stamos
Jeff Moss
Nico Sell
Cory Doctorow
Justine Osborne
Ian Robertson
Chris Hoff
Ivan Leichtling
Ed Felten
Stefan Savage
Avi Rubin
David Mortman
Jonathan Mayer
Karen Bell
Robert Edison Martin
David M. Cotter
Colin Clark
Jeff Rodman
Phil Karn
Neil R. Wyler
Barry Suskind
C. Furey DiDomeni
John Johnson
Josh Yavor

Travis Carelock
Katie Stamos
Alex Hutton
Erin Odenweller
Robert C. Trame
CyFi