



Memorandum
Congressman J. Randy Forbes
*Virginia's Fourth Congressional
District*

TO: JRF
FROM: SS/AV
SUBJECT: CYBERSECURITY LEGISLATION
DATE: 4/1/2013
CC:

Sir- Below is a table of contents for the memo. The memo summarizes the draft legislation, and analyzes it by examining the cases that have shaped the recent arguments for and against pursuing violations of the Computer Fraud and Abuse Act (CFAA), with particular regard to charging individuals under the 'exceeds authorized access' provision of the CFAA.

- I. Bottom Line: Summary of the Proposed Legislation**
- II. Summary of Opposition to the CFAA**
- III. Discussion of the Proposed Amendments**
 - A. Increasing most of the current penalty maximums.
 - B. Including the CFAA as an offense under the federal RICO statute.
 - C. Adding economic espionage and damage to a critical infrastructure computer to the list of offenses under the CFAA.
 - D. Clarifying the definition of "exceeds authorized access."
 - 1. Current and proposed definitions
 - 2. Public response to the proposed change
 - 3. Courts of Appeals interpretation of the phrase
 - 4. Congressman Issa and Congresswoman Lofgren
 - E. Adding data breach notification requirements with civil penalties.
- IV. High Profile Prosecutions**
 - A. MySpace
 - B. David Nosal
 - C. Aaron Swartz
 - D. Matthew Keys
 - E. Andrew Auernheimer ("Weev")
- V. Involved Members of Congress**
- VI. Feedback from Outside Groups**
 - A. Information Technology Industry Council (ITI), Andy Halataei
 - B. ECPI University, Mark Dreyfus
- VII. Myths and Facts of the Application of the CFAA** *(provided by Republican Judiciary Staff)*
- VIII. Tough questions and proposed responses**

I. Bottom Line: Summary of the Proposed Legislation

The proposed legislation seek to fix several issues within the CFAA and cover five main categories:

1. Increasing most of the penalty maximums;
2. Including the CFAA as an offense under the federal RICO statute;
3. Adding economic espionage and damage to a critical infrastructure computer to the list of offenses under the CFAA;
4. Clarifying the definition of “exceeds authorized access”; and
5. Adding data breach notification requirements with civil penalties.

There are three particular events of note that are motivating some of these changes. These events are described in detail in Section III. In summary:

1. MySpace: Lori Drew was indicted under the CFAA for creating a fake MySpace page and posing as a teenage boy to taunt her daughter’s rival, who eventually killed herself. The district court judge ultimately threw out the charges, stating that the prosecution had reached beyond the intended scope of the CFAA.
2. David Nosal: David Nosal worked with former colleagues to retrieve data from Korn/Ferry and set up a competing business. Though the colleagues had access to the information as employees, company policy prohibited employees from disclosing confidential information. In a controversial decision, the 9th Circuit broke from other circuits’ interpretations of the statute and ruled that the phrase “exceeds authorized access” does not apply to violations of an end user agreement.
3. Aaron Swartz: Aaron Swartz was charged under the CFAA for downloading millions of paid-access scholarly articles from JSTOR, intending to make them publically available. He killed himself before his case came to trial and his suicide has become a platform for CFAA reform. Congresswoman Lofgren has dubbed her proposed legislation “Aaron’s Law” in his memory and Congressman Issa spoke at Aaron’s memorial on Capitol Hill.

The proposed additions to the definition of “exceeds authorized access” attempt to achieve two fixes:

The MySpace Fix acknowledges that using the CFAA in cases like Lori Drew is a prosecutorial overreach and not consistent with the originally intended scope of the statute. The MySpace Fix attempts to prevent future prosecutions by defining a minimum level of severity for the cyber trespass, thus preventing federal prosecution for falsifying information on a social networking site or for accessing personal e-mail at work in violation of an employer’s computer policy.

The Nosal Fix recognizes that in many instances, individuals who commit cyber crime do so by exceeding their authorized access to corporate and government databases and, contrary to the 9th Circuit’s decision, preserves the “exceeds authorized access language” for such infractions. With the MySpace Fix firmly in place, the phrase “exceeds authorized access” cannot extend to minor infractions of end user agreements and should ease the concerns expressed by the 9th Circuit.

II. Summary of Opposition to the CFAA

Much of the tech community stands in strong opposition to the CFAA in its entirety and has been using the suicide of Aaron Swartz as a platform for massive change. The Electronic Frontier Foundation has set up a page to aid individuals to contact their representatives entitled “The Computer Fraud and Abuse Act is broken. Tell Congress to fix it.”¹

Anti-CFAA groups have requested three major changes:

1. No more criminal penalties for violating a website's fine print
2. No criminal penalties for circumvention techniques that protect privacy and promote security
3. Make penalties proportionate to offenses

A recent letter from several tech companies, including Reddit, O'Reilly Media, and the American Library Association sent a [letter](#) to Chairman Sensenbrenner and Ranking Member Bobby Scott asking them to amend the CFAA “to ensure it does not chill the development” of software and services. According to the letter, the three major changes to the CFAA these organizations have requested are:

1. Ensuring the violations of terms of service, contractual agreements, or other legal duties do not violate the statute;
2. Protecting technical steps necessary for interoperability and innovative means of access; and
3. Fixing the statute's penalty scheme so that the punishment better fits the crime, including making sure that prosecutors can't double-charge for the same conduct and ensuring that felony punishments only apply to most egregious behavior.

Opponents of the bill argue that the CFAA, both as it currently stands and in the proposed amendments, would have made a criminal of a young Bill Gates who hacked into his school's computer system to have mostly female classmates, as well as many other tech giants who have engaged in hacking at some point in their careers. Furthermore, opponents want to protect the ability to hack into computers, arguing that such hacking helps to fuel innovation and improve cyber security.

¹ https://action.eff.org/o/9042/p/dia/action/public/?action_KEY=9005

III. Discussion of the Proposed Amendments

A. Increasing most of the current penalty maximums.

The discussion draft completely strikes the old penalty language, replacing it with new language and doubling the imprisonment terms for most offenses. There are no penalty minimums in the current CFAA or in the proposed amendments.

Proposed Changes to CFAA Penalties <i>Chart Provided by Republican Judiciary Staff</i>	
Existing Law	Proposed Changes
<i>Computer crime involving national security information</i>	
Unauthorized access of a computer to obtain national security information: up to 10 years (up to 20 years for repeat offenders) 18 U.S.C. 1030(c)(1)	Up to 20 years, removes penalty for repeat offenders
<i>Obtaining information from computers by unauthorized access or by exceeding authorized access</i>	
With intent to defraud: up to 5 years (up to 10 years for repeated offenders) 18 U.S.C. 1030(c)(3)	Up to 20 years, removes penalty for repeat offenders
For commercial or financial gain, to further criminal or tortuous acts, or if the value of the information exceeds \$5,000: up to 5 years (up to 10 years for repeat offenders) 18 U.S.C. 1030(c)(2)(B) and (C)	Up to 10 years, removes penalty for repeat offenders
Otherwise obtains information: up to 1 year 18 U.S.C. 1030(c)(2)(A)	Up to 3 years
Simple trespass into a computer: up to 1 year (up to 10 years for repeat offenders) 18 U.S.C. 1030(c)(2)(A), (C)	Up to 1 year
<i>Causing damage to computers</i>	
Knowingly or recklessly causing death: any term of years in prison or life 18 U.S.C. 1030(c)(4)(F)	Any term of years in prison or life
Knowingly or recklessly causing serious bodily injury: up to 20 years 18 U.S.C. 1030(c)(4)(E)	Removed
Knowingly causing \$5,000 or more in damage, involving medical treatment, causing physical injury, threat to public safety, affecting a law enforcement, national security or national defense computer, affecting 10 or more protected computers: up to 10 years (20 years for repeat offenders) 18 U.S.C. 1030(c)(4)(B), (C)	Up to 20 years, removes penalty for repeat offenders
Recklessly causing \$5,000 or more in damage, involving medical treatment, causing physical injury, threat to public safety, affecting a law enforcement,	Up to 20 years, removes penalty for repeat offenders

national security or national defense computer, affecting 10 or more protected computers: up to 10 years (up to 20 years for repeat offenders) 18 U.S.C. 1030(c)(4)(A), (C)	
Causing loss: up to 10 years for repeat offenders 18 U.S.C. 1030(c)(4)(D)	Removed
Otherwise causing damage: up to 1 year 18 U.S.C. 1030(c)(4)(A), (C)	Up to 1 year
<i>Trafficking in passwords</i>	
Up to 1 year (up to 10 years for repeat offenders) 18 U.S.C. 1030(c)(2)(A),(C)	Up to 10 years, removes penalty for repeat offenders
<i>Extortion (threatening to damage computers)</i>	
Up to 5 years (up to 10 years for repeat offenders) 18 U.S.C. 1030(c)(3)	Up to 10 years, removes penalty for repeat offenders

Additionally, the draft legislation amends the current criminal forfeiture provisions to provide for both criminal and civil forfeiture of both personal and real property.

The draft legislation amends the current criminal forfeiture provisions to provide for both criminal and civil forfeiture. A civil action may be brought under the statute in limited circumstances, such as impairing a medical diagnosis or causing physical injury, and allows for compensatory damages and injunctive or other equitable relief.²

B. Including the CFAA as an offense under the federal RICO statute.

The CFAA is not currently included in the list of qualifying offenses under RICO. The discussion draft adds the CFAA to the list of RICO offenses to better facilitate the prosecution of hacking groups and organizations.

C. Adding economic espionage and damage to a critical infrastructure computer to the list of offenses under the CFAA.

The maximum penalty for economic espionage under § 1031(a) will increase from 15 to 20 years.

The amendments also create a section of the CFAA, § 1030A, with a new offense of damage to a critical infrastructure computer. Under this offense, a person who intentionally causes or attempts to cause damage to a critical infrastructure computer in the process of a felony violation of § 1030 could face a sentence of up to 30 years, without probation.

A critical infrastructure computer is defined as “a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated.”

² § 1030(g)

D. Clarifying the definition of “exceeds authorized access.”

The CFAA criminalizes knowingly accessing a computer without authorization or exceeding authorized access where such conduct is done with specified intent or results in specified outcomes. It is fairly self-apparent when an individual has violated the act by knowingly accessing a computer without authorization. However, there has been a significant amount of disagreement over the definition of “exceeding authorized access,” and the definition needs to be clarified in order to achieve consistent application of the statute.

1. Current and proposed definitions

The CFAA currently defines “exceeds authorized access” as meaning “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.”

The discussion draft changes this definition to “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter, *even if the accesser may be entitled to obtain or alter the same information in the computer for other purposes.*”

After incorporating the proposed changes, exceeding authorized access is only criminalized when combined with at least one of the following additional actions:

- Obtained information deemed to require protection against unauthorized access for reasons of national defense or foreign relations (§ 1030(a)(1));
- Obtains information from
 - A record of a financial institution,
 - Any department or agency of the United States, or
 - Any protected computer (§ 1030(a)(2)(A)); or
- Obtains information from a computer and the offense
 - Involves information exceeds \$5,000 in value,
 - Was committed to obtain sensitive or non-public information of another entity or individual, including wills, financial records, diaries, photographs, private correspondence, medical records, and trade secrets,
 - Was committed in furtherance of any criminal act (federal or state), unless the underlying state law would be based only on obtaining information without authorized access, or
 - Involves information obtained from a computer used by or for the government (§ 1030(a)(2)(B)).

2. Public response to the proposed change

Clarifying the unauthorized access element of the CFAA is likely to draw the most public attention and criticism. Until last year, the federal appellate courts had interpreted the phrase to apply to employees who violate end user agreements, including company computer use policies, to access company information without authorization or to access information for non-business purposes. However, the 9th Circuit’s decision in *United States v. Nosaj* in August, 2012 created a split in how the circuits have interpreted the phrase.

The discussion draft's alteration of the definition will likely be seen as a congressional override of the 9th Circuit's decision, which many support.

3. Courts of Appeals interpretation of the phrase

Courts have generally interpreted the definition of "exceeds authorized access" to mean one of the following three things:

1. The term exceeds authorized access does apply to violations of an end user agreement. An employee exceeds authorized access when they impermissibly use that access information without permission or to take information they were permitted to see but used it for an impermissible purpose.
2. The term exceeds authorized access cannot apply to violations of an end user agreement. However, when an employee uses their access to impermissibly view or use information, their authorized access has ceased and they are accessing information "without authorization." *This interpretation allows the court to limit the definition of "exceeds authorized access" while still leaving room for employees who misuse information from an employer database to be prosecuted under the CFAA.*
3. The term exceeds authorized access cannot apply to violations of an end user agreement.

In *Nosal*, the **9th Circuit** ruled that the phrase "exceeds authorized access" does not apply to violations of an end user agreement. The court articulated a series of concerns for its decision, including wariness that the statute could be used to unfairly prosecute and imprison individuals who lie about their age and weight on a dating service site, who allow other individuals to access social media accounts in violation of user agreements, and employees who impermissibly but harmlessly use work computers to access news, shopping, and social media. The dissenting opinion referred to the majority's opinion as successfully knocking down several straw men in a parade of horrible that distracted the majority from addressing the real issue. The 9th Circuit remanded the case to the district court and no final decision has been issued in the case. On March 12, 2013, the district court refused *Nosal's* motion to dismiss the CFAA charges in light of the 9th Circuit's ruling, holding that properly accessing a computer with one's username and password and then turning that computer over to a third party may still be a violation of the CFAA.

Shortly after the 9th Circuit issued its opinion, the **4th Circuit** adopted the same reasoning in *WEC Carolina Energy Solutions LLC v. Miller*, taking what the court called a literal and narrow interpretation of the phrases "without authorization" and "exceed authorized access." The court agreed with the 9th Circuit's reasoning "that the CFAA fails to provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded." The court stated:

Our conclusion here likely will disappoint employers hoping for a means to rein in rogue employees. But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy. *See Nosal*, 676 F.3d at 863. ("We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals."). Providing such recourse not only is unnecessary, given that other legal remedies exist for these grievances, also is violative of the Supreme Court's counsel to

construe criminal statutes strictly. *Lanier*, 520 U.S. at 266. Thus, we reject an interpretation of the CFAA that imposes liability on employees who violate a use policy, choosing instead to limit such liability to individuals who access computers without authorization or who obtain or alter information beyond the bounds of their authorized access.

A **district court** in the **2d Circuit** also recently adopted the *Nosal* reasoning. On March 20, 2013, a federal judge in the Southern District of New York released his opinion in *JCB Holdings NY, LLC v. Pakter*. An employee of an executive placement service used her access to her employer's databases to gain information to support her own competing business. The employer alleged a violation under the CFAA. The district court acknowledged that although other district courts within the 2d Circuit have split between the narrow and broad definitions of "exceeds authorized access," the court chose the narrow definition under the same reasoning as *Nosal*.

Most other circuits to consider the phrase have concluded that the statute *does* apply to end user agreements including:

- *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001). The **1st Circuit** held that an employee likely exceeded his authorized access when he used that access to disclose information in violation of an employee confidentiality agreement.
- *United States v. John*, 597 F.3d 263, 271-73 (5th Cir. 2010). The **5th Circuit** upheld a conviction where an employee exceeded her authorized access by accessing confidential customer information in violation of the employer's computer use policy. The obtained information was then used to commit fraud. The court stated that when an employee "knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of [a criminally fraudulent] scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access.'" *Id.* at 273.
- *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). The **7th Circuit** held that an employee's authorization to access his employer's laptop ended when he breached his duty of loyalty. Once the duty of loyalty was breached, what was previously authorized access became unauthorized access.
- *United States v. Teague*, 646 F.3d 1119, 1121-22 (8th Cir. 2011). The **8th Circuit** upheld a conviction where an employee of a government contractor used his privileged access to a government database to obtain President Obama's private student loan records.
- *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). The **11th Circuit** upheld a one year sentence for a Social Security Administration employee who used a government database to look up the personal information of seventeen people for personal reasons, despite the fact that the Administration's policy prohibited using the database for anything other than official business purposes. The court upheld Rodriguez's conviction under the plain language of the statute barring someone from unauthorized access and the Administration's policy that information was only accessible for business purposes.

4. Congressman Issa and Congresswoman Lofgren

Congressman Issa and Congresswoman Lofgren have both put spoken in favor of reforming the CFAA. Congressman Issa, in conjunction with Congressman Cummings, recently began investigating the Justice Department's prosecution of Aaron Swartz. Aaron killed himself in January after being charged under the CFAA for downloading millions of paid-access scholarly articles from JSTOR and making them publically available. Congressman Issa stated, "I'm not condoning his hacking, but he's certainly someone who worked very hard. . . . Had he been a journalist and taken that same material that he gained from MIT, he would have been praised for it. It would have been like the Pentagon Papers."³

Congresswoman Lofgren's draft legislation would eliminate the "exceeds unauthorized access" element of the CFAA entirely and has dubbed it "Aaron's Law." In a recent interview, she stated, "I do think we need to take a look at [protecting] private users, people who are not making commercial exploitation of copy protected material. We need to take a look at the whole statutory damages issue... what we're doing now is clearly not working. It brings law enforcement and the federal government into disregard, especially among young people."⁴

E. Adding data breach notification requirements with civil penalties.

The proposed amendments create a national standard for security breach notifications and impose civil penalties for organizations that fail to adhere to the notification requirements. Data breach notification laws are currently in effect in at least forty-six states, and many claim the variations between states are so numerous that businesses engaged in interstate commerce are faced with compliance challenges.⁵ The proposed amendments would preempt all current state laws and create a single, national standard for notifying customers that their personal information has been hacked.

Covered entities, defined as "a commercial entity that acquires, maintains, stores, or utilizes personal information," will be required to notify affected customers within fourteen days of a security breach. Where a breach is discovered by a third party entity or service provider, they are required to notify the covered entity who can, in turn, notify affected customers. If the breach constitutes a major security breach, a covered entity is required to notify the Secret Service of the FBI within seventy-two hours of when the breach occurred. The current discussion draft seems to require notification from the date of breach and not from the date of discovery of the breach (see sec. 201(a)). It is also unclear in sec. 201(b)(3) whether a covered entity has 14 days from the breach of 14 days from notice when notified by a third party entity or service provider to notify affected customers.

Notification may be delayed if a state or federal law enforcement, national security, or homeland security agency determines that notification under the statute would impede a civil or criminal investigation. Notification may be delayed for the length of time deemed necessary by the law enforcement agency. There is a maximum civil penalty of \$50,000 for any covered entity that violates the requirements. Intentional violations carry a maximum penalty of \$1,000,000. Private causes of action are prohibited.

³ Zach Carter, *Darrell Issa Probing Prosecution Of Aaron Swartz, Internet Pioneer Who Killed Himself*, HUFFINGTON POST, Jan. 15, 2013 (10:46 AM), <http://www.huffingtonpost.com/2013/01/15/darrell-issa-aaron-swartz- n 2481450.html>.

