KEYNOTE

Hacking into the Computer Fraud and Abuse Act: The CFAA at 30

*Sheldon Whitehouse**

Thank you, Orin, for that kind introduction.

It is a pleasure to be here today to participate in a discussion about the future of the Computer Fraud and Abuse Act ("CFAA").[1] Now in its thirtieth year, the CFAA has never been more important or controversial than it is today.

As a nation, we are under siege from cybercriminals who are leveraging the power of the internet to commit crime on an unprecedented scale, costing our economy more than one hundred billion dollars each year.

These staggering economic losses often overshadow the threat these crimes pose to our personal privacy.

We ignore this threat at our peril.

Our computers store our most important and private information. With access to our computers, criminals can empty our bank accounts, download our health records, read our most sensitive and intimate

* United States Senator from the State of Rhode Island. This piece is based on the Author's remarks delivered on November 5, 2015 at the dinner for *The George Washington Law Review*'s Symposium entitled "Hacking into the Computer Fraud and Abuse Act: The CFAA at 30."

1 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

communications, and even use the webcams and microphones built into our computers to wiretap our homes.

The threats don't stop there. Companies large and small, that we trust with our most private health and financial data, are falling victim to hacking at an astounding rate. It is estimated that nearly half of all Americans had personal information exposed by hackers in the past year alone. Much of this damage can be traced to massive corporate and government data breaches, which have become so common that the mainstream media has begun to lose interest.

The CFAA is the primary tool used by prosecutors to combat these assaults on our privacy and our economic well-being. Given the scope of the threat we face, it is essential that the CFAA remain an effective tool to combat cybercrime and that the CFAA keep pace with the rapidly-evolving tactics of the cyber underground. A robust CFAA is critical to our nation's ability to defend itself against cybercrime.

That said, we must do more to carve out innocent and trivial conduct from the CFAA's reach by decriminalizing violations of so-called terms of service agreements. Corporate lawyers have billed countless hours drafting online terms of service agreements that nobody actually reads. These contracts of adhesion are often difficult for consumers to find and are routinely ignored.

How many Americans have shared an account password with a family member? Or have provided an inaccurate phone number when opening an account to avoid marketing calls? Or have shaved a few digits off their age or weight when registering with a dating website? All of these mundane acts would constitute violations of terms of service agreements. Thanks to these agreements, we are a nation of scofflaws.

These trivial acts should not become federal criminal offenses.

As a former Attorney General and U.S. Attorney for Rhode Island, I believe that prosecutorial discretion plays a vital role in our justice system. I think, despite the ill-advised Lori Drew prosecution,[2] the Department of Justice has largely been judicious in its use of the CFAA. But a law that criminalizes the conduct of virtually every American, and then allows prosecutors to pick and choose which targets are worthy of jail time, is simply bad policy.

So how do we fix the CFAA without jeopardizing the important role it plays in protecting our economic well-being and privacy? I

2 *See* United States v. Drew, 259 F.R.D. 449, 452–55 (C.D. Cal. 2009).

have worked closely with Senator Lindsey Graham to draft bipartisan legislation, known as the International Cybercrime Prevention Act ("ICPA"),[3] that will soon be introduced in the Senate.

As I talk about the specifics about the ICPA, I also want to address some of the misunderstandings that often animate the debate over reforming the CFAA. I call these the three myths of CFAA reform.

Myth #1: The CFAA's Penalties Are Punitive and Disproportionate

Critics of the CFAA often argue that the CFAA's penalty provisions lead to sentences that are disproportionate to the crimes committed.

Sentencing data from the U.S. Sentencing Commission tells a different story. According to the Sentencing Commission, the average sentence in a computer-related criminal case is twenty-three months.[4] Defendants who commit other white-collar offenses, including health care fraud, identity theft, and securities fraud receive much longer average sentences—nearly three times as long in the case of securities fraud.[5]

The same data shows that judges routinely depart from the sentencing guidelines' recommendations and impose lower sentences in computer-related cases. In fully thirty-three percent of all computer-related cases, courts impose a below-guidelines sentence over the objections of the government.[6] Departures in other white-collar cases, including mortgage fraud, securities fraud, and mail fraud, are much less common.[7]

Given this data, I am not convinced that reducing the penalties in the CFAA is warranted. Indeed, I think we need to take a close look at whether CFAA offenses that target critical infrastructure computers are sufficiently punished. The ICPA creates a new offense for

---

3 S. Amdt. 2626 to S. 754, 114th Cong. (2015). The amendment, which included several of the key provisions from the ICPA, was proposed on October 20, 2015 and ruled nongermane by the chair on October 27, 2015. As of the printing of these statements, no further action has been taken by the Senate.

