Cybersecurity: Recommendations Regarding the CFAA

Names

University

Cybersecurity: Recommendations Regarding the CFAA

Ladies and gentlemen,

Information Technology is an integral part of our lives. We use computers in everything from commerce and defense to entertainment. However, computing has created an interconnected ecosystem to the extent that one malicious agent has the potential of wreaking havoc on entire economies. Take the credit card fraud case in New Jersey, in 2013, for example. That case indicted some individuals who stole over $300 million from companies such as Visa, Carrefour, and even NASDAQ – the largest fraud in the US history.

Thus, today, I wish to talk about some of the legal and legislative measures that the authorities have taken to ensure that future cybersecurity threats are dealt with comprehensively within the confines of the law. Specifically, my focus would be on the Computer Fraud and Abuse Act (CFAA). I will explain some of the recommendations regarding the implementation of the Act that I think would make it properly applicable in the ever-changing arena of technology, and ultimately, allow it to bolster cybersecurity.

I will divide my recommendations into three sections – those that must be implemented, those that I highly recommend, and those that I generally recommend.

# The “Must Implement” Recommendations

Let me start by reminding you that most authorities around the world go to great lengths to protect the information technology assets that are used in critical operations, such as governance, energy, and defense. In the US, the government even introduced the legal provision for ‘protected computers.’ These, as the National Information Infrastructure Protection Act (of 1996) puts it, are:

1. exclusively for the use of the Government of the United States, or
2. are used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

Moreover, it is illegal for people to tamper with the Government’s computing assets in a manner that leads to espionage, fraud, trespassing, among other concerns.

However, my main concern with these legal provisions is that they tend to be too vaguely worded, which has resulted in unfortunate incidences like that of the wrongful prosecution of Aaron Swartz, which ultimately led to his suicide. As the House Representative from California, Zoe Lofgren, put it in an Huffington Post article (in 2013), Americans were deeply troubled. People had now learnt that existing legislations like the CFAA (which was first enacted in 1986) could give the justice system room to misinterpret user agreement provisions of online services, leading to overly punitive sentences even in cases where no malice or misuse was intended.

Now apart from requiring the legislature to reword the laws to make them a bit more pragmatic, I would also wish to see authorities keeping abreast of the latest technological advancements to help them define what a “computer” is when applying the CFAA. In the *United States v. Neil Scott Kramer* (of 2011) case, for instance, the courts relied on the definition of a computer as found in 18 U.S.C. § 1030(e)(1), which states that a computer is a :

an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device …

However, I have a problem with that definition because it fails to appreciate that computing is a rapidly advancing technological field and that more electronic devices could act as computers even if they do not have the physical features of common computing devices.

My proposal would be for the legislature to employ computing specialists who could foresee how future computing devices could look like. That way, the laws would cover any crimes that could occur regarding information technology in posterity.

Apart from that, there are other laws that I would also highly recommend in matters concerning cybersecurity as pertains to the CFAA.

# The “Highly Recommend” Recommendations

Let me bring your attention to how the CFAA has evolved over the years. Let me start with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (of 2001) – which is a mouthful for what we usually call the Patriot Act. The main repercussion of this law is that it allows the government to spy on its citizens illegally – and that is using the same technologies that it discourages its citizens from tampering with. This weakness was first highlighted by a New York Times report (in 2005) titled *Spy Agency Mined Vast Data Trove*. We got wind that President Bush was essentially above the law when he employed the National Security Agency (NSA) to spy on Americans in the premise that it would facilitate the Government to listen in on terrorists before they struck.

Worryingly, the Atlantic reported in 2013 that the United Nations (UN) had found out more countries had gone the US surveillance way. The report cited copycat implementations in areas as far flung as the Middle East (in Bahrain) and Europe (in the Netherlands).

So, my proposal would be for the US to review the legislation it enacts carefully to avoid leading the world into a blatant abuse of computing technology. Remember, acts such as the Patriot Act straddle a fine line between oversight and contravention of fundamental rights like the Fourth Amendment, which provides for:

the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause (U.S. Constitution, 2017)

Besides, I am concerned that the US Government assumes that most computing aspects are primarily geared towards abuse. Take the proposal by President Obama (in 2015) to institute stricter legislation against cybercrime. He termed it as the Modernizing Law Enforcement Authorities to Combat Cyber Crime proposal, but in essence, it was an attempt to outlaw the majority of online activities. I would thus suggest that authorities look into ways of cultivating healthy computer usage instead of bogging it with punitive laws.

# The “Generally Recommend” Recommendations

But generally, I would recommend private entities to develop their computer use ethics in line with their organizational culture and avoid bringing in the CFAA every time they feel aggrieved. Take the 2011 case of *Lee v. PMSI, Inc.*, for instance. Why should companies drag the courts into internal affairs that trivialize the CFAA? My suggestion would be for institutions to interrogate their objectives when introducing some computing facilities and set the necessary ethical conduct requirements to reduce over-burdening the courts with matters that could be solved in-house concerning computer use.

# Conclusion

So, in conclusion, I wish to remind you that nearly four billion people are online at any particular time. Of course, a small percentage of those users are out to cause harm. But otherwise, the majority are getting entertained, educated, and growing their businesses. So, laws such as the CFAA will always be important to the system governing fair computer usage. But, that notwithstanding, fundamental rights should not be infringed upon in the guise of protecting the public.

Thank you.

References

Khazan, O. (2013, June 6). Actually, most countries are increasingly spying on their citizens, the UN says. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2013/06/actually-most-countries-are-increasingly-spying-on-their-citizens-the-un-says/276614/

Lee v. PMSI, Inc. (2011).

Lichtblau, E., & Risen, J. (2005, December 24). Spy agency mined vast data trove, officials report. *The New York Times*. Retrieved from http://www.nytimes.com/2005/12/24/politics/spy-agency-mined-vast-data-trove-officials-report.html

Reilly, R. J. (2013, January 15). Zoe Lofgren introduces ‘Aaron’s Law’ to honor Swartz on Reddit. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/01/15/zoe-lofgren-aarons-law-swartz\_n\_2483770.html

The White House. (2015, January 13). Securing cyberspace - President Obama announces new cybersecurity legislative proposal and other cybersecurity efforts. *The White House Press Release*. Washington, DC. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat

U.S. Congress. Computer Fraud and Abuse Act, Pub. L. No. 114–38 18 U.S. Code § 1030 (1986).

U.S. Congress. National Information Infrastructure Protection Act, Pub. L. No. 104–294 110 Stat. 3488 (1996).

U.S. Congress. Patriot Act, Pub. L. No. 107–56 115 Stat. 272 (2001).

U.S. Constitution. (2017). Fourth Amendment. Retrieved from https://www.law.cornell.edu/constitution/fourth\_amendment

United States v. Neil Scott Kramer (2011).