⁴ Joe Mullin, *Ars Q&A: Silicon Valley Congresswoman talks the 2013 tech agenda*, ARSTECHNICA, Jan. 13, 2013 (9:00PM), <http://arstechnica.com/tech-policy/2013/01/silicon-valley-congresswoman-lays-out-tech-agenda-for-2013/>

⁵ <http://www.crs.gov/Products/R/PDF/R42475.pdf>.

IV. High Profile Prosecutions

A. MySpace⁶

Lori Drew was indicted under the CFAA for creating a MySpace page under a fake identity that she used to contact Megan Meier, a girl with whom her daughter had been feuding. Drew posed as a 16 year old boy who was interested in Megan and used the account to pick on her. Megan eventually killed herself.

When prosecutors could not find an applicable state charge to bring against Drew, federal prosecutor took up the case under the CFAA on the theory that Drew had exceeded authorized access by creating a fake profile with the intent to cause harm to Megan. Drew was charged with 4 felony counts under the CFAA and a jury convicted her of three misdemeanor charges, throwing out the fourth charge. The district court judge, however, threw out the charges on the grounds that the prosecution had reached beyond the intended scope of the CFAA.

B. David Nosal

David Nosal worked with former colleagues to retrieve data without authorization from former employer Korn/Ferry in order to set up a competing business. Though the colleagues were employed by Korn/Ferry and had access to the databases, company policy prohibited employees from disclosing confidential information. Nosal was convicted of aiding and abetting his former colleagues in exceeding their authorized access in violation of the CFAA.

On appeal, the 9th Circuit ruled that the phrase “exceeds authorized access” does not apply to violations of an end user agreement. The court articulated a series of concerns for its decision, including wariness that the statute could be used to unfairly prosecute and imprison individuals who lie about their age and weight on a dating service site, who allow other individuals to access social media accounts in violation of user agreements, and employees who impermissibly but harmlessly use work computers to access news, shopping, and social media. The dissenting opinion referred to the majority’s opinion as successfully knocking down several straw men in a parade of horrible that distracted the majority from addressing the real issue.

C. Aaron Swartz

Aaron Swartz was charged under the CFAA for downloading millions of paid-access scholarly articles from JSTOR and making them publically available. He was facing up to 35 years in prison. Tragically, Aaron killed himself earlier this year, 2013. His suicide has made him a martyr among those who believe that all information on the internet should be public property and has become a platform for CFAA reform. Congresswoman Lofgren has dubbed her proposed legislation “Aaron’s Law” in his memory and Congressman Issa spoke at Aaron’s memorial on Capitol Hill.

Attorney General Holder defended the Justice Department’s decision to prosecute Aaron in a Senate hearing against heavy questioning by Senator John Cornyn. General Holder stated that Aaron had

⁶ <http://latimesblogs.latimes.com/lanow/2009/07/myspace-sentencing.html/>

refused multiple plea deals that would have capped his sentence at 3 to 6 months.⁷ It is important to note that Aaron was investigated by the FBI in 2009 for downloading more than 18 million pages of information from the government-run Public Access to Court Electronic Records, PACER.⁸

D. Matthew Keys⁹

Matthew Keys, a Reuters employee, was charged with conspiracy to cause damage to a protected computer. He was disgruntled after being fired from his job at the Tribune Co. In retaliation, he provided his user name and password to the Tribune system to hackers associated with the group Anonymous. The hackers then used the access information to change a headline on an LA Times article. Matthew was indicted for conspiracy under § 1030(a)(5)(A) and (c)(4)(B) to _____ and with attempt to cause the transmission of a program, information, code, and command to intentionally cause damage without authorization for a protected computer that would have resulted in at least \$5,000 in loss.

E. Andrew Auernheimer (“Weev”)¹⁰

Andrew was found guilty of identity fraud and conspiracy to access a computer without authorization in November, 2012 after he found a security breach in AT&T’s website that allowed him to access thousands of e-mail addresses of iPad users. He then gave the e-mail addresses to a journalist in a claimed effort to expose AT&T’s security flaws. Michael Bloomberg and Rahm Emanuel were among the individuals whose e-mails were revealed. Andrew was sentenced to over three years in prison and fined over \$73,000 in damages.

⁷ <http://www.theverge.com/2013/3/6/4072518/attorney-general-holder-defends-aaron-swartz-prosecution>

⁸ <http://www.cnn.com/2013/01/12/us/new-york-reddit-founder-suicide>

⁹ <http://www.nytimes.com/2013/03/18/technology/outcry-over-computer-crime-indictment-of-matthew-keys.html?pagewanted=all& r=1&>

¹⁰ <http://www.guardian.co.uk/technology/2013/mar/18/us-hacker-andrew-auernheimer-at-t>

Summary of Charges

Name	CFAA Subsection(s) Charged		Sentence	Comments
Lori Drew	(a)(2)(C)	UA or EAA and obtains information from any protected computer*	Jury convicted, District Judge threw out	
David Nosal	(a)(4)	UA or EAA to a protected computer knowingly and with intent to defraud and obtains something of value worth >\$5,000	9th Circuit dismissed	
Aaron Swartz	(a)(4), (a)(2), (a)(5)(B)	<p>UA or EAA to a protected computer knowingly and with intent to defraud and obtains something of value worth >\$5,000</p> <p>UA or EAA and obtains information from a financial institution, any US department or agency, or any protected computer</p> <p>Intentionally access a protected computer and as a result, recklessly causes damage</p>	Never went to trial	<p>Justice Department offered plea deal with 3-6 months</p> <p>Aaron was originally charged with (a)(4); (a)(2); (c)(2)(B)(iii); (a)(5)(B); (c)(4)(A)(i)(I), (VI). Indictment was modified after <i>Nosal</i> was decided</p>
Matthew Keys	(a)(5)(A)	Knowingly causes transmission of information, causing damage without authorization to a protected computer	Trial pending	
Andrew Auernheimer ("Weev")	(a)(2)(C)	UA or EAA and obtains information from any protected computer	Convicted, sentenced to 3 years, appealing	Prison sentence also took into account ID theft conviction

* A protected computer includes most computers used for a financial institution or the US government and computers used in or affecting interstate or foreign commerce or communication, § 1030(e)(2).

V. Feedback from Outside Groups

A. Information Technology Industry Council (ITI), Andy Halataei

Andy Halataei has reviewed the draft legislation and met with Caroline Lynch from the Judiciary Committee. Most of ITC's concerns are with the data breach notifications section of the amendments.

ITI "strongly supports" a common sense, uniform national data breach standard. They submitted a three page document (see attachment in Section IX) of key elements they believe such a standard should include. They also submitted the following feedback in response to the current draft:

House Data Breach Notification Bill Comments

Sec 201 Clarify the use of the word 'data' rather than 'security'

In the draft bill, we believe the word "data breach," or "data" would be more appropriate than the word "security breach" "or security" where appropriate. Data breach refers to instances where personally identifiable information is been breached or compromised, whereas a "security breach" is a broader term and concept that could encompass any type of security incident, even if personal data is not compromised. As an industry we have had concerns in the past year with three other proposals to mandate reporting of security breaches including: The FY2013 NDAA Act (Section 941), The Secure IT Act of 2012 (Sec. 102), and the European Union (EU)'s proposed Cybersecurity Directive.

Sec 201(a) Include stronger notification trigger requirement

Under the bill, notification is required any time there is a "security breach" – which could be interpreted to mean any unauthorized access or acquisition of personal information. Most previous data breach notification bills have included a trigger that requires notice only when there is a reasonable risk of identity theft, fraud, or other unlawful conduct. As drafted, this bill could require notice if (for example) an employee at a call center accessed the "personal information" for Tom Johnson rather than Tim Johnson. There should be both an exception for good faith acquisition (which is found under most state laws) and a strong risk trigger (i.e. identity theft, fraud, or other unlawful conduct) before notice is required. We would recommend the addition of language from the Toomey data breach bill (or similar language) that reads:

(1) IN GENERAL.—A covered entity that owns or licenses data in electronic form containing personal information shall give notice of any breach of the security of the system following discovery by the covered entity of the breach of the security of the system to each individual who is a citizen or resident of the United States whose personal information was or that the covered entity reasonably believes to have been accessed and acquired by an unauthorized person and that the covered entity reasonably believes has caused or will cause, identity theft or other financial harm.

Sec 201(a) Provide for adequate time notice requirement

Our first preference would be the notification should be required "*as expeditiously as practicable and without unreasonable delay, consistent with any measures necessary to determine the scope of the security*

breach and restore the reasonable integrity of the data system that was breached.” as written in the Toomey data breach bill and is the standard found in most state data breach laws. Only a few states require notice within a particular timeframe, the shortest of 45 days under Florida law.

Second, any timeline or notification trigger must start upon discovery of the breach, not when the breach occurred, in a way that is consistent with measures to identify affected individuals and restore the integrity of the data system. The draft bill starts the notification timeline with the occurrence of the breach.

We are also very concerned with a second notification requirement of only 72 hours for “Major Security Breaches” to law enforcement. Federal legislation must allow entities to conduct thorough investigations of suspected security breaches before notifying customers or government agencies. A tremendous amount of forensics, decision-making, and legal work is required before ascertaining the nature and scope of a breach and determining the appropriate form of notification to a federal regulator. Federal legislation must provide realistic and workable time requirements.

Sec 201: Add method of notification language:

The draft bill should accommodate both traditional companies that communicate with customers by mail, telephone or fax and online companies that communicate predominantly through electronic communication (e.g., electronic mail). Consumer trust is essential in an effective breach notice and they should be notified in a manner that is consistent with previous communications and is done so in an expedient and timely manner. A consumer receiving a telephone call from their email provider outlining a breach and urging action would be justifiably suspicious. We would urge the addition of such language in the Toomey data breach bill that reads:

METHOD OF NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) shall be in compliance with such requirement if the covered entity provides such notice by one of the following methods:

- (i) Written notification, sent to the postal address of the individual in the records of the covered entity.*
- (ii) Telephone.*
- (iii) Email or other electronic means.*

Sec 202 Civil Remedies:

State AG Enforcement: We have no objection to the inclusion of state AG enforcement as allowed by most federal consumer protection laws.

We have concerns with the level of fines provided for in the bill and the increased fines for so-called “intentional” violations.

Sec. 203 Definitions

Remove soft preference for encryption: The bill specifically mentions encryption as one possible method for rendering data unreadable under the notification safe harbor. We would recommend the draft strike the word “encryption” and use a more tech neutral approach such as the language found in the President’s data breach proposal which reads: *“There shall be a presumption that no significant risk of harm to the individual whose sensitive personally identifiable*

information was subject to a security breach if such information was otherwise rendered unusable, unreadable, or indecipherable through the use of data security technology that is generally accepted by experts in the field of information security as an effective information security practice.”

Sec. 204 Clarify State Preemption Language

The preemption language in Sec. 204 should include the word ‘data’ to clarify the bill’s intent to preempt state data breach notification laws as opposed to other ‘security’ laws that various states have passed. Language found in the Toomey data breach bill reads: *“This Act preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, relating to the protection or security of data in electronic form containing personal information or the notification of a breach of security.”*

B. ECPI University, Mark Dreyfus

After reviewing the draft legislation and the section by section analysis provided by the Judiciary Committee staff, Mr. Dreyfus responded, “This looks fine to us.”

VI. Involved Members of Congress

Members of Congress who have recently voiced opinions on the CFAA include: Congressman Issa, Congresswoman Lofgren, Congressman Scott, Congressman Sensenbrenner, and Senator Cornyn.

General Commentary

The House Subcommittee on Crime, Terrorism, Homeland Security and Investigations held a hearing on March 13, 2013 at which several committee members seemed disinclined to relax provisions of the CFAA.

According to *The Hill*, Congressman Bobby Scott “said he is open to updating the CFAA to address new threats but that lawmakers must be careful to ‘actually improve the law and not just ratchet up penalties in an exercise of soundbite politics’ He said he is opposed to mandatory minimum penalties, which he said often result in sentences that are ‘violative of common sense.’”¹¹

Similarly, “Congressman Jim Sensenbrenner said that it may be time for Congress to ‘augment and improve’ the CFAA to address international criminal groups. He said he would be concerned with any proposal that would decriminalize computer abuse that is currently illegal but . . . warned that exempting terms of service violations could create loopholes in the law and legalize some damaging behavior.”¹²

On March 20, a group of tech companies, including Reddit, O’Reilly Media, and the American Library Association sent a letter to Chairman Sensenbrenner and Ranking Member Bobby Scott asking them to amend the CFAA “to ensure it does not chill the development” of software and services. According to the letter, the three major changes to the CFAA these organizations have requested are:

¹¹ <http://thehill.com/blogs/hillcon-valley/technology/287987-house-lawmakers-skeptical-of-relaxing-computer-crime-law>

¹² <http://thehill.com/blogs/hillcon-valley/technology/287987-house-lawmakers-skeptical-of-relaxing-computer-crime-law>

1. Ensuring the violations of terms of service, contractual agreements, or other legal duties do not violate the statute;
2. Protecting technical steps necessary for interoperability and innovative means of access; and
3. Fixing the statute's penalty scheme so that the punishment better fits the crime, including making sure that prosecutors can't double-charge for the same conduct and ensuring that felony punishments only apply to most egregious behavior.

Aaron Swartz and Altering the Definition of "Exceeds Authorized Access"

Congressman Issa and Congresswoman Lofgren have both put spoken in favor of reforming the CFAA. Congressman Issa, in conjunction with Congressman Cummings, recently began investigating the Justice Department's prosecution of Aaron Swartz. Aaron killed himself in January after being charged under the CFAA for downloading millions of paid-access scholarly articles from JSTOR and making them publically available. Congressman Issa stated, "I'm not condoning his hacking, but he's certainly someone who worked very hard. . . . Had he been a journalist and taken that same material that he gained from MIT, he would have been praised for it. It would have been like the Pentagon Papers."¹³

Congresswoman Lofgren's draft legislation would eliminate the "exceeds unauthorized access" element of the CFAA entirely and has dubbed it "Aaron's Law." In a recent interview, she stated, "I do think we need to take a look at [protecting] private users, people who are not making commercial exploitation of copy protected material. We need to take a look at the whole statutory damages issue... what we're doing now is clearly not working. It brings law enforcement and the federal government into disregard, especially among young people."¹⁴

Congresswoman Zoe Lofgren recently told the Huffington Post, "The idea that you could be charged with multiple felonies and face up to 35 years in prison under the statute is a mistake. It needs to be changed The entire statute is in need of a complete overhaul. I mean, it was written in 1986. So on a parallel track, we should do that. But I also hope that we can act promptly to make some discrete changes in the statute so that no one else would face what Aaron faced."¹⁵

Congressman Jared Polis was quoted by The Hill as saying, "The charges were ridiculous and trumped-up. . . . It's absurd that he was made a scapegoat. I would hope that this doesn't happen to anyone else."¹⁶ According to The Hill, Congressman Polis called Aaron "a 'martyr' for why Congress should limit the discretion of prosecutors."

¹³ Zach Carter, *Darrell Issa Probing Prosecution Of Aaron Swartz, Internet Pioneer Who Killed Himself*, HUFFINGTON POST, Jan. 15, 2013 (10:46 AM), <http://www.huffingtonpost.com/2013/01/15/darrell-issa-aaron-swartz- n 2481450.html>.

¹⁴ Joe Mullin, *Ars Q&A: Silicon Valley Congresswoman talks the 2013 tech agenda*, ARSTECHNICA, Jan. 13, 2013 (9:00PM), <http://arstechnica.com/tech-policy/2013/01/silicon-valley-congresswoman-lays-out-tech-agenda-for-2013/>

¹⁵ <http://www.huffingtonpost.com/2013/01/17/aaron-swartz-prosecution n 2498586.html>

¹⁶ <http://thehill.com/blogs/hillicon-valley/technology/277353-lawmakers-blast-trumped-up-doj-prosecution-of-internet-activist>

Criminal Penalties

Congressman Loui Gohmert wants to decriminalize “hacking back,” which involves installing malware on one’s computer that, if hacked, causes the hacker’s computer to become infected and possibly send the user a picture of the hacker.¹⁷

Shortly after Aaron Swartz’s suicide, Senator John Cornyn sent a [letter](#) to Attorney General Holder, asking several pointed questions about the U.S. Attorney’s intent in prosecuting Aaron. The letter clearly articulates Senator Cornyn’s concerns that the prosecution was overly aggressive and that the charges were retaliation for Aaron’s prior actions and his significant number of information requests under the Freedom of Information Act. Senator Al Franken also sent a [letter](#) to Mr. Holder, asking to be copied on Mr. Holder’s response to Senator Cornyn.

Congressman John Conyers supports criminal penalties for data breach notification and included such penalties in his data breach bill last year, the Cyber Privacy Fortification Act of 2012, H.R. 6183 (112th). The bill was cosponsored by Congressman Henry Johnson and Congressman Bobby Scott.

VII. Myths and Facts of the Application of CFAA

MYTH: The draft legislation expands the application of the Computer Fraud and Abuse Act (CFAA).

FACT: The draft legislation significantly narrows the CFAA.

- Under current law, in order to prove a person guilty of certain provisions of the CFAA, the government need only prove that an individual
 1. intentionally
 2. exceeded authorized access, and
 3. obtained information from (A) a financial record of a financial institution, (B) a department or agency of the United States, or (C) any protected computer.

- Now, under the draft legislation, the government must prove that an individual
 1. intentionally
 2. exceeded authorized access,
 3. obtained information from (A) a financial record of a financial institution, (B) a department or agency of the United States, or (C) any protected computer, **AND**
 4. the offense (1) involves information that exceeds \$5,000 in value, (2) was committed for the purpose of obtaining sensitive or non-public information, (3) was committed in furtherance of certain criminal acts, or (4) involves information obtained from a computer used by or for a government entity.

- As with any criminal prosecution, the government has the burden of proving to a jury or a court each element of a CFAA offense (including the new element listed in #4 above) beyond a reasonable doubt. So, the government must introduce evidence to prove, for instance, that the information obtained is valued at \$5,000 or more.

¹⁷ <http://www.courthousenews.com/2013/03/13/55697.htm>

MYTH: The draft legislation threatens individual privacy.

FACT: The draft legislation protects individual privacy by keeping important cyber prosecution tools intact in the CFAA and requiring consumer notification of a data breach.