4 U.S. Sentencing Comm'n, Economic Crime Public Data Briefing 20 (2015), http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20150109/fraud_briefing.pdf.

5 *Id.*

6 *Id.* at 19.

7 *Id.*

these rare but extremely serious crimes. The ICPA also gives judges the discretion to impose stricter sentences in these cases, which reflect the reality that hacking into a restaurant is a very different crime from hacking into a power plant.

MYTH #2: THE REFORMS IN "AARON'S LAW" WOULD HALT CONTROVERSIAL PROSECUTIONS UNDER THE CFAA

Legislation in the Senate known as Aaron's Law[8] would eliminate the term "exceeding authorized access" from the CFAA.[9]

For a number of reasons, I think this is the wrong approach.

Eliminating "exceeding authorized access" from the CFAA would decriminalize insider hacking. Corrupt police officers like the notorious "Cannibal Cop" in New York City—who searched a sensitive government database in order to gather information about a potential victim—could no longer be charged under the CFAA.[10] Neither could Roberto Rodriguez, the employee of the Social Security Administration ("SSA"), who was convicted of searching the SSA's database for information used to stalk his ex-wife and sixteen other women.[11]

Aaron's Law also fails to relieve the overcriminalization concerns that exist about the current CFAA. Even under Aaron's Law, using your spouse's password to access his or her email account contrary to the applicable terms of service, or clearing the cookies on your computer to evade a paywall on a news site, would both likely constitute violations of the CFAA.

Senator Graham and I propose a different solution in the ICPA. Rather than decriminalizing insider hacking entirely, we propose to restrict such prosecutions to the most serious cases, where: (1) the value of the information obtained exceeds $10,000; (2) the hacking is done in furtherance of a limited group of state or federal felonies; or (3) government computers are targeted.

Further, we entirely forbid prosecutions based solely on consumer terms of service agreements.

---

8 Aaron's Law Act of 2015, S. 1030, 114th Cong.

9 Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(1) (2012).

10 United States v. Valle, 301 F.R.D. 53, 59–78 (S.D.N.Y. 2014). On December 3, 2015, the Second Circuit reversed Valle's CFAA conviction, holding that his personal use of a law enforcement database did not exceed his authorized access to the database. *See* United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015).

11 United States v. Rodriguez, 628 F.3d 1258, 1260–62 (11th Cir. 2010).

Myth #3
The CFAA Is Keeping Pace with the Tactics of Cyber Criminals

Critics of the CFAA argue that the statute should be narrowed, and that there is no need to expand its reach to cover emerging cybercrimes. I very strongly disagree.

One example is botnets. Although botnets are not new, these networks of compromised computers have never been more ubiquitous, more powerful, or posed a larger threat. In recent years, the criminals responsible for creating these networks have begun to outsource. They broker deals with resellers who sell access to the compromised computers in the botnet to other criminals in online forums and elsewhere.

No current crime captures this conduct, because the resellers have no role in damaging the compromised computers. And, assuming the resellers are smart enough not to ask too many questions of their clients, charging them with conspiracy or aiding and abetting a CFAA violation is a difficult case to make.

The ICPA recognizes that trafficking in compromised computers is criminal conduct and amends the CFAA by adding a new subsection to ensure that these cases can be prosecuted.

Those of us in Congress who are concerned about cybersecurity will continue to work to strengthen our laws and better protect our nation against cyber attacks. An important part of this work is ensuring that the CFAA remains effective and keeps pace with the rapidly evolving tactics of cyber criminals.

I thank Senator Graham for his partnership in this effort, and I thank Professor Orin Kerr and *The George Washington Law Review* for the opportunity to discuss my views on the right ways to reform the CFAA. I would be happy to answer any questions you may have.