- Critics claim that draft bill threatens individual privacy. In fact, the opposite is true. By prosecuting individuals who access computers and read or download information they are not entitled to, Congress is actually enhancing the privacy of Americans.
- The draft legislation ensures that a person cannot exceed authorized access and obtain sensitive or non-public information including medical records, wills, diaries, private correspondence, financial records, photographs or a sensitive or private nature, trade secrets, or sensitive or non-public commercial business information.
- It's as simple as this: Just because you invite a friend to your house for dinner doesn't mean they have permission to rifle through your tax records or search your medicine cabinet.
- Certain proponents of CFAA reform have called for removing the ability of the government to prosecute a cyber criminal for exceeding authorized access to certain computer information. Doing so would significantly threaten personal, sensitive information held by private companies or in government databases and give hackers free reign to access private information from the inside.
 - Suppose a law enforcement officer accesses the National Crime Information Center (NCIC) computers in order to look up sensitive information about his ex-spouse, his girlfriends, and others. What if he goes further and does look-ups for money, not knowing how that information will be used by the purchaser.
 - Consider a recent investigation in which a system administrator used his access to company email systems to snoop on the email of the CEO and the company's lawyers, and funneled that information to a competing company.
 - What if a government employee accesses the passport information of political candidates, their student loan records, and their tax returns, and makes that information public?
- Title II of the draft legislation takes an important additional step to protect consumer privacy by establishing a national, uniform data breach notification requirement. If financial data, social security numbers or other personal information is accessed by hackers, the company must notify consumers and federal law enforcement. Consumers will now be better equipped to prevent identity theft or credit card fraud and law enforcement can investigate and prosecute the cyber criminals.

MYTH: A person who exceeds authorized access under the CFAA can easily be prosecuted under other existing federal laws.

FACT: There are certain cases in which a private sector or government employee violates his employer's computer use policy that are not chargeable by some other means but still threaten individual privacy and pose financial and other risks to the employer.

- Preventing all use of access policies to define the scope of authorization would, in some instances, prevent prosecution of exactly the kind of serious privacy violations that the Department handles on a

regular basis: situations where a government employee is given access to sensitive information stored by the State Department, Internal Revenue Service, or crime database systems subject to express access restrictions, and then violates those access restrictions to access the database for personal gain, the stalk individuals, or simply to publish it to gain notoriety.

- “In some cases, the very person responsible for monitoring the company's computer network for suspicious activity is the rogue employee himself. A survey last year of nearly 200 IT professionals found that ‘despite the attention that hackers and other external security threats receive, it is internal, not *external* threats, which are perceived as greater risks,’ according to the security firm AlgoSec.”¹⁸
- In many prosecutions involving insiders, the “terms of service” and similar rules in employment contexts define whether the individual charged was entitled to obtain or alter the information at issue.
- This is almost identical to prosecutions under other statutes, in which internal procedures, agreements, and communications must be examined by a fact-finder to determine, for example, whether a particular payment was authorized, or embezzlement or fraud.

MYTH: The addition of the CFAA as a RICO predicate allows the government to treat hackers like mobsters.

FACT: The addition of the CFAA as a RICO predicate allows the government to prosecute organized cyber rings.

- The CFAA is the primary statute used to prosecute hacking crimes. Computer technology has become a key tool of organized crime. Indeed, criminal organizations are operating today around the world to: hack into public and private computer systems, including systems key to national security and defense; hijack computers for the purpose of stealing identity and financial information; extort lawful businesses with threats to disrupt computers; and commit a range of other cybercrimes. Many of these criminal organizations are similarly tied to traditional Asian and Eastern European organized crime organizations.
- The addition of 18 U.S.C. § 1030 as a RICO “predicate” does not, by itself, make a person who violates the CFAA also guilty of RICO.
- In spite of its name and origin, RICO is not limited to “mobsters” or members of “organized crime” as those terms are popularly understood. Rather, it covers those activities which Congress believes characterize the conduct of organized crime, no matter who actually engages in them.
- In order to be prosecuted under the RICO statute, an individual must engage in a *pattern of racketeering* (i.e. the patterned commission of **two or more** designated state or federal crimes) or the *collection of an unlawful debt* in order to (a) acquire or operate an enterprise using racketeering proceeds; (b) control an enterprise using racketeering activities; or (c) conduct the affairs of an enterprise using racketeering activities.

¹⁸ Gerry Smith, “Matthew Keys Case Shows Rogue Employees Can Be Just As Dangerous As Hackers,” HUFFINGTON POST (Mar. 19, 2013), available at http://www.huffingtonpost.com/2013/03/19/matthew-keys-rogue-employee-hackers_n_2903021.html.

MYTH: The draft bill expands the CFAA to those who attempt or conspire to violate the statute.

FACT: The draft bill simply clarifies existing law and long-standing congressional intent.

- Whether or not a cyber criminal is ultimately successful in completing a crime, or is the person who actually “pushed the buttons” to commit the crime, should not matter – the intent of the criminal to commit a serious computer crime is what matters.
- Legislation sponsored by Senator Leahy and enacted during the 110th Congress (P.L. 110-326), amended subsection (b) to add conspiracies to the already existing prohibition against attempts.
- A drafting error in the penalties under subsection (c), which explicitly identifies attempts but not conspiracies, has led to confusion about whether Congress intended to punish both conspiracies and attempts as completed offenses.
- The clarification to subsection (b) corrects this drafting error and the resulting confusion and brings the offenses under the CFAA in line with a host of other federal statutes that subject all criminals with the same criminal intent to the same potential penalties.

VIII. Tough questions and proposed responses

The proposed amendments to the CFAA clarify the statutes vagueness that has concerned so many while preserving the government's ability to prosecute individuals who violate privacy and property rights, who cause significant damage to tangible and intangible property, and who hack into a critical infrastructure computer. Just because something can be done does not mean it should be done. The criminal code must deter a wrongful taking of another's property, whether tangible or intangible, in a way that promotes and encourages properly channeled innovation.

Anti-CFAA groups have requested three major changes to the current law:

1. No more criminal penalties for violating a website's fine print,
2. No criminal penalties for circumvention techniques that protect privacy and promote security, and
3. Make penalties proportionate to offenses.

The following chart is a list of claims from groups opposed to the CFAA and the proposed amendments, followed by suggested responses.

Claim	Response
<p>There should be no civil or criminal penalties for violating any terms of service, contractual agreement, or other legal duty.</p>	<p>There is a need to narrow the definition of EAA within the CFAA to ensure that individuals who harmlessly share passwords on a social media website or fudge their age and weight on a dating website cannot be criminally prosecuted under the CFAA.</p> <p>However, eliminating the EAA element altogether would handicap our ability to prosecute individuals who use granted access to a program or database to cause or attempt to cause harm to interests of privacy, property, and national security.</p> <p>The CFAA is an essential prosecutorial tool to reach those who breach personal and governmental computers and disclose information that is private, protected, or essential to national security.</p>
<p>Criminalizing hacking will put an end to security research. We need to protect technical steps necessary for interoperability and innovative means of access.</p>	<p>We agree that it is essential to maintain the ability to conduct research into the cyber health of government systems and private databases.</p> <p>However, for the safety and security of protected information, such research must be overseen. There should not be a safe harbor for those who abuse their impressive technical abilities to publicize private information.</p> <p><i>Thought: add a whistleblower safe harbor, with strict regulations as to what the hacker does with the information in order to qualify?</i></p>

<p>Penalties are disproportionate to the offense. Prosecutors should not be able to “double charge” for the same conduct.</p>	<p>This claim confuses the difference between double jeopardy and the legitimate ability of the prosecutor to charge multiple crimes based on the same conduct and reveals a misunderstanding of how the indictment and trial process functions.</p> <p>Most criminal indictments involve allegations of multiple crimes committed within a singular series of events. It is then up to the jury to determine whether the elements for each crime have been met to support a guilty verdict.</p> <p><i>Note: many democrats, including President Obama’s administration, have advocated for harsher, not lighter, criminal penalties. The proposed amendments to not adopt most of these recommendations.</i></p>
<p>The amendments criminalize just talking about hacking in violation of the CFAA.</p>	<p>False. The Amendments clarify that conspiracy is punishable to the same extent as a completed offense. It is already possible to charge an individual with conspiracy under the CFAA. Even if conspiracy were not in the CFAA, an individual could still be charged under the general conspiracy statute.</p>
<p>The amendments increase the possibility of the over prosecution faced by Aaron Swartz.</p>	<p>False. The amendments <i>narrow</i> the definition of “exceeds authorized access” under the statute, limiting the situations in which someone can be charged.</p> <p>Under the amended definition, there is a minimum threshold of trespass or damage that must be met before a criminal charge may be brought. An individual must exceed their authorized access to obtain specified private information AND the offense</p> <ul style="list-style-type: none"> • Involves information that exceeds \$5,000 in value • Was committed for purposes of obtaining sensitive or non-public information such as medical and financial records, private correspondence, or trade secrets • Was committed in furtherance of another crime OR • Involves information obtained from a computer used by or for a government entity.
<p>The proposed amendments are all bad; they make a bad bill worse.</p>	<p>The amendments actually address some of the concerns expressed by opponents of the CFAA. For example, the definition of EAA has been narrowed to make it clear that an individual cannot be prosecuted for lying about their age on a dating site or sharing a password to a social media account.</p> <p>The amendments create a distinction between moderate hacking and hacking that threatens national security and the public health and welfare by defining damage to a critical infrastructure computer and setting out a separate penalty scheme for this more serious offense.</p>

	<p>Finally, the creation of a national standard for data breach notification merely adopts the principles of required notification already in effect in 46 states, unifying the standard to ease the compliance burden on affected businesses.</p>
--	--

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 47 - FRAUD AND FALSE STATEMENTS

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

- (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
- (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
 - (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) ¹ of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
 - (B) information from any department or agency of the United States; or
 - (C) information from any protected computer;
- (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is 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;
- (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;
- (5)
 - (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
 - (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
 - (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.²
- (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
 - (A) such trafficking affects interstate or foreign commerce; or
 - (B) such computer is used by or for the Government of the United States;³
- (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscpri.html>).

- (A) threat to cause damage to a protected computer;
 - (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
 - (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;
- shall be punished as provided in subsection (c) of this section.
- (b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
 - (c) The punishment for an offense under subsection (a) or (b) of this section is—
 - (1) (A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
 - (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
 - (2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
 - (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—
 - (i) the offense was committed for purposes of commercial advantage or private financial gain;
 - (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
 - (iii) the value of the information obtained exceeds \$5,000; and
 - (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
 - (3) (A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
 - (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),⁴ or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
 - (4) (A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—
 - (i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

- (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;
 - (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
 - (III) physical injury to any person;
 - (IV) a threat to public health or safety;
 - (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or
 - (VI) damage affecting 10 or more protected computers during any 1-year period; or
 - (ii) an attempt to commit an offense punishable under this subparagraph;
 - (B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—
 - (i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or
 - (ii) an attempt to commit an offense punishable under this subparagraph;
 - (C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—
 - (i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or
 - (ii) an attempt to commit an offense punishable under this subparagraph;
 - (D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—
 - (i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or
 - (ii) an attempt to commit an offense punishable under this subparagraph;
 - (E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;
 - (F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or
 - (G) a fine under this title, imprisonment for not more than 1 year, or both, for—
 - (i) any other offense under subsection (a)(5); or
 - (ii) an attempt to commit an offense punishable under this subparagraph.
- (d) (1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
- (2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscpri.html>).

- (3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
- (e) As used in this section—
- (1) the term “computer” means 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;
- (2) the term “protected computer” means a computer—
- (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
- (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
- (3) the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
- (4) the term “financial institution” means—
- (A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
- (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
- (C) a credit union with accounts insured by the National Credit Union Administration;
- (D) a member of the Federal home loan bank system and any home loan bank;
- (E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
- (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
- (G) the Securities Investor Protection Corporation;
- (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
- (I) an organization operating under section 25 or section 25(a)¹ of the Federal Reserve Act;
- (5) the term “financial record” means information derived from any record held by a financial institution pertaining to a customer’s relationship with the financial institution;
- (6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
- (7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
- (8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;
- (9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
- (10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
- (11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscodeprint.html>).

to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses⁵ (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i) (1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A) such person’s interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section⁶

Footnotes

¹ See References in Text note below.

² So in original. The period probably should be a semicolon.

³ So in original. Probably should be followed by “or”.

⁴ So in original. The comma probably should not appear.

⁵ So in original. Probably should be “subclause”.

⁶ So in original. Probably should be followed by a period.

(Added Pub. L. 98–473, title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub. L. 99–474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub. L. 100–690, title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub. L. 101–73, title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub. L. 101–647, title XII, § 1205(c), title

[DISCUSSION DRAFT]113TH CONGRESS
1ST SESSION**H. R.** _____

To amend title 18, United States Code, to provide for additional restrictions on fraud and related activity in connection with computers, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend title 18, United States Code, to provide for additional restrictions on fraud and related activity in connection with computers, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “_____ Act
5 of 2013”.

1 **TITLE I—CRIMINAL PROVISIONS**

2 **SEC. 101. PROTECTING U.S. BUSINESSES FROM FOREIGN**
3 **ESPIONAGE.**

4 Section 1831(a) of title 18, United States Code, is
5 amended, in the matter after paragraph (5), by striking
6 “15 years” and inserting “20 years”.

7 **SEC. 102. FRAUD AND RELATED ACTIVITY IN CONNECTION**
8 **WITH COMPUTERS AS RICO PREDICATE.**

9 Section 1961(1)(B) of title 18, United States Code,
10 is amended by inserting after “section 1029 (relating to
11 fraud and related activity in connection with access de-
12 vices), section 1084 (relating to the transmission of gam-
13 bling information),” the following: “section 1030 (relating
14 to fraud and related activity in connection with com-
15 puters),”.

16 **SEC. 103. FRAUD AND RELATED ACTIVITY IN CONNECTION**
17 **WITH COMPUTERS.**

18 Section 1030 of title 18, United States Code, is
19 amended as follows:

20 (1) **TRAFFICKING IN PASSWORDS.**—In sub-
21 section (a), by striking paragraph (6) and inserting
22 the following:

23 “(6) knowingly and with intent to defraud traf-
24 fics (as defined in section 1029) in any password or
25 similar information or means of access through

1 which a protected computer as defined in subpara-
2 graphs (A) and (B) of subsection (c)(2) may be
3 accessed without authorization; or”.

4 (2) CONSPIRACY AND ATTEMPT.—In subsection
5 (b), by inserting “for the completed offense” after
6 “punished as provided”.

7 (3) PENALTIES.—By striking subsection (c)
8 and inserting the following:

9 “(c) The punishment for an offense under subsection
10 (a) or (b) of this section is—

11 “(1)(A) except as otherwise provided in this
12 paragraph, in the case of an offense under sub-
13 section (a)(5)(A) of this section, if the offender at-
14 tempts to cause or knowingly or recklessly causes
15 death from conduct in violation of subsection
16 (a)(5)(A), a fine under this title, imprisonment for
17 any term of years or for life, or both;

18 “(B) a fine under this title, imprisonment
19 for not more than 20 years, or both, in the case
20 of an offense under subsection (a)(5)(A) of this
21 section, if the offense caused—

22 “(i) loss to 1 or more persons during
23 any 1-year period (and, for purposes of an
24 investigation, prosecution, or other pro-
25 ceeding brought by the United States only,

1 loss resulting from a related course of con-
2 duct affecting 1 or more other protected
3 computers) aggregating at least \$5,000 in
4 value;

5 “(ii) the modification or impairment,
6 or potential modification or impairment, of
7 the medical examination, diagnosis, treat-
8 ment, or care of 1 or more individuals;

9 “(iii) physical injury to any person;

10 “(iv) a threat to public health or safe-
11 ty;

12 “(v) damage affecting a computer
13 used by, or on behalf of, an entity of the
14 United States Government in furtherance
15 of the administration of justice, national
16 defense, or national security; or

17 “(vi) damage affecting 10 or more
18 protected computers during any 1-year pe-
19 riod;

20 “(C) a fine under this title, imprisonment
21 for not more than 10 years, or both, in the case
22 of an offense under subsection (a)(5)(B), if the
23 offense caused a harm provided in clause (i)
24 through (vi) of subparagraph (A) of this sub-
25 section; or

1 “(D) a fine under this title, imprisonment
2 for not more than 1 year, or both, for any other
3 offense under subsection (a)(5) of this section;

4 “(2) a fine under this title or imprisonment for
5 not more than 20 years, or both, in the case of an
6 offense under—

7 “(A) subsection (a)(1) of this section; or

8 “(B) subsection (a)(4) of this section;

9 “(3) a fine under this title or imprisonment for
10 not more than 10 years, or both, in the case of an
11 offense under—

12 “(A) subsection (a)(6) of this section;

13 “(B) subsection (a)(7) of this section;

14 “(4)(A) except as provided in subparagraph
15 (B), a fine under this title or imprisonment for not
16 more than 3 years, or both, in the case of an offense
17 under subsection (a)(2); or

18 “(B) a fine under this title or imprison-
19 ment for not more than 10 years, or both, in
20 the case of an offense under paragraph (a)(2)
21 of this section, if—

22 “(i) the offense was committed for
23 purposes of commercial advantage or pri-
24 vate financial gain;

1 “(ii) the offense was committed in the
2 furtherance of any criminal or tortious act
3 in violation of the Constitution or laws of
4 the United States, or of any State; or

5 “(iii) the value of the information ob-
6 tained, or that would have been obtained if
7 the offense was completed, exceeds \$5,000;
8 or

9 “(5) a fine under this title or imprisonment for
10 not more than 1 year, or both, in the case of an of-
11 fense under subsection (a)(3) of this section;”.

12 (4) EXCEEDS AUTHORIZED ACCESS.—In sub-
13 section (a), by striking paragraph (2) and inserting
14 the following:

15 “(2) intentionally—

16 “(A) accesses a computer without author-
17 ization, and thereby obtains—

18 “(i) information contained in a finan-
19 cial record of a financial institution, or of
20 a card issuer as defined in section 1602(n)
21 of title 15, or contained in a file of a con-
22 sumer reporting agency on a consumer, as
23 such terms are defined in the Fair Credit
24 Reporting Act (15 U.S.C. 1681 et seq.);

1 “(ii) information from any department
2 or agency of the United States; or

3 “(iii) information from any protected
4 computer; or

5 “(B) exceeds authorized access, and—

6 “(i) thereby obtains from a computer
7 information defined in paragraph (A)(i)
8 through (iii); and

9 “(ii) the offense—

10 “(I) involves information that ex-
11 ceeds \$5,000 in value;

12 “(II) was committed for purposes
13 of obtaining sensitive or non-public in-
14 formation of an entity or another indi-
15 vidual (including such information in
16 the possession of a third party), in-
17 cluding medical records, wills, diaries,
18 private correspondence, financial
19 records, photographs of a sensitive or
20 private nature, trade secrets, or sen-
21 sitive or non-public commercial busi-
22 ness information;

23 “(III) was committed in further-
24 ance of any criminal act in violation
25 of the Constitution or laws of the

1 United States or of any State, unless
2 such state violation would be based
3 solely on the obtaining of information
4 without authorization or in excess of
5 authorization; or

6 “(IV) involves information ob-
7 tained from a computer used by or for
8 a government entity; or”.

9 (5) FORFEITURES.—By striking subsections (i)
10 and (j) and inserting the following:

11 “(i) CRIMINAL FORFEITURE.—(1) The court, in im-
12 posing sentence on any person convicted of a violation of
13 this section, or convicted of conspiracy to violate this sec-
14 tion, shall order, in addition to any other sentence imposed
15 and irrespective of any provision of State law, that such
16 person forfeit to the United States—

17 “(A) such person’s interest in any property,
18 real or personal, that was used, or intended to be
19 used, to commit or facilitate the commission of such
20 violation; and

21 “(B) any property, real or personal, consti-
22 tuting or derived from any gross proceeds, or any
23 property traceable to such property, that such per-
24 son obtained, directly or indirectly, as a result of
25 such violation.

1 “(2) The criminal forfeiture of property under this
2 subsection, including any seizure and disposition of the
3 property, and any related judicial or administrative pro-
4 ceeding, shall be governed by the provisions of section 413
5 of the Comprehensive Drug Abuse Prevention and Control
6 Act of 1970 (21 U.S.C. 853), except subsection (d) of that
7 section.

8 “(j) CIVIL FORFEITURE.—(1) The following shall be
9 subject to forfeiture to the United States and no property
10 right, real or personal, shall exist in them:

11 “(A) Any property, real or personal, that was
12 used, or intended to be used, to commit or facilitate
13 the commission of any violation of this section, or a
14 conspiracy to violate this section.

15 “(B) Any property, real or personal, consti-
16 tuting or derived from any gross proceeds obtained
17 directly or indirectly, or any property traceable to
18 such property, as a result of the commission of any
19 violation of this section, or a conspiracy to violate
20 this section.

21 “(2) Seizures and forfeitures under this subsection
22 shall be governed by the provisions in chapter 46 of title
23 18, United States Code, relating to civil forfeitures, except
24 that such duties as are imposed on the Secretary of the
25 Treasury under the customs laws described in section

1 981(d) of title 18, United States Code, shall be performed
2 by such officers, agents and other persons as may be des-
3 ignated for that purpose by the Secretary of Homeland
4 Security or the Attorney General.”.

5 (6) DEFINITION.—In subsection (e)(6), by in-
6 serting after “alter” the following: “, even if the
7 accesser may be entitled to obtain or alter the same
8 information in the computer for other purposes”.

9 **SEC. 104. DAMAGE TO CRITICAL INFRASTRUCTURE COM-**
10 **PUTERS.**

11 (a) IN GENERAL.—Chapter 47 of title 18, United
12 States Code, is amended by inserting after section 1030
13 the following:

14 **“SEC. 1030A. AGGRAVATED DAMAGE TO A CRITICAL INFRA-**
15 **STRUCTURE COMPUTER.**

16 “(a) DEFINITIONS.—In this section—

17 “(1) the terms ‘computer’ and ‘damage’ have
18 the meanings given such terms in section 1030; and

19 “(2) the term ‘critical infrastructure computer’
20 means a computer that manages or controls systems
21 or assets vital to national defense, national security,
22 national economic security, public health or safety,
23 or any combination of those matters, whether pub-
24 licly or privately owned or operated, including—

1 “(A) gas and oil production, storage, and
2 delivery systems;

3 “(B) water supply systems;

4 “(C) telecommunication networks;

5 “(D) electrical power delivery systems;

6 “(E) finance and banking systems;

7 “(F) emergency services;

8 “(G) transportation systems and services;

9 and

10 “(H) government operations that provide
11 essential services to the public.

12 “(b) OFFENSE.—Whoever, during and in relation to
13 a felony violation of section 1030, intentionally causes or
14 attempts to cause damage to a critical infrastructure com-
15 puter, and such damage results in (or, in the case of an
16 attempt, would, if completed have resulted in) the substan-
17 tial impairment—

18 “(1) of the operation of the critical infrastruc-
19 ture computer, or

20 “(2) of the critical infrastructure associated
21 with the computer,

22 shall be fined under this title, imprisoned for not more
23 than 30 years, or both.

24 “(c) CONSECUTIVE SENTENCE.—Notwithstanding
25 any other provision of law—

1 “(1) a court shall not place on probation any
2 person convicted of a violation of this section;

3 “(2) except as provided in paragraph (4), no
4 term of imprisonment imposed on a person under
5 this section shall run concurrently with any other
6 term of imprisonment, including any term of impris-
7 onment imposed on the person under any other pro-
8 vision of law, including any term of imprisonment
9 imposed for the felony violation section 1030;

10 “(3) in determining any term of imprisonment
11 to be imposed for a felony violation of section 1030,
12 a court shall not in any way reduce the term to be
13 imposed for such crime so as to compensate for, or
14 otherwise take into account, any separate term of
15 imprisonment imposed or to be imposed for a viola-
16 tion of this section; and

17 “(4) a term of imprisonment imposed on a per-
18 son for a violation of this section may, in the discre-
19 tion of the court, run concurrently, in whole or in
20 part, only with another term of imprisonment that
21 is imposed by the court at the same time on that
22 person for an additional violation of this section,
23 provided that such discretion shall be exercised in
24 accordance with any applicable guidelines and policy

1 statements issued by the United States Sentencing
2 Commission pursuant to section 994 of title 28.”.

3 (b) TECHNICAL AND CONFORMING AMENDMENT.—
4 The table of sections for chapter 47 of title 18, United
5 States Code, is amended by inserting after the item relat-
6 ing to section 1030 the following:

“Sec. 1030A. Aggravated damage to a critical infrastructure computer.”.

7 **SEC. 105. PREPAREDNESS OF FEDERAL COURTS TO PRO-**
8 **MOTE CYBER SECURITY.**

9 Not later than 180 days after the date of enactment
10 of this Act, the Administrative Office of the United States
11 Courts shall submit to the Committee on the Judiciary
12 of the House of Representatives and the Committee on
13 the Judiciary of the Senate a report providing an assess-
14 ment of the vulnerability of the Federal courts’ computer
15 and network systems to cyber intrusion and attacks that
16 includes recommendations on changes and improvements
17 to the Federal courts’ computer and network security sys-
18 tems to address any deficiencies in computer and network
19 security.

20 **SEC. 106. AUTHORIZATION OF NATIONAL CYBER INVES-**
21 **TIGATIVE JOINT TASK FORCE.**

22 The Attorney General is authorized to establish the
23 National Cyber Investigative Joint Task Force, which
24 shall be charged with coordinating, integrating, and shar-

1 ing information related to all domestic cyber threat inves-
2 tigations.

3 **TITLE II—DATA SECURITY AND**
4 **BREACH NOTIFICATION**

5 **SEC. 201. NOTIFICATION OF INFORMATION SECURITY**
6 **BREACH.**

7 (a) IN GENERAL.—Except as otherwise provided in
8 this section, a covered entity shall notify its customers of
9 a security breach affecting such customers not later than
10 **[14]** days after that security breach.

11 (b) ADDITIONAL NOTIFICATION REQUIREMENTS.—

12 (1) THIRD-PARTY ENTITIES.—In the event of a
13 security breach of a system maintained by a third-
14 party entity, such third-party entity shall notify such
15 covered entity of the security breach.

16 (2) SERVICE PROVIDERS.—If a service provider
17 becomes aware of a security breach involving data in
18 electronic form containing personal information that
19 is owned or possessed by a covered entity that con-
20 nects to or uses a system or network provided by the
21 service provider for the purpose of transmitting,
22 routing, or providing intermediate or transient stor-
23 age of such data, such service provider shall notify
24 the covered entity who initiated such connection,

1 transmission, routing, or storage if such covered en-
2 tity can be reasonably identified.

3 (3) COVERED ENTITY NOTIFICATION.—Upon
4 receiving notification from a third-party entity or a
5 service provider under this subsection, a covered en-
6 tity shall provide notification as required under sub-
7 section (a) or subsection (d).

8 (c) DELAY OF NOTIFICATION AUTHORIZED FOR LAW
9 ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

10 (1) LAW ENFORCEMENT.—If a Federal [or
11 State] law enforcement agency determines that the
12 notification required under subsection (a) would im-
13 pede a civil or criminal investigation, such notifica-
14 tion shall be delayed upon the request of the law en-
15 forcement agency for any period which the law en-
16 forcement agency determines is reasonably nec-
17 essary. A law enforcement agency may, by a subse-
18 quent request, revoke such delay or extend the pe-
19 riod set forth in the original request made under
20 this subparagraph by a subsequent request if further
21 delay is necessary.

22 (2) NATIONAL SECURITY.—If a Federal na-
23 tional security agency or homeland security agency
24 determines that the notification required under this
25 section would threaten national or homeland secu-

1 rity, such notification may be delayed upon the writ-
2 ten request of the national security agency or home-
3 land security agency for any period which the na-
4 tional security agency or homeland security agency
5 determines is reasonably necessary. A Federal na-
6 tional security agency or homeland security agency
7 may revoke such delay or extend the period set forth
8 in the original request made under this subpara-
9 graph by a subsequent written request if further
10 delay is necessary.

11 (d) MAJOR SECURITY BREACH; NOTICE TO LAW EN-
12 FORCEMENT.—A covered entity shall notify the United
13 States Secret Service or the Federal Bureau of Investiga-
14 tion of the fact that a major security breach has occurred
15 not later than [72 hours] after such major security
16 breach has occurred.

17 (e) CONTENT OF NOTIFICATION.—Regardless of the
18 method by which notification is provided to an individual
19 under subsection (a) with respect to a security breach,
20 such notification, to the extent practicable, shall include—

- 21 (1) the date, estimated date, or estimated date
22 range of the security breach;
- 23 (2) a description of the personal information
24 that was accessed and acquired, or reasonably be-
25 lieved to have been accessed and acquired, by an un-

1 authorized person as a part of the security breach;
2 and

3 (3) information that the individual can use to
4 contact the covered entity to inquire about—

5 (A) the security breach; or

6 (B) the information the covered entity
7 maintained about that individual.

8 (f) TREATMENT OF PERSONS GOVERNED BY OTHER
9 FEDERAL LAW.—A covered entity who is in compliance
10 with any other Federal law that requires such covered en-
11 tity to provide notification to individuals following a secu-
12 rity breach shall be deemed to be in compliance with this
13 section.

14 **SEC. 202. CIVIL REMEDIES.**

15 (a) CIVIL ACTION.—The Attorney General may in a
16 civil action obtain a civil penalty of not more than
17 \$500,000 from any covered entity that engages in conduct
18 constituting a violation.

19 (b) SPECIAL RULE FOR INTENTIONAL VIOLA-
20 TIONS.—If the violation of this title described in sub-
21 section (a) is intentional, the maximum civil penalty is
22 \$1,000,000.

23 (c) NO PRIVATE CAUSE OF ACTION.—Nothing in this
24 title shall be construed to establish a private cause of ac-
25 tion against a person for a violation of this title.

1 **SEC. 203. DEFINITIONS.**

2 In this title:

3 (1) SECURITY BREACH.—The term “security
4 breach” means unauthorized access and acquisition
5 of data in electronic form containing personal infor-
6 mation.

7 (2) COVERED ENTITY.—

8 (A) IN GENERAL.—The term “covered en-
9 tity” means a commercial entity that acquires,
10 maintains, stores, or utilizes personal informa-
11 tion.

12 (B) EXEMPTIONS.—The term “covered en-
13 tity” does not include the following:

14 (i) Financial institutions subject to
15 title V of the Gramm-Leach-Bliley Act (15
16 U.S.C. 6801 et seq.).

17 (ii) An entity covered by the regula-
18 tions issued under section 264(c) of the
19 Health Insurance Portability and Account-
20 ability Act of 1996 (Public Law 104–191)
21 to the extent that such entity is subject to
22 the requirements of such regulations with
23 respect to protected health information.

24 (3) DATA IN ELECTRONIC FORM.—The term
25 “data in electronic form” means any data stored
26 electronically or digitally on any computer system or

1 other database and includes recordable tapes and
2 other mass storage devices.

3 (4) MAJOR SECURITY BREACH.—The term
4 “major security breach” means any security breach
5 involving—

6 (A) means of identification pertaining to
7 10,000 or more individuals is, or is reasonably
8 believed to have been acquired;

9 (B) databases owned by the Federal Gov-
10 ernment; or

11 (C) means of identification of Federal Gov-
12 ernment employees or contractors involved in
13 national security matters or law enforcement.

14 (5) MEANS OF IDENTIFICATION.—The term
15 “means of identification” has the meaning given
16 that term in section 1028 of title 18, United States
17 Code.

18 (6) PERSONAL INFORMATION.—

19 (A) IN GENERAL.—The term “personal in-
20 formation” means an individual’s first name or
21 first initial and last name in combination with
22 any one or more of the following data elements
23 for that individual:

24 (i) Social Security number.

1 (ii) Driver's license number, passport
2 number, military identification number, or
3 other similar number issued on a govern-
4 ment document used to verify identity.

5 (iii) Financial account number, or
6 credit or debit card number, and any re-
7 quired security code, access code, or pass-
8 word that is necessary to permit access to
9 an individual's financial account.

10 (B) EXEMPTIONS FROM PERSONAL INFOR-
11 MATION.—

12 (i) PUBLIC RECORD INFORMATION.—
13 Personal information does not include in-
14 formation obtained about an individual
15 which has been lawfully made publicly
16 available by a Federal, State, or local gov-
17 ernment entity or widely distributed by
18 media.

19 (ii) ENCRYPTED, REDACTED, OR SE-
20 CURED DATA.—Personal information does
21 not include information that is encrypted,
22 redacted, or secured by any other method
23 or technology that renders the data ele-
24 ments unusable.

1 (7) SERVICE PROVIDER.—The term “service
2 provider” means an entity that provides electronic
3 data transmission, routing, intermediate, and tran-
4 sient storage, or connections to its system or net-
5 work, where such entity providing such services does
6 not select or modify the content of the electronic
7 data, is not the sender or the intended recipient of
8 the data, and does not differentiate personal infor-
9 mation from other information that such entity
10 transmits, routes, stores, or for which such entity
11 provides connections. Any such entity shall be treat-
12 ed as a service provider under this title only to the
13 extent that it is engaged in the provision of such
14 transmission, routing, intermediate and transient
15 storage, or connections.

16 (8) THIRD-PARTY ENTITY.—The term “third-
17 party entity” means an entity that has been con-
18 tracted to maintain, store, or process data in elec-
19 tronic form containing personal information on be-
20 half of a covered entity who owns or possesses such
21 data.

22 **SEC. 204. EFFECT ON FEDERAL AND STATE LAW.**

23 The provisions of this title shall supersede any provi-
24 sion of the law of any State, or a political subdivision

- 1 thereof, relating to notification by a covered entity of a
- 2 security breach.

H.R. _____
Judiciary Cyber-Security Draft – March 2013
Section-by-Section

Section 1. Short Title. This section cites the short title of the bill as the “_____ Act of 2013.”

TITLE I -- CRIMINAL PROVISIONS

Section 101. Protecting U.S. Businesses from Foreign Espionage. This section increases the statutory maximum for violations of section 1831(a) of title 18 from 15 to 20 years for economic espionage offenses.

Section 102. Fraud and Related Activity in Connection with Computers as RICO Predicate. This section adds section 1030 computer crimes to the list of predicate offenses in section 1961 of title 18 for purposes of the Racketeer Influenced and Corrupt Organizations (RICO) statute.

Section 103. Fraud and Related Activity in Connection with Computers. This section makes a series of changes to section 1030 of title 18.

Paragraph (1) of Section 103 amends paragraph (6) of subsection (a) dealing with trafficking in passwords to expand the prohibition to include trafficking in other means of access into a protected computer, which could include fingerprint or biometric technologies.

Paragraph (2) of Section 103 of the bill clarifies that an attempt or conspiracy to violate section 1030 is punishable to the same extent as a completed offense. Subsection (b) of section 1030 already prohibits attempts or conspiracies to violate the Computer Fraud and Abuse Act.

Paragraph (3) of Section 103 streamlines and revises the penalties under subsection (c) of section 1030.

Paragraph (4) of Section 103 revises paragraph (2) of subsection (a) of section 1030. It maintains the current prohibition against intentionally accessing a computer without authorization and thereby obtaining certain financial information, information from a federal agency or department, or information from a protected computer. Paragraph (4) narrows the prohibition against obtaining information from a computer by “exceeding authorized access” by not only requiring that the individual obtain certain financial information, information from a federal agency or department, or information from a protected computer, but also by requiring that the offense involve (1) information that exceeds \$5,000 in value, (2) the offense was committed for the purpose of obtaining sensitive or non-public information, (3) the offense was committed in furtherance of certain criminal acts, or (4) the offense involves information obtained from a computer used by or for a government entity.

Paragraph (5) of Section 103 amends the existing forfeiture provisions of section 1030 to allow for the forfeiture of real property used or intended to be used to commit or facilitate an offense and to clarify that the gross proceeds obtained as a result of the offense are eligible for forfeiture.

Paragraph (6) of Section 103 amends the definition of “exceeds authorized access” to clarify that a person is considered to have exceeded such access if they have permission to access certain information but do so for an impermissible purpose.

Section 104. Damage to Critical Infrastructure Computers. This section creates a new section 1030A in title 18 to penalize those who cause damage or attempt to cause damage to a critical infrastructure computer, imposing a maximum 30 year sentence. A person convicted of a violation of section 1030A is ineligible for probation and a sentence under this section must run consecutively to sentences for violations of other criminal laws, except that multiple convictions for violations of 1030A sentenced at the same time may be sentenced concurrently.

Section 105. Preparedness of Federal Courts to Promote Cyber Security. This section directs the Administrative Office of the Courts to submit to the House and Senate Judiciary Committees within 180 days of enactment a report on the ability of the federal judiciary to protect its computers and networks from cyber intrusions.

Section 106. Authorization of National Cyber Investigative Joint Task Force. This section authorizes the FBI-led National Cyber Investigative Joint Task Force. The NCIJTF is the focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force, which includes 19 intelligence agencies and law enforcement, working side by side to identify key players and schemes. Its goal is to predict and prevent what’s on the horizon and to pursue the enterprises behind cyber attacks.

TITLE II – DATA SECURITY AND BREACH NOTIFICATION

Section 201. Notification of Information Security Breach. This section requires commercial entities that acquire, maintain, store, or utilize personal information to report a security breach to its customers within [14 days]. This section also requires certain third-party entities and service providers to notify a covered entity of a breach. The covered entity must then, in turn, notify its customers.

This section authorizes a delay in notification to customers affected by a breach for law enforcement or national security purposes. In the case of a major security breach, a covered entity must also notify the FBI or Secret Service of such breach within [72 hours].

This section describes the content of breach notifications to customers. A covered entity that complies with the notification requirements of any other federal law is deemed to be in compliance with this section.

Section 202. Civil Remedies. This section establishes civil fines, enforceable by the Justice Department, against a covered entity that fails to comply with the notification requirements of

Section 201, with a base fine of \$500,000, increasing to \$1,000,000 for intentional violations. The section does not provide for a private right of action.

Section 203. Definitions. This section provides definitions for terms for this section, including “covered entity,” “data in electronic form,” “major security breach,” “means of identification,” “personal information,” “service provider,” and “third-party entity.”

Section 204. Effect on Other Laws. This section instructs that the data breach notification requirement established in this title supersedes state or local data breach notification laws.

[Get Email Updates](#) | [Contact Us](#)[Home](#) • [Briefing Room](#) • [Presidential Actions](#) • [Executive Orders](#)The White House
Office of the Press Secretary

For Immediate Release

February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

Search WhiteHouse.gov

Search



BLOG POSTS ON THIS ISSUE

April 01, 2013 1:00 PM EDT

From the Archives: Play Ball, Mr. President!
In honor of the new baseball season the National Archives put together a collection of baseball photos from 13 Presidential Libraries reflecting upon America's favorite pastime.

April 01, 2013 10:00 AM EDT

A Special Message From the President
The White House releases a special video message from the President, available only at WhiteHouse.gov.

April 01, 2013 7:40 AM EDT

Watch Live and Follow Online: The 2013 Easter Egg Roll

Don't miss a minute of the fun -- check out all the action live from the South Lawn of the White House where this year's theme is "Be Healthy, Be Active, Be You!"

[VIEW ALL RELATED BLOG POSTS](#)[Facebook](#)[YouTube](#)[Twitter](#)[Vimeo](#)[Flickr](#)[iTunes](#)[Google+](#)[LinkedIn](#)

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and

technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and

coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

WWW.WHITEHOUSE.GOV

En español | Accessibility | Copyright Information | Privacy Policy | Contact
USA.gov | Developers | Apply for a Job



[Home](#) [About Us](#) [Hearings & Markups](#) [Latest News](#) [Issues & Views](#)

Press Releases

**Statement of Judiciary Committee Chairman Bob Goodlatte
Subcommittee on Crime, Terrorism, Homeland Security, and
Investigations Hearing on "Investigating and Prosecuting 21st Century
Cyber Threats" As Prepared/Statement Submitted for the Record**

For Immediate Release
March 13, 2013

Contact: Kathryn Rexrode or Jessica Baker, (202) 225-3951

**Statement of Judiciary Committee Chairman Bob Goodlatte
Subcommittee on Crime, Terrorism, Homeland Security, and Investigations
Hearing on "Investigating and Prosecuting 21st Century Cyber Threats"
As Prepared/Statement Submitted for the Record**

Chairman Goodlatte: The 21st century has brought us a more connected, inter-dependent world. The Internet and portable computer systems make it possible for people, businesses and governments to interact on a global level never seen before.

The United States, with its bounty of personal freedom and free enterprise, is a leader in advancing the technology that enables us to stay in touch almost everywhere with almost everyone.

However, our technological advancement also makes the United States increasingly vulnerable to cyber attacks – from routine cyber crimes to nation-state espionage. Earlier this week, we all heard about the high profile cyber breach that exposed sensitive personal and financial information about high-ranking government officials and celebrities from FBI Director Mueller and Attorney General Holder to Beyonce and Donald Trump. The truth is that all citizens are vulnerable to these kinds of cyber attacks.

We are also currently experiencing a profound cyber-spying conflict on the nation-state level. Most Americans are familiar with the Wikileaks case, which resulted in the public disclosure of hundreds of thousands of secret State Department cables. And many of us are familiar with the cyber attack on the Chamber of Commerce, in which Chinese hackers gained access to the files on the Chamber's 3 million member companies.

But these cyber intrusions are just the tip of the iceberg. In November, 2011, the National Counterintelligence Executive, the agency responsible for countering foreign spying on the U.S. government, issued a report that hackers and illicit programmers in China and Russia are pursuing American technology and industrial secrets, jeopardizing an estimated \$398 billion in U.S. research spending. According to the report, "China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of U.S. economic information and technology." The report drew on 2009-2011 data from at least 13 agencies, including the Central Intelligence Agency and the Federal Bureau of Investigation.

And in January of this year, the New York Times reported it has been the victim of a sustained cyber attack by Chinese hackers. Shortly afterward, the Wall Street Journal and the Washington Post also reported they too had been breached by similar sources. The Times commissioned a report from Mandiant, a private investigative agency, which traced the cyber attacks to a unit of the Chinese People's Liberation Army. According to the report, the Chinese are engaged in massive cyber spying on the American industrial base and in areas the Chinese are trying to develop for their own national purposes.

Just yesterday, for the first time in his annual presentation to Congress, National Intelligence Director James Clapper spoke about cyber-attacks first in his list of possible threats. Although Clapper told the Senate Intelligence Committee he only saw a "remote chance" of a major cyberattack in the next two years, he warned that such an attack could "cripple America's infrastructure and economy," and was a more immediate and pressing threat to the United States than a major terrorist attack.

Earlier this year, the Administration issued a cyber security Executive Order and Presidential Directive aimed at helping secure America's cyber networks. The Executive Order is a first step towards protecting our public and private networks from attack. But Congress can and must do more. The Judiciary Committee is responsible for ensuring that our federal criminal laws keep pace with the ever-evolving cyber landscape.

Our challenge is to create a legal structure that protects the invaluable government and

private information that hackers seek to exploit, while allowing the freedom of thought and expression that made this country great. One thing is clear: cyber attacks can have devastating consequences for citizens, private industry and America's national security and should be treated just as seriously as more traditional crimes by our criminal justice system.

The risks to our national infrastructure, our national wealth, and our citizens are profound, and we must protect them. We must not allow cyber crime to continue to grow and threaten our economy, safety and prosperity.



[LATEST NEWS](#) | [SCHEDULE](#) | [ABOUT THE COMMITTEE](#) | [CONTACT](#) | [ISSUES & VIEWS](#) | [SEARCH](#) | [MINORITY WEB SITE](#)

US House of Representatives Committee on the Judiciary
2138 Rayburn House Office Building Washington, DC 20515 p/202.225.3951

United States Senate

WASHINGTON, DC 20510-4305

January 18, 2013

The Honorable Eric Holder
Attorney General
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Attorney General Holder:

Like many Americans, I was saddened to learn last week of the death of Aaron Swartz. Mr. Swartz was, among other things, a brilliant technologist and a committed activist for the causes in which he believed – including, notably, the freedom of information. His death, at the young age of twenty-six, was tragic.

As you are doubtless aware, Mr. Swartz was facing an aggressive prosecution by the Department of Justice when he took his own life. The U.S. Attorney's Office for the District of Massachusetts accused him of breaking into the computer networks of the Massachusetts Institute of Technology and downloading without authorization thousands of academic articles from a subscription service. While the subscription service did not support a prosecution, in July 2011 the U.S. Attorney's office indicted him on four counts of fraud and computer crimes, charges that reportedly could have resulted in up to 35 years imprisonment and a \$1 million dollar fine. This past September, the U.S. Attorney's office filed a superseding indictment charging Mr. Swartz with thirteen felony counts and the prospect of even longer imprisonment and greater fines.

Mr. Swartz's case raises important questions about prosecutorial conduct:

First, on what basis did the U.S. Attorney for the District of Massachusetts conclude that her office's conduct was "appropriate?" Did that office, or any office within the Department, conduct a review? If so, please identify that review and supply its contents.

Second, was the prosecution of Mr. Swartz in any way retaliation for his exercise of his rights as a citizen under the Freedom of Information Act? If so, I recommend that you refer the matter immediately to the Inspector General.

Third, what role, if any, did the Department's prior investigations of Mr. Swartz play in the decision of with which crimes to charge him? Please explain the basis for your answer.

Fourth, why did the U.S. Attorney's office file the superseding indictment?

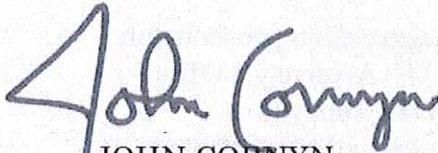
Fifth, when the U.S. Attorney's office drafted the indictment and the superseding indictment, what consideration was given to whether the counts charged and the associated penalties were proportional to Mr. Swartz's alleged conduct and its impact upon victims?

Sixth, was it the intention of the U.S. Attorney and/or her subordinates to "make an example" of Mr. Swartz? Please explain.

Finally, the U.S. Attorney has blamed the "severe punishments authorized by Congress" for the apparent harshness of the charges Mr. Swartz faced. Does the Department of Justice give U.S. Attorneys discretion to charge defendants (or not charge them) with crimes consistent with their view of the gravity of the wrongdoing in a specific case?

I appreciate your prompt and thorough answers to these questions.

Sincerely,

A handwritten signature in blue ink that reads "John Cornyn". The signature is written in a cursive, flowing style.

JOHN CORNYN

United States Senator

March 12, 2013

Chairman Jim Sensenbrenner
House Subcommittee on Crime, Terrorism, and Homeland Security
Rayburn House Office Building B-370B
Washington, DC 20515

Ranking Member Bobby Scott
House Subcommittee on Crime, Terrorism, and Homeland Security
Rayburn House Office Building B-351
Washington, DC 20515

Dear Subcommittee Chairmen Sensenbrenner, Ranking Member Scott, and Members of the Committee,

We, a wide array of Internet innovators, write to support efforts led by Representative Lofgren to reform the Computer Fraud and Abuse Act. This issue is important to us not just because of the tragic death of Aaron Swartz, but because the CFAA chills innovation and economic growth by threatening developers and entrepreneurs who create groundbreaking technology.

We strongly believe in protecting our users' data from unauthorized access. We recognize that computer criminals and cyber-spies pose a serious threat to American companies, their property, and our national security. It is therefore crucial that federal laws deter and punish those who would maliciously attack U.S. computers and networks. But deterring digital criminals can be done without criminalizing harmless contractual breaches and imposing felony liability on developers of innovative technologies. In the nearly three decades since the CFAA's enactment, the law has lost its way.

This is primarily because the CFAA makes it illegal—a felony, potentially—to “obtain information” from virtually any computer “without” or “in excess of” authorization, but fails to explain what that means. Several prosecutors and courts have interpreted this vague language to render mere breaches of contractual agreements or policies, like website's terms of service, or legal duties, like those between employer and employee, a violation of the CFAA.¹ And at least one other court has found that taking minimal technological steps taken to ensure interoperability of web sites violates the CFAA.²

These interpretations of the CFAA give incumbent companies a dangerous and unfair weapon to wield against competitors and developers of innovations that build on existing services. And

¹ See, e.g., *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (holding that breach of an employment-related confidentiality agreement exceeded authorized access under the CFAA); *United States v. Rodriguez*, 628 F.3d 1258, 1260-65 (11th Cir. 2010) (holding that defendant had exceeded authorized access under the CFAA when he accessed information in a Social Security Administration database in violation of SSA employee policy); *United States v. Drew*, 259 F.R.D. 449, 452-53, 467 (C.D. Cal. 2009) (rejecting prosecution argument that a defendant who violated a website's terms of service exceeded authorized access under the CFAA).

² <https://www.eff.org/cases/facebook-v-power-ventures>.

because the statute contains criminal penalties as well as civil remedies, prosecutors have the discretion to bring the full weight of harsh criminal penalties against innovators, too.

Some examples of where the CFAA has been, or could be, used to thwart innovation include:

- A large social networking company sued the creators of a tool that let users view, manage, and use multiple social networks on one screen, claiming the tools violated the CFAA and a similar California computer crime law. The tool allowed users to exchange private messages with any of their social networking friends through a single interface of their choice, rather than having to separately check their messages on Gmail, Twitter, and Facebook.³
- A major website used the CFAA to sue developers of a tool that let users automatically place apartment ads from numerous classified ad websites onto a mapping website and added content such as the price range for apartments in that area.⁴
- The CFAA threatens tools that help mobile users automatically fill out forms and otherwise interact with websites without having to type out their information on a tiny keyboard, when a website prevents this automated access either through terms of service or technically blocking the service. This threat can especially hurt the millions of Americans who have only mobile devices yet increasingly must use the Internet to seek employment and services.

Of course, the greatest loss for consumers may be unseen: the innovations that quietly died when their creators were threatened with CFAA claims by more established competitors, or innovations that never emerged because developers or investors feared potential CFAA liability. Nothing chills ingenuity like the shadow of felony charges for tools that harm no one.

Other existing laws recognize the importance of permitting reverse-engineering and interoperability. For instance, U.S. copyright law has long considered the copying of computer code necessary to build an interoperable computer program to be fair use. This change arose out of attempts by companies like Sony and Sega to stop competitors from building interoperable games and consoles.⁵ Similarly, the Digital Millennium Copyright Act's anti-circumvention provisions contain a specific exception that allows reverse engineering to achieve interoperability even if it circumvents a technological protection measure protecting a copyrighted work.⁶ The DMCA is not perfect, but this exception reflects Congress's recognition that technological barriers can be misused as anticompetitive barriers to entry by incumbents threatened by innovative ideas.

Many of today's best-known innovators—from Steve Jobs and Steve Wozniak to Paul Allen and Bill Gates to Mark Zuckerberg—could have likely been prosecuted under overly broad computer

³ <https://www.eff.org/cases/facebook-v-power-ventures>. The case was civil, not criminal, but the CFAA ties the two together so that, had a prosecutor wished to do so, he could bring a criminal case for the same activity.

⁴ <http://gigaom.com/2012/07/24/craigslist-sues-competitor-padmapper-over-listings/>

⁵ See *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).

⁶ 17 U.S.C. § 1201(f).

crime laws like the CFAA when they were young, simply for doing what innovators do: pushing boundaries.⁷ The point is not that everything they might have done should necessarily be legal, but that stepping over the line should not trigger the draconian penalties that the CFAA currently carries. We therefore urge Congress to amend the CFAA to ensure it does not chill the development of innovative and interoperable software and services. We believe that this should be accomplished by:

- 1) ensuring that violation of terms of service, contractual agreements or other legal duties do not violate the statute;
- 2) protecting technical steps necessary for interoperability and innovative means of access and;
- 3) fixing the statute's penalty scheme so that the punishment better fits the crime, including making sure that prosecutors can't double-charge for the same conduct and ensuring that felony punishments only apply to most egregious behavior.

Sincerely,

Internet Infrastructure Coalition (i2Coalition)

Engine Advocacy

O'Reilly Media

Reddit

OpenDNS

Stack Exchange

PadMapper

heyzap

Agile Learning Labs

Vuze

#sfbeta

ZeroCater

Vidmaker

4Chan and Canvas

Notcot Inc.

The Lewis Charitable Foundation

Get Satisfaction

VigLink

Zemamai

American Library Association

cc: Members of the House Committee on the Judiciary

⁷ Jobs and Wozniak: <http://www.kottke.org/10/09/woz-and-jobs-phone-phreaks>; Allen and Gates: <http://www.v3.co.uk/v3-uk/news/2044825/paul-allen-spills-beans-gates-criminal-past>; Zuckerberg: <http://www.businessinsider.com/how-mark-zuckerberg-hacked-into-the-harvard-crimson-2010-3>; generally: <http://www.newyorker.com/online/blogs/newsdesk/2013/01/everyone-interesting-is-a-felon.html>.

House Judiciary Committee New Draft Bill on Cybersecurity is Mostly DOJ's Proposed Language from 2011

<http://www.volokh.com/2013/03/25/house-judiciary-committee-new-draft-bill-on-cybersecurity-is-mostly-doj-proposed-language-from-2011/>

April 1, 2013

Orin Kerr

The Hill reports that [a draft of language](#) to reform the CFAA is being circulated among House Judiciary Committee members for feedback:

A draft cybersecurity bill circulating among House Judiciary Committee members would stiffen a computer hacking law used to bring charges against Internet activist Aaron Swartz. □□ The bill draft would tighten penalties for cyber crimes and establish a standard for when companies would have to notify consumers that their personal data has been hacked, according to a copy obtained by The Hill.

It would also change existing law so that an attempt at a cyber crime can be punished as harshly as an actual offense. Such measures could spark concern among advocates outraged over the death of Swartz, the 26-year-old Internet activist and computer programmer who killed himself earlier this year while facing a possible 35-year prison term for hacking. Advocates have called on Congress to make changes to what they say is a draconian law that led to too harsh a prosecution of Swartz.

... It's unclear which Judiciary members are sponsoring the draft bill, which is unnamed. A House Judiciary Committee aide said the bill is still in the early drafting stage and is being circulated to stakeholders for their feedback on possible changes.

They're looking for feedback, so here is mine: Stop taking DOJ's language from back in 2011 and packaging it as something new. Based on a quick read, it seems that the amendments for 1030 in [the new draft](#) are mostly copied from a bill that Senator Leahy offered (with substantial input from DOJ, as I understand it) back in November 2011. I criticized that language [here](#). The new circulating draft also adopts the sentencing enhancements (minus mandatories) and the proposed 1030a that DOJ advocated in May 2011. I criticized that initial DOJ language [here](#). (There's also a breach notification provision in the new language, but I haven't followed that issue closely; I don't know if that proposal is also based on old language.)

In some ways, the new circulating language is even more severe and harsh than DOJ wanted even in the Lori Drew case. For example, the proposed language would make it a felony crime to violate Terms of Service if the TOS violation:

(I) involves information that exceeds \$5,000 in value; (II) was committed for purposes of obtaining sensitive or non-public information of an entity or another individual (including such information in the possession of a third party), including medical records, wills, diaries, private correspondence, financial records, photographs of a sensitive or private nature, trade secrets, or sensitive or non-public commercial business information; (III) was committed in furtherance of any criminal act in violation United States or of any State, unless such state violation would be based solely on

the obtaining of information without authorization or in excess of authorization; or (IV) involves information obtained from a computer used by or for a government entity;

This language is really, really broad. If I read it correctly, the language would make it a felony to lie about your age on an online dating profile if you intended to contact someone online and ask them personal questions. It would make it a felony crime for anyone to violate the TOS on a government website. It would also make it a federal felony crime to violate TOS in the course of committing a very minor state misdemeanor. If there is a genuine argument for federal felony liability in these circumstances, I hope readers will enlighten me: I cannot understand what they are.

In short, this is a step backward, not a step forward. This is a proposal to give DOJ what it wants, not to amend the CFAA in a way that would narrow it.

Or at least that's how it seems to me based on a quick read. If I am misreading something, which is always possible when in a hurry, I hope readers will point that out in the comment thread; I'll be offline for a few hours for Passover but I'll plan on posting updates/corrections later tonight if necessary.

[OUR MISSION](#) [THE TEAM](#) [CAMPAIGNS](#) [BLOG](#) [DONATE](#)





If you're already on **Facebook**, [click here to share with your friends.](#)



If you're already on **Twitter**, [click here to tweet about the campaign:](#)

Paid for by Demand Progress (DemandProgress.org) and not authorized by any candidate or candidate's committee.
Contributions to Demand Progress are not deductible as charitable contributions for federal income tax purposes.

[Privacy Policy](#) [Contact Us](#) [Join Our Press List](#) [Home](#)



SEARCH

Computer Fraud And Abuse Act Reform

[Donate to EFF](#)

Stay in Touch

[SIGN UP NOW](#)

Follow EFF

Wow, there is lots of big news from @EFF today. Some of it is literally unbelievable:
<https://eff.org/r.1bNy>

APR 1 @ 10:29AM

Come see @EFF at next week's National Conference for Media Reform in Denver, hosted by @freepress
<https://eff.org/r.b6Nw>

MAR 29 @ 2:34PM

Victory for open source and common sense: Texas court confirms you can't patent math <https://eff.org/r.3bNv>

MAR 29 @ 12:06PM

[Twitter](#)

[Facebook](#)

[Identi.ca](#)

Projects

[Bloggers' Rights](#)

[Coders' Rights](#)

[Follow EFF](#)

[Free Speech Weak Links](#)

[Global Chokepoints](#)

[HTTPS Everywhere](#)

[Open Wireless Movement](#)

[Patent Busting](#)

[Surveillance Self-Defense](#)

- [Introduction Blog Post](#)
- [Proposal Language](#)
- [Explanation of Proposal](#)
- [Chart of Penalties Reform After Proposed Language](#)

[Takedown Hall of Shame](#)

[Teaching Copyright](#)

[Transparency Project](#)

[Ways To Help](#)

[BLOG POSTS](#) [PRESS RELEASES](#) [IN THE NEWS](#) [DOCUMENTS](#) [CASES](#)

MARCH 21, 2013

[Secret Service Reopens Aaron Swartz Freedom of Information Act Requests](#)

MARCH 14, 2013

[The Matthew Keys Case, the CFAA, and Why Maximum Sentences Matter](#)

MARCH 12, 2013

[Startups and Innovators Send Letter to Congress Demanding CFAA Reform](#)

MARCH 7, 2013

[Senate Demands Answers About Aaron Swartz, But More Must Be Done](#)

MARCH 7, 2013

[Reform the CFAA: Don't Let It Stop The Next Steve Jobs, Bill Gates, Mark Zuckerberg, or Steve Wozniak](#)

FEBRUARY 8, 2013

[Rebooting Computer Crime Part 3: The Punishment Should Fit the Crime](#)

FEBRUARY 4, 2013

[Rebooting Computer Crime Law Part 2: Protect Tinkerers, Security Researchers, Innovators, and Privacy Seekers](#)

FEBRUARY 4, 2013

[Rebooting Computer Crime Law Part 1: No Prison Time For Violating Terms of Service](#)

FEBRUARY 1, 2013

[Aaron's Law 2.0: Major Steps Forward, More Work to Be Done](#)

JANUARY 29, 2013

[Critical Fixes for the Computer Fraud and Abuse Act](#)

JANUARY 22, 2013

[アロン・シュワルツの死でみんな目が覚めた、コンピューター犯罪者に適用される厳しい法律を見直そう!](#)

JANUARY 17, 2013

[EFF's Initial Improvements to Aaron's Law for Computer Crime Reform](#)

JANUARY 14, 2013

[In the Wake of Aaron Swartz's Death, Let's Fix Draconian Computer Crime Law](#)



[Thanks](#) | [RSS Feeds](#) | [Copyright Policy](#) | [Privacy Policy](#) | [Contact EFF](#)

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. [Find out more here](#)

theguardian

Printing sponsored by:

Kodak
All-in-One Printers

DANGILLMOR
ON DIGITAL BEING

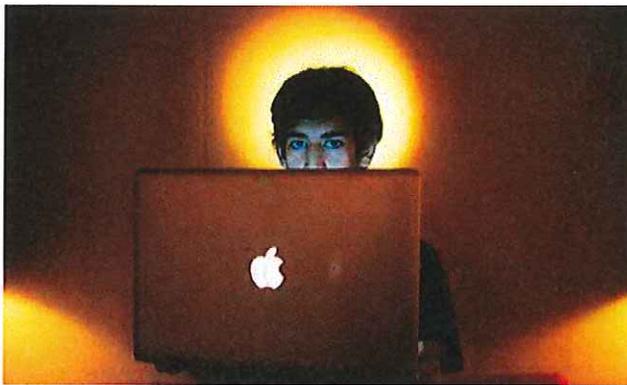


Is the Computer Fraud and Abuse Act the 'worst law in technology'?

It is bad – enabling federal prosecutors' harassment of Aaron Swartz. But America's copyright regime is an even greater threat



Dan Gillmor
guardian.co.uk, Wednesday 20 March 2013 11.17 EDT



California Democrat Zoe Lofgren has proposed 'Aaron's law', named after the late internet activist Aaron Swartz (pictured), to reform the CFAA. Photograph: Michael Francis Mcelroy/AP

Is the Computer Fraud and Abuse Act the "worst law in technology", as [Columbia Law School's Tim Wu](#) calls the statute? I think there are worse laws for the technology industry and its customers, but the CFAA is more than bad enough – a vague, outdated and Draconian law, abused by the government in several high-profile cases – to have spurred calls for repeal.

As Wu and many others (including me) have pointed out over the years, the [vagueness of the CFAA](#) has given prosecutors a tool that should worry everyone. This is because the government contends that the statute's ban on "unauthorized access" to someone else's computer is a felony, period, with potential penalties you'd associate with serious violent crime.

The late [Aaron Swartz](#) has been the highest-profile target of overreaching federal prosecutors relying in large part on the CFAA, in a case where he downloaded hundreds of thousands of academic papers from an organization that didn't want him prosecuted and ultimately decided to make the material freely available. There's little question that

his suicide was spurred, in part, by the government's escalating threats, made possible thanks to prosecutors' ability to use the CFAA as sledgehammer.

But he wasn't the first. The Bush administration relied on the CFAA to prosecute the easy-to-dislike Lori Drew, who was among several people who created a bogus MySpace account of a fictitious teenaged boy who wooed and rejected the daughter of Drew's neighbor in suburban St Louis. The girl killed herself. When Missouri prosecutors said they had no relevant state law to prosecute Drew and her admittedly heartless helpers in this scheme, a federal prosecutor in Los Angeles hauled Drew there to face charges under the CFAA.

The case boiled down to Drew's misstatements in her MySpace profile. (Shamefully, MySpace supported the prosecution.) The jury convicted Drew of one charge, but the judge in the case wisely overturned it, pointing out that the government would have made everyone who's ever violated a "terms of service" agreement, no matter how minor the violation, at risk for criminal charges.

The threat of this law is not just from government prosecution. It's been stretched widely in civil cases, as well. Wu says the way to fix this intolerable situation is to persuade President Obama to fix it:

"The Computer Fraud and Abuse Act is egregiously over-broad in a way that has clearly imposed on the rights and liberties of Americans. With just one speech, the president can set things right."

But no, he can't. At least, not in a way we could trust.

First, presidential dispensation is useful, but it's not remotely permanent. White House occupants change. A more authoritarian chief executive than Obama won't be bound by what he does.

Presidents also change, or their positions do. That's the second big problem with Wu's suggestion: wishful thinking. Obama's record on civil liberties and executive power is simply abysmal – worse than George W Bush's in many ways, and better in only a few (such as gay rights).

Obama's Justice Department has made clear it believes the CFAA gives it the power to go after anyone. That includes you and me, assuming you've ever violated a terms of service in any way, as you undoubtedly have done.

Banana republics have lots of laws designed to be widely broken, providing leverage for prosecution of people either not liked by the government or who do otherwise legal things that annoy the leaders. So, even though you and I are exceedingly unlikely to become targets of the CFAA, we *could be* – and that's why the law is intolerable as it stands.

Wu doubts, fairly, that this Congress in particular can be persuaded to act on almost anything. And it's no exaggeration to say that lawmakers are terrified in general of doing anything that might cause them to be accused of being soft on crime. But like it or not, this is ultimately an issue for Congress, which writes the laws.

The lawmakers' tendency to favor vagueness has some merit – it gives the people who carry out enforcement and make regulations the ability to adjust to changing circumstances – but in cases like this, where the abuse by the executive branch is blatant, Congress should take the risk of doing its job.

Representative Zoe Lofgren, a California Democrat, has proposed an "Aaron's Law" that would help redress the current imbalance.

Reforming CFAA is also an issue for the press – or would be, if we had more journalists who took seriously their duty to hold power accountable. Journalists in aggregate have

two problems with this law: a superficial understanding, at best, and an ongoing deference to government positions on criminal justice and security. Even when journalists are directly threatened by overreaching, as they are in the WikiLeaks case, they still demonstrate a reluctance to take a stand.

If enough news organizations put the Obama civil liberties record under the spotlight it deserves, perhaps the American people would care more about what they're losing. Or maybe, we're willing to live in a more banana-like republic all the time; but I hope not.

I said earlier that the CFAA, bad as it is, isn't the worst law relating to technology. At least one, by my reckoning, is worse: the increasingly harsh copyright regime that has already turned countless millions of Americans into lawbreakers and deterred countless innovators.

Copyright in America started life in the US constitution as a way to promote innovation by giving creators of works strong rights for limited periods. It has metastasized into a system that has perverts the founders' intent and given giant corporations overwhelming – and increasing – power over not just entertainment but everything that contains information, including software, which is now part of almost everything.

In a rare defeat for the Copyright Cartel, the [supreme court has upheld the "first sale doctrine"](#) – the principle that once you buy a book or CD, you can resell it – in a closely watched case. The court's rationale was that Congress didn't mean to create a different standard for works bought overseas as opposed to ones bought in the US. But the same court also just refused to hear an appeal of a Minnesota woman who's been ordered to pay more than \$220,000 for downloading two-dozen songs – a testament to Congress' gift to Hollywood and its allies in the form of absurdly stiff penalties for minor infringement.

In the end, people who want change in bad laws have to work for it. This is doubly hard given Congress' pay-to-play system of legal bribery, where dollars translate into votes. Maybe that will have to change first, as [the "United Re:Public" coalition says](#), but we need to get started or get used to a system that puts everyone at risk. We could begin by calling our legislators and insist they get behind "Aaron's Law".

More from the Guardian [What's this?](#)

[Fifty Shades of Grey got us into BDSM – now my wife has gone off it](#) 01 Apr 2013

[Jonathan Creek returns – but what is the detective's appeal?](#) 27 Mar 2013

[Five of the worst movie sex scenes](#) 26 Mar 2013

[Why do I stay with my aggressive, manipulative husband?](#) 31 Mar 2013

[Slash corporate tax rates? Let's start with ending the business breaks](#) 29 Mar 2013

[China 'will appoint next Hong Kong leader regardless of election result'](#) 28 Mar 2013

More from around the [What's this?](#)

web

[10 Great Small Cities for Retirement](#) (AARP)

[7 paradoxes we bet you can't solve](#) (Funnyist)

[The Supreme Court May Make Resale Illegal](#) (Web2Carz)

[If You Want To Be Awesome At Emails, Add Yesware To Your Gmail Today](#) (Forbes.com)

[The 12 Worst Supermarkets in America](#) (The Fiscal Times)

[Law on Locking-Blade Pocket Knives](#) (eHow)

© 2013 Guardian News and Media Limited or its affiliated companies. All rights reserved.

;



Membership Services Jobs Cars Real Estate Subscribe Rentals Weekly Circulars Custom Publishing Place Ad

Los Angeles Times

LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH LIVING TRAVEL OPINION SHOP

EDITORIALS OP-ED LETTERS OPINION L.A. READERS' REP ENDORSEMENTS

YOU ARE HERE: LAT Home → Collections → **Opinion** Editorial

Ads by Google

Outfox the competition.



Stanford University certifies in engineering leadership & management

[LEARN MORE](#)

Advertisement



Save up to **30%***

* vs. Cascade Complete® Pacs on an average cost per load basis

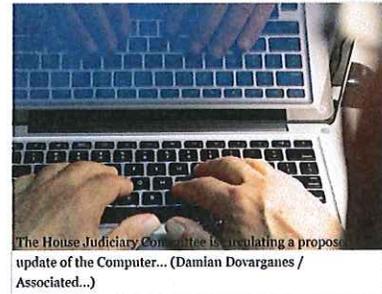
Sunlight

Cyber security run amok

Congress should reconsider a proposed update of the Computer Fraud and Abuse Act.

March 28, 2013 | By The Times editorial board

Congress passed the Computer Fraud and Abuse Act in the early days of the Internet to crack down on malicious hackers, but federal prosecutors have stretched the law since then to apply to computer users who merely violated a website's terms of service. Now, the House Judiciary Committee is circulating a proposed **update** of the act that, instead of fixing its flaws, would enable prosecutors to threaten alleged violators with dramatically bigger penalties. That's a dangerous step that lawmakers shouldn't even consider in light of the well-documented misuses of the law.



The House Judiciary Committee is circulating a proposed update of the Computer... (Damian Dovarganes / Associated...)

Ads by Google

George Mason Cyber Degree

A unique cyber security program, learn more at upcoming info session som.gmu.edu/cyber

2013 Best Skin Tighteners

An Unbiased Review List of The Top Performing Skin Tighteners In 2013 www.SkinCareSearch.com/FaceLifting

RELATED

A federal judge lifts the cone of silence over national security letters

Cellphone unlocking for all, not just for some

White House reiterates its support for cellphone unlocking. Now what?

FROM THE ARCHIVES

Congress' horse-and-buggy computer laws *February 6, 2013*

U.S. House watchdogs want explanation of Aaron Swartz...

January 29, 2013

The pushback against Aaron Swartz misses the point

FOR THE RECORD:

Computer Fraud and Abuse Act: A March 28 editorial about a federal anti-hacking law mentioned a 41-year prison sentence for exposing a security flaw online. The sentence was 41 months.

The 1986 act makes it a crime to gain access to information on a computer in an unauthorized way — for example, by hacking through the passwords protecting a shopping website's server and copying the credit card numbers stored there. That prohibition applies to both people who aren't authorized to use the computer and to people who exceed the authority they were granted.

The problem is that the act doesn't clearly define what it means by exceeding one's authorization. As a result, some prosecutors have argued — and some judges have agreed — that simply violating a site's

January 18, 2013

Aaron Swartz and the law

January 18, 2013

One bit of Aaron Swartz's legacy: Fixing a bad law?

January 16, 2013

MORE STORIES ABOUT

Opinion

Editorials

Not_live_web

Prosecutors

Los Angeles Times Copyright 2013 Los Angeles Times

terms of service is equivalent to gaining unauthorized access. The draft circulated by the Judiciary Committee's staff maintains the sorry status quo, affirming that those who violate terms of service to obtain information from a government website or "sensitive or nonpublic information" from any other site could be prosecuted. As cyber-law expert Orin Kerr observed, "the language would make it a felony to lie about your age on an online dating profile if you intended to contact someone online and ask them personal questions."

A much better idea is the proposal by Rep. Zoe Lofgren (D-San Jose) to narrow the law so that merely violating a site's terms of service to obtain information would not be a crime. Lofgren's proposal is backed by numerous online groups and civil libertarians. The committee's draft, however, reflects the Justice Department's desire for an even bigger hammer to use against online offenders. Among other things, it would enable prosecutors to bring federal racketeering charges against people accused of two or more violations of the 1986 law.

It's easy to understand lawmakers' interest in more powerful tools to combat cyber criminals, who pose an ever-growing threat. But Congress' first step should be to narrow the law to protect people against overzealous prosecutors. When people are being threatened with 35 years in prison for downloading too many articles from an academic database, or sentenced to 41 years for exposing a security flaw that revealed nothing but email addresses, there's something seriously wrong with the law. Congress shouldn't expand the Computer Fraud and Abuse Act in any way until it fixes that problem.

Ads by Google

Powell Law Offices, P.C

Verdicts & Settlements 30 years experience

www.lawinfo.cc

FEATURED



Justices poised to strike down entire healthcare law



Red meat: What makes it unhealthy?



Volcano-induced die-off paved way for dinosaurs, study suggests

MORE:

Are raspberry ketones a 'miracle' fat burner? Dr. Oz weighs in.

How to find your lost or stolen iPhone 5

To Comment on this story, click here



Draft House Judiciary cybersecurity bill would stiffen anti-hacking law

By Jennifer Martinez - 03/25/13 11:02 AM ET

A draft cybersecurity bill circulating among House Judiciary Committee members would stiffen a computer hacking law used to bring charges against Internet activist Aaron Swartz.

The bill draft would tighten penalties for cyber crimes and establish a standard for when companies would have to notify consumers that their personal data has been hacked, according to a copy obtained by The Hill.

It would also change existing law so that an attempt at a cyber crime can be punished as harshly as an actual offense.

Such measures could spark concern among advocates outraged over the death of Swartz, the 26-year-old Internet activist and computer programmer who killed himself earlier this year while facing a possible 35-year prison term for hacking. Advocates have called on Congress to make changes to what they say is a draconian law that led to too harsh a prosecution of Swartz.

Swartz faced a fine of up to \$1 million and up to 35 years in prison for charges that he broke into a university computer network and stole more than four million academic articles from a subscription service. His family believes the charges contributed to Swartz's death.

It's unclear which Judiciary members are sponsoring the draft bill, which is unnamed. A House Judiciary Committee aide said the bill is still in the early drafting stage and is being circulated to stakeholders for their feedback on possible changes.

While the draft proposal increases the maximum sentence a judge can impose for computer crimes, the aide noted that it's still up to a judge to determine the length of a sentence. The aide said the proposed changes in the bill would likely not have changed how a federal judge calculated Swartz's sentence under the federal sentencing guidelines.

Orin Kerr, a law professor at George Washington University, wrote in a blog post that the draft bill is similar to another measure Senate Judiciary Chairman Patrick Leahy (D-Vt.) introduced in Nov. 2011. Kerr was critical of Leahy's bill, arguing that it was written too broadly.

"In short, this is a step backward, not a step forward," [Kerr writes](#) about the new bill draft. "This is a proposal to give [Justice Department] what it wants, not to amend the CFAA in a way that would narrow it."

Momentum for cybersecurity legislation has increased in recent weeks amid alarms from top administration officials about hacker attacks on American companies and key infrastructure. Lawmakers and government officials have raised concern about reports of Chinese hackers siphoning valuable intellectual property and trade secrets from American companies.

Several House committees are teeing up bills that could come to the House floor as early as next month.

Key language in the draft bill would modify the Computer Fraud and Abuse Act to state that an attempt or conspiracy to conduct computer fraud or a related crime "is punishable to the same extent as a completed offense."

It also proposes to amend the law so it would crack down on people who gain unauthorized access to a computer and obtain "sensitive or non-public information of an entity or another individual," including "medical records, wills, diaries, private correspondence ... photographs of a sensitive and private nature, trade secrets, or sensitive or non-public commercial business information."

People would also run afoul of the law if they gain unauthorized access to a computer and the offense involve information that "exceeds \$5,000 in value." Some concerns have been raised about how that threshold has been set and who determines the value of the accessed information.

Additionally, the draft bill would allow authorities to seize "real property used or intended to be used" to commit or facilitate a cyber crime.

The first section of the bill targets foreign economic espionage. It proposes to stiffen the penalties for hackers that steal intellectual property from U.S. companies by raising the statutory maximum punishment for economic espionage offenses to 20 years from 15 years.

The draft bill would also create a new section in the anti-hacking law that is focused on punishing those who attempt to cause damage or inflict damage on a computer that powers critical infrastructure, such as water supply systems or telecommunications networks. It would impose a maximum 30-year sentence; a person convicted of violating that section would be ineligible for probation.

The final section of the draft bill establishes a data breach notification standard, which tells companies when they need to notify consumers about data breaches on their computer systems. The White House has called for a federal data breach notification standard to replace the patchwork of laws used by various states.

The draft bill would require companies that acquire, store or use personal information to report a security breach to its customers within 14 days. That number is bracketed in the bill draft and is therefore subject to change.

If a company suffers a massive data breach, the draft bill would require them to notify the FBI or Secret Service within 72 hours. That number is also bracketed in the draft bill.

Additionally, third parties and service providers would be also required to notify a company about a breach.

This story was last updated at 6:03 p.m.

RECOMMENDED STORIES

[Students demand prayer breakfast critic be pulled from commencement](#)

[Supreme Court takes up Mich. law banning affirmative action](#)

[Sen. Paul: Obama, Bush 'lucky' they weren't arrested for smoking pot as kids](#)

[Lawmakers introduce bill to void 'Redskins' trademark](#)

[Jeb Bush says brother taken to painting dogs 'with a vengeance'](#)

[Limbaugh on gay marriage: 'The issue is lost'](#)

ALSO ON THE WEB

[What Toyota Doesn't Want You to Know About the Prius \(Consumer Car Reviews\)](#)

[Property Tax Rates by State. Find Out Where You Rank. \(DexKnows\)](#)

[NASCAR: Jeff Gordon and Wife Ingrid Open Up About Their Marriage \(E! Online\)](#)

[6 In-Demand Jobs Worth Going back to School For \(Work Reimagined\)](#)

[How Canada Plans to Steal Silicon Valley's Immigrant Entrepreneurs \(BusinessWeek\)](#)

[Plastic Surgery Disasters: Lil Kim, Meg Ryan & More \(Hollyscoop\)](#)

Recommended by

[28 Comments](#)

Source:

<http://thehill.com/blogs/hillicon-valley/technology/290103-draft-cybersecurity-bill-aims-to-stiffen-computer-hacking-law>

The contents of this site are © 2013 Capitol Hill Publishing Corp., a subsidiary of News Communications, Inc.

The logo for Nextgov, featuring the word "Nextgov" in a white, sans-serif font on a black rectangular background.

Anti-Hacking Laws Hamper Private Efforts to Hunt Cybercriminals

By Aliya Sternstein

March 27, 2013

Public-private partnerships can take years to clinch cybercrime cases due to privacy laws, according to one security provider that cooperates with authorities worldwide.

Tokyo-based Trend Micro every day monitors a proprietary stash of statistics on the activity of individuals participating in the "underground economy" of crimeware sales. The database tracks publicly accessible online marketplaces that peddle in, among other things, \$160 malicious software, \$25 private networks for masking identities, and \$100 services that check whether antivirus vendors have discovered the malware yet.

When transactions suggesting a coordinated plot begin to pile up, the company's policy, at least in America, bans mingling with the suspects or penetrating their accounts to investigate further, said Max Goncharov, Trend Micro senior threat researcher.

For example, the vendor in 2007 began picking up the trail of what turned out to be a "botnet" compromising 4 million infected computers that criminals had hijacked remotely to do their bidding -- from spreading additional malware to clicking on paid advertisements. But the FBI did not shutdown the operation until 2011.

"They need us, because there are not enough cyber defenders in the government," Trend Micro Chief Technology Officer Raimund Genes said. "We have well paid experts who have been around for a quite a while and build a reputation -- offering this in a government job is very unlikely."

Under the 1986 Computer Fraud and Abuse Act, it is illegal for private researchers to hack command and control servers, even if they determine those machines have overtaken innocent people's computers.

If Trend Micro uncovers suspicious activity, then it hands over data to the FBI. And then it's up to federal authorities to rebuild the case, Genes explained. Unlike Trend Micro, the feds can infiltrate hacker groups and obtain warrants to access their private accounts. In the botnet case, dubbed Ghost Click, the FBI seized computers and servers. Many Asian countries look the other way when researchers, including experts from Trend Micro, try to hack into the hackers systems, Genes said.

Some civil liberties groups say authorities misuse the 1986 hacking law by arresting computer scientists who find vulnerabilities in systems, and they flout other privacy laws by procuring emails without a warrant.

Earlier this month, the Electronic Frontier Foundation and other Internet activists denounced the sentencing of Andrew "Weev" Auernheimer for informing the media that AT&T had configured its servers to allow the harvesting of iPad owners' unsecured email addresses.

"Weev is facing more than three years in prison because he pointed out that a company failed to protect its users' data, even though his actions didn't harm anyone," EFF Senior Staff Attorney Marcia Hofmann said in a statement. "The punishments for computer crimes are seriously off-kilter, and Congress needs to fix them." The foundation has joined Auernheimer's legal team to appeal the decision.

(Image via [Tatiana Popova/Shutterstock.com](#))

By Aliya Sternstein

March 27, 2013

<http://www.nextgov.com/cybersecurity/2013/03/anti-hacking-laws-hamper-private-efforts-hunt-cybercriminals/62132/>



Lawmakers slam DOJ prosecution of Swartz as 'ridiculous, absurd'

By Brendan Sasso and Jennifer Martinez - 01/15/13 06:52 PM ET

House lawmakers blasted federal prosecutors on Tuesday for pushing aggressive hacking charges against Internet activist Aaron Swartz, who killed himself on Friday.

Rep. Darrell Issa (R-Calif.) says his Oversight panel will look into whether federal prosecutors acted inappropriately.

Meanwhile, two other members of the House Judiciary Committee said prosecutors acted too aggressively.

“The charges were ridiculous and trumped-up,” Rep. Jared Polis (D-Colo.) told The Hill. “It’s absurd that he was made a scapegoat. I would hope that this doesn’t happen to anyone else.”

Polis called Swartz — a co-creator of Reddit who was accused of stealing articles from a computer archive at the Massachusetts Institute of Technology — a “martyr” for why Congress should limit the discretion of prosecutors.

Rep. Zoe Lofgren (D-Calif.) said the government’s handling of the case was “pretty outrageous.”

“Based on what I know, I think the Department of Justice was way out of line on the case,” she told The Hill.

All three lawmakers serve on the House Judiciary Committee, which has jurisdiction over the Justice

Department.

The lawmakers worked with Swartz and his group Demand Progress last year to defeat online piracy legislation backed by the entertainment industry.

In 2011, federal prosecutors accused Swartz of breaking into a computer network at MIT and downloading 4.8 million documents from JSTOR, a subscription service for academic articles.

He faced up to 35 years in prison and a fine of up to \$1 million. His trial was scheduled to begin in April.

In a statement on Saturday, Swartz's family blamed overzealous prosecutors for driving him to take his own life.

"Aaron's death is not simply a personal tragedy. It is the product of a criminal justice system rife with intimidation and prosecutorial overreach," the family said.

Swartz struggled with depression for years, and had discussed as much publicly.

The Justice Department has not commented on the case since Swartz's suicide, citing concern for his family's privacy. But in a statement last year, the DOJ defended bringing charges against Swartz.

"Stealing is stealing whether you use a computer command or a crowbar, and whether you take documents, data or dollars. It is equally harmful to the victim whether you sell what you have stolen or give it away," U.S. Attorney Carmen Ortiz said in a statement when Swartz was charged.

Issa expressed sympathy with some of Swartz's goals. While "cybercrime and hacking has to be taken seriously," he said, Congress should take up Swartz's cause of making more information freely available to the public.

"We're looking at the real question of open government," Issa said. "Has the government or even MIT been holding back materials that the public has a right to know?"

Issa said he wanted to make sure "that what is paid for is as widely available as possible to the American people."

Many materials on JSTOR are funded by public universities or government research grants. Subscriptions to JSTOR cost thousands of dollars.

He also said "whether or not there was excessive prosecution is something we'll look at."

Since Swartz's death, some advocates have called for Congress to re-examine the decades-old Computer Fraud and Abuse Act, arguing that it's written too vaguely and allows for draconian punishments.

Polis said he is willing to consider changes to the law, and urged Attorney General Eric Holder to set guidelines curtailing the ability of prosecutors to seek overly harsh punishments.

"Prosecutors shouldn't have the kind of discretion to seek absurd penalties for minor crimes," Polis said.

Lofgren said she isn't sure whether the Judiciary Committee will update the Computer Fraud and Abuse

Act this year, but she said it is “certainly something I am looking at.”

Source:

<http://thehill.com/blogs/hillicon-valley/technology/277353-lawmakers-blast-trumped-up-doj-prosecution-of-internet-activist>

The contents of this site are © 2013 Capitol Hill Publishing Corp., a subsidiary of News Communications, Inc.

New Posts

Popular

Lists

Video

Try out Forbes magazine for FREE!

Log in | Sign up | Help

COUNTING CARS HE FINDS 'EM, AND FLIPS 'EM. **NEW SEASON PREMIERES APRIL 9 TUESDAYS 9/8c** **CLICK TO EXPAND** **HISTORY**



Jim Zirin, Contributor

I write about law, foreign relations and politics.

OP/ED | 3/29/2013 @ 1:08PM | 1,009 views

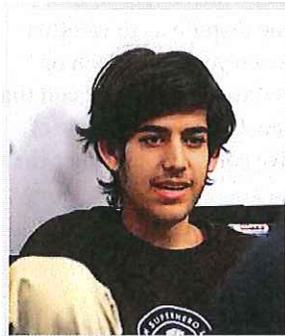
Aaron Swartz' Suicide Forces Hard Questions About The Criminal Justice System

By James D. Zirin

This is the Easter season. Believers say that the holiday is about sacrifice for others and forgiveness for a misguided humanity.

Some two months ago, a 27-year old computer hacker named Aaron Swartz committed suicide rather than face a federal indictment that he thought might send him to jail for a lot of years.

It was a tragic loss of a gifted and talented human life. The case raises tough questions about the criminal justice system.



Aaron Swartz (1986-2013)

An Internet visionary, Swartz was one of the founders and developers of the social media site Reddit. The "crime" was relatively trivial, if it was a crime at all. A research fellow at Harvard, Swartz had a JSTOR account. JSTOR is a "dump" for scholarly articles. Swartz had authorized access to JSTOR's articles. In fact, all visitors to MIT's "open campus" enjoyed authorized access JSTOR through the MIT network.

Swartz downloaded millions of academic articles from JSTOR in violation of its "Terms of Service Agreement" with the intention of making the articles available to all of humanity—not just JSTOR subscribers. You know all about the "Terms of Service Agreement." It's the one everyone clicks his or her agreement to, but nobody reads. In the JSTOR world, this was a no-no. His action is a digital version of someone who has a valid library card, but borrows more books than he should from a public library, the only conceivable distinction being that a hardcover over-borrower denies books to other borrowers. Swartz did not deny anyone anything. What he downloaded remained on the site to be accessed by anyone who wanted a look.

Prosecutors indicted Swartz for violating Section 1030 of the Computer Frauds and Abuse Act, the anti-hacking statute, related to unauthorized accessing of a computer and obtaining information therefrom.



Most Read on Forbes



Jim Zirin

Contributor

Jim Zirin is the host of the critically acclaimed television talk show, "Digital Age," which can be seen weekly throughout the New York metropolitan area. The program has a viewing audience exceeding two million people. Jim is a leading litigator, who has appeared in federal and state courts around the nation. He is a former Assistant United States Attorney for the Southern District of New York, having served in the Criminal Division of that office under the legendary Robert M. Morgenthau. Jim has written over 200 op-ed articles for Forbes, Barron's, the LA Times, the London Times, the Washington Times, the New York Sun and the New York Law Journal. In August 2003, Mayor Michael R. Bloomberg appointed him to the New York City Commission to Combat Police Corruption. He is a member of the Grievance Committee Attorney Panel for the Southern District of New York. He is a Fellow of the American College of Trial Lawyers, the past chair of its International Law Committee and a past chair of its Alternatives for Dispute Resolution Committee; a member of the International Academy of Trial Lawyers; the advisory board of the Woodrow Wilson School of Public and International Affairs of Princeton University; the board of trustees of New York Law School; the executive committee of The Pilgrims of the United States; and the Board of Editors of the

Title 18, §1030 provides [New Posts](#) [Popular](#) [Lists](#) [Video](#)

(a)Whoever—

(2)intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(C)information from any protected computer****[commits a felony].

Called before the Senate Judiciary Committee, Attorney General Eric Holder called the Swartz case “a good use of prosecutorial discretion.” Nonsense. “Prosecutorial discretion” should have been exercised in Swartz’ favor, because Swartz had no prior criminal record, he had access authorization, he harmed no one, either physically or economically, and made not a nickel out of the deal.

For this “crime,” Holder’s Justice Department, which presumably has better things to do, indicted Swartz on 13 felony counts of wire fraud, RICO and violations of the Computer Fraud and Abuse Act, which exposed him theoretically to 50 years in prison. There is some dispute as to whether prosecutors in [Massachusetts](#) offered Swartz seven years in prison or something less if he pleaded guilty. After Swartz’ suicide, Holder said that the US Attorney had offered a three month sentence. It was a clear case of prosecutorial overkill, which Holder should have condemned rather than supported.

Senator John Coryn, Republican of [Texas](#), a member of the Judiciary Committee, questioned Holder sharply:

CORYN: Does it strike you as odd that the government would indict someone for crimes that would carry penalties of up to 35 years in prison and million dollar fines, and then offer him a three or four-month prison sentence? (Swartz was actually facing up to 50 years in prison.)

HOLDER: No.

Senator Coryn pressed the point:

CORYN: So you don’t consider this a case of prosecutorial overreach or misconduct?

HOLDER: No, I don’t look at what necessarily was charged as much as what was offered, in terms of how the case might have been resolved.

New York Law Journal. He is a member of the Council on Foreign Relations. A graduate of Princeton University with honors, he received his law degree from the University of Michigan Law School where he was an editor of the Michigan Law Review and a member of the Order of the Coif. He is listed in “Who’s Who in America.”

The author is a Forbes contributor. The opinions expressed are those of the writer.

JIM ZIRIN’S POPULAR POSTS

[The Stranger Case of Oscar Pistorius](#) 20,558 views

[Why Israel Will Attack Iran](#) 7,243 views

[The Dominique Strauss-Kahn Affair: To Proceed Or Not To Proceed?](#) 4,888 views

[Gay Marriage Cases Will Bring Ideological War Between Chief Justice Roberts and Obama to the Forefront](#) 2,882 views

[Holder v. Congress: Political Firefight or Legal Contempt?](#) 1,650 views

MORE FROM JIM ZIRIN

2ND LOWEST COST OF DOING BUSINESS NATIONALLY.*
*Past 5 years.
IOWA economic development

Who Just Made a Billion Dollars?



Our Real-Time Billionaires scoreboard tracks the biggest holdings for 50 of the world’s wealthiest people.

[See who’s up & who’s down right now »](#)

Opinion

You're Entitled To Our Opinion

› tech policy & law

Tweet 348

69

Share 12

We Need to Think Beyond the Aaron in 'Aaron's Law'

› By Micah Schaffer

› 02.05.13

› 2:05 PM



Photo: Dustball / Flickr

The Computer Fraud and Abuse Act (CFAA)'s disproportionate penalties and lack of nuance played a role in Aaron Swartz' prosecution and likely in his subsequent suicide. So three weeks ago, California Representative Zoe Lofgren introduced "Aaron's Law" to update the CFAA. Lofgren modified Aaron's Law based on community feedback and released the updated version this past Friday. The Electronic Frontier Foundation has also proposed much-needed changes to CFAA's penalty provisions. The law has yet to go before Congress, but these efforts matter. But as we consider further ways to improve the CFAA, it's important to keep in mind the less sympathetic young people who will inevitably violate this law. It's tempting to focus on the CFAA's treatment of hackers who fight political oppression or want to free information, but we can't ignore the less sympathetic cases: the talented, angry, isolated, vulnerable, and often at-risk ones.

These kids — though not all of them are minors — deface websites, wage denial-of-service attacks, and engage in the online equivalents of petty crime. Their transgressions may not be

high-minded or altruistic, but they too are entitled to justice. How do we explain to a young person who hacked their school's website that they might be imprisoned for five years? Yet if they had physically destroyed the web server with a hammer, they would have faced no more than one year. This equation does not reflect the values of our society.

The misalignment of values and law not only leads to unjust prosecutions and unjust penalties, it also fails to create deterrents. Swartz' prosecutors clearly intended to send a message, yet the message being received by the next generation of internet pioneers is that when it comes to technology, *the law is arbitrary*.

Micah Schaffer

Micah Schaffer is a technology policy consultant in San Francisco, California who campaigned as a youth for the balanced treatment of hackers in the public sphere. Schaffer was an early employee of YouTube, where he was responsible for policy creation and enforcement — including working extensively with law enforcement to protect child safety.

As a teenager, I attended one of computer hacker Kevin Mitnick's pre-trial hearings. He was experiencing what would become four and a half years of pre-trial detention, repeatedly waiving his constitutional right to a speedy trial because the prosecution refused to provide access to the evidence (a tactic also employed against Swartz, who had been waiting nearly two years).

If prosecutors were trying to send a message, my friends and I were the exact audience it was intended for. However, we understood the evidence and found the allegations of harm to be absurdly exaggerated. My conclusion at the time was that it didn't actually matter *what* he had done. It wasn't that I thought Mitnick was innocent. (He wasn't.) It was that I — and my peers — recognized he was being denied due process of law.

The lesson we drew was that when it came to technology, the criminal justice system was divorced from reality. Judges appeared to be ignorant and easily manipulated by fear. Actual evidence seemed irrelevant compared to the whims and career ambitions of prosecutors. Despite this budding cynicism, I focused my energy on activism and advocacy rather than delinquency. Because I, like Swartz, had benefited from a stable, comfortable upbringing — with access to mentors and opportunities. I grew up, and I've now had the privilege of working alongside former computer-crime prosecutors in the private sector — all of whom were inspiring, principled colleagues.

Others had a different path.

I was once working for a company that experienced a sudden wave of high-profile user accounts being hacked; the attacker was adding spam links to posts, making money off each click. Although those spam links had garnered less than \$100 at that point, each compromised account was considered a felony violation of the Computer Fraud and Abuse Act.

As part of our investigation into the security breaches, I contacted the company paying for the spam. While pursuing the information they provided, I found numerous other accounts and message board posts from the same person.

One post in particular indicated a deeply unhappy family situation.

The message being received by the next generation of internet pioneers is that when it comes to technology, the law is arbitrary.

We could have reported the crime to the FBI at any time, but we didn't. Instead, I called the attacker on the phone: He turned out to be a very scared child.

He had a small, quivering voice. I identified myself and asked gently, did he know why I was calling? He did. We talked and he confirmed it had been a simple dictionary attack; he had written a script to retry passwords over and over until he found the right one. I was relieved to have confirmation as we had already implemented a fix earlier in the day.

It was surprising no one had done this to us sooner. I told him he was very bright, that many great software engineers had started out like him. But he needed to stay out of trouble if he wanted to grow up and become like them and that other people wouldn't be so tolerant. In exchange for a simple e-mail apology (with a copy of the script he wrote as proof), we considered the matter resolved.

Many such cases don't warrant more than a lecture, but if prosecuted under the CFAA, defendants can face decades in prison and millions of dollars in fines. The threat of such a severe penalty also gives prosecutors too much power to coerce defendants into a plea bargain regardless of guilt.

This was true in Aaron Swartz' case. According to a report in *Massachusetts Lawyers Weekly*, the district attorney's office intended to admonish, not prosecute, Swartz. (After all, he probably did trespass into a closet at MIT.) His legal nightmare, however, only began when federal prosecutors took over the case. Prosecutorial discretion has an important role in our criminal justice system, yet the obscure, technical nature of computer crimes — combined with harsh sentencing guidelines — make the CFAA particularly vulnerable to abuse by overzealous prosecutors.

No one is saying we should decriminalize computer intrusion. But we must bring the CFAA in line with our country's values of proportional sentencing and due process of law if we hope to instill a sense of legitimacy and faith in justice among digital natives. Otherwise, we will continue to radicalize and alienate the next generation of innovators — while failing to deter crime.

- › Related
- › You Might Like
- › Related Links by Contextly



- ›  Is Good for Democracy

- ›  Aaron Swartz: We Don't Need Martyrs ... But Changes

- ›  Open Access Work, We Need to Do More Than Liberate Journal Articles

- › 'Aaron's Law' Proposes Reining in Federal Anti-Hacking Statute



US Attorney Says Aaron Swartz Prosecution 'Was Appropriate' - Wired



Work Events Join the Contextual-Computing Party



It's Hard, Let's Go Demoing



Fix CISPA — Let's Fix It, Because We Need It



Forget the GUI: It's Time for a Conversational User Interface

Post Comment | 31 Comments and 245 Reactions | [Permalink](#)

[Back to top](#)

[Tweet](#) [348](#) [69](#)

[Reddit](#) [Digg](#) [Stumble Upon](#) [Email](#)

31 comments • **245 reactions**

★ 3



Leave a message...

Best Community [Share](#)

Jim Duncalf • a month ago
Today, prosecutors can hide exculpatory evidence, bribe witness, make up stories even lie with total immunity from any consequences, They use race, status or political connections as deciding factors of rather to prosecute or not. But true justice requires equal treatment. The law of Moses, the 14th amendment and common sense tells us this. So why do we see thousands of cases each year where innocent people are driven to desperation, bankruptcy and sometimes even suicide? This

[Collapse](#)

[Previous Article](#)
How Facebook Can Totally Undermine Apple and Google in the Platform Games



LAWFARE

HARD NATIONAL SECURITY CHOICES

House Judiciary CFAA Bill

By [Paul Rosenzweig](#)

Tuesday, March 26, 2013 at 2:19 PM

The House Judiciary Committee [has released a draft](#) cyber bill that would modify the Computer Fraud and Abuse Act. The bill is on a fast track as the House hopes to have a week of “cyber” legislation in the middle of April to include an R&D bill, FISMA reform and CISPA, in addition to this bill.

My quick review and reaction to this bill is that it seems to answer most of what the Department of Justice wants with very little for the internet online community in return. Most notably the bill would make violations of the CFAA predicate acts for a RICO criminal charge — what this means is that if you engage in just two instances of violating the CFAA, then you are engaged in a pattern of racketeering, with substantial criminal penalties and ..since the criminal definitions translate directly to civil liability .. a very significant possibility of a “bet the company” civil suit. Not a move designed to foster innovation, I think.

The only modest change that might be viewed as a victory for online activists is the setting of a \$5000 valuation floor for criminal charges based upon actions that “exceed authorization.” I [have written about this before](#) and [explained why a carve-out that decriminalizes violations of terms of service is a much better option](#). But at least the valuation floor would exclude minor ToS charges (like lying about your weight on a dating site) from prosecution, so it’s a marginal step in the right direction.

[UPDATE: [As my friends at CDT point out](#), I may have been too quick in reading the draft to laud the \$5000 valuation floor as an improvement. It turns out that the valuation test is only one of several ways in which a ToS violation may result -- and at least one of the other ways would almost certainly be an expansion of the CFAA rather than a contraction. [As Orin Kerr notes](#), since one clause makes it a crime to violate a ToS to secure non-public information, it would now be a crime to lie about your age on a dating site if you wanted her phone number. Letting the private sector define a federal crime by defining the ToS is just bad practice -- and this bill doesn't look like it is making it better.]

There is more of course — we will, for example, get a new protected category of “critical infrastructure computers” that include those vital to public health and safety or national security and controlling:

- (A) gas and oil production, storage, and delivery systems;
- “(B) water supply systems;
- “(C) telecommunication networks;
- “(D) electrical power delivery systems;
- “(E) finance and banking systems;
- “(F) emergency services;
- “(G) transportation systems and services; and
- “(H) government operations that provide essential services to the public

That isn't *everything* in America ... but it sure is an awful lot.

 Send to Kindle

Share |

Recommend

5

Send



Add a comment..

Comment

Facebook social plugin

Filed under: [Cybersecurity](#), [Cybersecurity: Crime and Espionage](#), [Cybersecurity: Legislation](#)

Tags: [Computer Fraud and Abuse Act](#)

CRAFTED BY CHARLIE ON WORDPRESS ¶ INSPIRED BY VERYPLAINTEXT BY SCOTT WALICK ¶ © 2013

Forbes



Eric Goldman, Contributor

I teach Internet Law, IP and Advertising Law at Santa Clara University

TECH | 3/28/2013 @ 4:21PM | 463 views

The Computer Fraud and Abuse Act Is a Failed Experiment

In light of Aaron Swartz's tragic suicide, there has been a lot of discussion—some productive, some not—about reforming the Computer Fraud & Abuse Act (the “CFAA”). I support some of the reform proposals, but they don't go far enough.

Initially, the CFAA banned hacking, but over the years, it has morphed into a general restriction against online trespass to chattels. In this post, I'll explain

why—and how—the concept of online

trespass to chattels should be eliminated from the CFAA and analogous state law doctrines.



No Trespassing (Photo credit: compujeramey)

The Current Law of Online Trespass to Chattels

Trespass to Chattels Offline. “Chattel” means tangible personal property, as opposed to real property like real estate or intangible assets like intellectual property. Colloquially, we often refer to chattel as our “stuff.”

In the offline world, a chattel owner has the exclusive right to possess the chattel. If someone permanently takes someone else's chattel, we call this “theft” or “conversion,” and we punish it both civilly and criminally.

Chattel interferences less significant than theft/conversion, such as temporarily depriving the chattel owner of possession (e.g., taking someone else's car for a “joyride”), may be actionable as “trespass to chattel.” Trespass to chattels is a venerable doctrine (it dates back centuries), but it does not apply to all interactions with someone else's offline chattel. The owner must show some damage from the interference. Petting someone's dog (pets are chattel) or touching someone's car with your finger may technically interfere with the chattel, but typically it's not actionable as a trespass because the chattel owner hasn't suffered any harm. The requirement that the chattel owner show some harm differs from trespass to real property, which in contrast can occur merely by a person's unauthorized presence even if the owner has experienced no other damage.

Trespass to Chattels Online. The Internet operates by passing bits of data over computer equipment, such as servers, routers and cables. All of that equipment is owned by someone. In other words, Internet data moves over a

network of privately owned chattel.

Over the years, legislatures and the courts progressively have treated the unauthorized movement of data bits over someone else's chattel into a "trespass" of that chattel—an activity I'll call "online trespass to chattels." For example, many states have enacted computer crime laws that restrict unauthorized use of Internet and telecommunications equipment. In 1997, *CompuServe v. Cyber Promotions*, a federal district court held that sending spam to an third party's email router constituted trespass to chattels under the common law (common law is judge-made law, not enacted by a legislature). Many subsequent courts have embraced that precedent. And over the years, Congress has progressively expanded the Computer Fraud & Abuse Act so that it has become, in effect, a federal prohibition on trespassing someone else's Internet equipment by sending data to it or taking data from it. With respect to the CFAA and some state computer crime laws, we punish violations both civilly and criminally.

All of these legal doctrines (the CFAA, state computer crimes, common law trespass to chattels) require that the online chattel owner show that the defendant's activity was unauthorized and that the owner suffered some damage from the defendant's use of the chattel, but the legal standards differ somewhat between the doctrines. In practice, the required damages showing is often trivial. For example, both the CFAA and California's computer crime law count the chattel owner's efforts to prevent the defendant's usage as actionable damage—and in California's case, no further showing of harm to the chattel owner is required. Effectively, simply making unauthorized use of a third party's Internet-connected chattel violate the state computer crime law. Some parts of the CFAA requires a higher quantitative showing of damages, but many cases easily clear that threshold.

Rethinking Online Trespass to Chattels

Stretching the ancient doctrine of trespass to chattels to apply to Internet activities has been an experiment in law-making. Unfortunately, I think the experiment has failed completely. The CFAA and state computer crime laws initially were designed to restrict hackers from breaching computer security—a sensible objective that, as I discuss below, should be preserved. The expansion of these laws to cover all sending or receiving of data from an Internet-connected server hasn't worked for at least three reasons.

Connecting to the Internet. When a chattel owner affirmatively connects its chattel to the Internet, we might presume that the owner wants to exchange data via the Internet. Of course, not all Internet data exchanges will be welcome; the chattel owner may have security restrictions on who can access some or all of the chattel, and no website wants to be overwhelmed with bogus exchange requests (i.e., denial-of-service attacks).

Acknowledging those caveats, we ought to legally presume that Internet-connected chattel is intended to exchange data with other Internet users. If we start with this presumption, the chattel owner can "bargain" with other Internet users to restrict their usage through a contract specifying permitted and unpermitted uses. Current online trespass to chattels doctrines contemplate this bargaining process, but the laws often let websites communicate their usage restrictions on obscure web pages that most people won't see.

Chattel owners also can use technological controls, such as security measures, to restrict unwanted chattel usage. For example, websites often use "rate

limits” to throttle the amount of data that can be gathered from the website during a specified time period and “IP address blocks” to restrict website access by specified computers.

Given that chattel owners can easily restrict how their Internet-connected chattel is used, they should bear the onus to take the contractual or technological steps to do so. Otherwise, society incurs significant transaction costs for individual users trying to determine their rights to interact with Internet-connected chattel, and overly protective legal doctrines create border cases where users engaged in socially beneficially conduct nevertheless unintentionally commit legal violations.

(Side note for economics buffs: the Coase Theorem says it doesn’t matter where we set the property entitlement so long as there are no transaction costs. I favor giving the entitlement to Internet users because (a) the chattel owner chose to connect to the Internet, and (b) it’s cheaper for the chattel owner to bargain back for the rights).

Unintended Consequences. Online trespass to chattels now reaches scenarios far beyond the hacking scenarios, sometimes in farcical ways. Three examples of troubling applications of online trespass to chattels:

- because virtually every employee uses computers at work and some employees download company data onto their personal devices, employers now routinely assert CFAA violations against ex-employees. This illustrates the CFAA’s scope creep; the CFAA wasn’t designed to apply to ordinary employee activities, but sloppy and expansive drafting enables that possibility. Fortunately, courts have balked at this trend (see, e.g., [Nosal](#) and [WEC](#)). I still favor punishing rogue employees, but online trespass to chattels is not the way to do it.
- websites may assert online trespass to chattels when a third party’s automated script gather information from their website (a process sometimes called “scraping” or “spidering”). Technically, search engine spiders commit online trespass to chattels when they access a website without permission, although we don’t often see cases asserting that. Instead, more typically [we see anti-competition lawsuits](#), including efforts to thwart price competition or shut down third party developers who enhance a website’s functionality (such as [Craigslist’s](#) and [Facebook’s](#) crackdowns).
- Lori Drew’s CFAA prosecution over Megan Maier’s suicide due to Drew’s use of a fake MySpace profile. To establish the CFAA violation, the government ([unsuccessfully](#)) argued that MySpace was the victim of Drew’s ruse because she lied to them when she created her online account. The government’s theory threatened to make virtually every Internet user a criminal because Internet users routinely fib during online account registration processes.

Doctrinal Overlap. In many situations currently covered by online trespass to chattels, at least one—and often numerous—other legal doctrines already apply. For example, trade secret law already applies to employees who walk out the door with a company’s confidential information, whether the confidential information is analog or digital. Copyright law already applies to search engines republished copyrighted material they scrape. MySpace could have brought a breach of contract claim against Drew for violating its user agreement (if it cared).

Indeed, because legal doctrines already overlap so extensively, we almost never see an online trespass to chattels claim asserted on a standalone basis. Instead, an online trespass to chattels claim is usually just one of numerous legal violations asserted against the defendant. These doctrinal overlaps mean we usually don’t need online trespass to chattels either to supplement the more squarely applicable claims or to act as a “gap-filler” to plug the rare and narrow holes left by the other legal doctrines.

Reforming Online Trespass to Chattels [click to next page]

Lawmakers aren't very good at acknowledging when their legal experiments fail ([Tim Wu](#) discusses this point more). But if lawmakers honestly judge the results of their online trespass to chattels experiment, they should:



Tim Wu
(Photo
credit:
Wikipedia)

- 1) Repeal most provisions of the CFAA (that don't relate to government-run computers) and preempt all analogous state laws, including state computer crime laws and common law trespass to chattels as applied online. Note: without dealing with analogous state laws, reforming the CFAA is an incomplete solution.
- 2) Retain only the (A) restrictions on criminal hacking, which I would define as the defeat of electronic security measures for the goal of fraud or data destruction (and some of these efforts are already covered by other laws like the Electronic Communications Privacy Act), and (B) restrictions on denial-of-service attacks, which I would define as the sending of data or requests to a server with the intent of overloading its capacity.
- 3) Eliminate all civil claims for this conduct, so that only the federal government can enforce violations.
- 4) Specify that any textual attempts to restrict server usage fail unless the terms are presented in a properly formed contract (usually, a mandatory click-through agreement).

Obviously, these proposals are dramatic, but they are in keeping with my goal of eliminating the legal concept of online trespass to chattels. Even if we do that, chattel owners are hardly defenseless. They can still take advantage of a panoply of other legal doctrines, they can still use (properly formed) contracts to bargain back the rights from users, and they can still use technological controls. As a result, these proposed changes will end the adverse consequences from the online trespass to chattels experiment while letting chattel owners prevent socially disadvantageous online usage of their chattels.

This article is available online at:

<http://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/>



March 21, 2013

HUFF
POST TECH

Matthew Keys Case Shows Rogue Employees Can Be Just As Dangerous As Hackers

Posted: 03/19/2013 4:13 pm EDT | Updated: 03/19/2013 5:50 pm EDT

The 26-year-old Reuters editor allegedly behind the hacking of the Los Angeles Times website was not a hacker. He said so himself.

"I'm not a hacker," Matthew Keys allegedly wrote in an online chatroom he shared with members of Anonymous. "I'm an ex-employee."

Federal prosecutors charged last week that Keys used his access as a former employee of the Tribune Co. to help a hacker deface the website of the Los Angeles Times in 2010. The Tribune Co. owns the paper as well as the Sacramento TV station where Keys had worked until he was fired -- two months before the hacking incident.

The charges highlight a security threat that often goes overlooked as media attention to cybersecurity tends to focus on the possibility of state-sponsored Chinese hackers infiltrating American computer systems. Industry experts say corporations are also under attack from disgruntled employees or ex-employees, who can hijack sensitive data.

The industry calls them "insider threats." One study claims they are responsible for more than two-thirds of all intellectual property theft.

Ex-employees divulge corporate secrets "all the time," said John Pescatore, director of emerging security trends at SANS Institute, a nonprofit cybersecurity research organization. The problem is especially pronounced during economic downturns, when companies lay off workers but fail to cut off their access to corporate networks, he said.

According to Pescatore, rogue insiders can cause more damage than outside hackers because they are harder to detect, giving them more time to wreak havoc. It takes companies on average nearly three years to notice an employee is stealing secrets, according to a study published last year by Carnegie Mellon University. Malicious insiders are already able to access sensitive information as part of their jobs, so "no alarms are going to go off," Pescatore said.

In some cases, the very person responsible for monitoring the company's computer network for suspicious activity is the rogue employee himself. A survey last year of nearly 200 IT professionals found that "despite the attention that hackers and other external security threats receive, it is internal, not *external* threats, which are perceived as greater risks," according to the security firm AlgoSec.

"Moles, opportunists, contractors, disgruntled employees, and ex-IT personnel all currently pose a greater risk to corporate intellectual property than state-sponsored hacking," said a report issued earlier this year by Kroll Advisory Solutions, a security firm.

The profile of an employee who chooses to share corporate secrets isn't fixed. Some are spies who provide company information to other organizations or countries. Others take proprietary information for personal gain. Many are disgruntled employees seeking revenge against their employers.

Federal prosecutors says Matthew Keys, who had been in charge of social media for Fox 40 in Sacramento, fit this latter description.

After he was fired from the station in October 2010, Keys wrote on his personal blog that Tribune Co. was a "bankrupt news organization that didn't value its employees on the assembly line."

In a search warrant affidavit, the FBI said Keys later entered an online chatroom with members of Anonymous and "specifically asked if anyone was interested in defacing Fox or the LA Times." After passing on a username and password, Keys allegedly told the hackers: "go f**k some s**t up!"

Keys did not return emails or phone calls Tuesday seeking comment. His attorneys say he did not provide hackers access to Tribune's network and that he was working as an undercover journalist when he communicated online with members of Anonymous.

Keys faces up to 25 years in prison and fines of up to \$750,000 -- strong penalties, but not uncommon for insider hacking cases.

Perhaps the most famous case of an employee accused of causing trouble on his employer's network is that of Pfc. Bradley Manning, who was charged with providing thousands of government documents to the anti-secrecy group WikiLeaks. Last month, Manning pleaded guilty on some counts, but military prosecutors plan to pursue further charges that could yield a sentence of life in prison without parole.

In 2008, San Francisco city engineer Terry Childs hijacked the computer network used by city employees for email and data. Childs had been recently reassigned but was the only employee who knew all the codes and passwords to operate the system. He was arrested but refused to give up the network log-in details until San Francisco Mayor Gavin Newsom visited Childs in jail and convinced him to

release the information. Childs was sentenced in 2010 to four years in prison.

In 2009, a computer engineer who worked for the mortgage giant Fannie Mae planted a logic bomb -- a malicious code set to damage the company's network on a certain date -- after he was fired. The logic bomb, which would have shut down the company for a week, was discovered before it could go off. The engineer, Rajendrasinh Babubha Makwana, was sentenced in 2010 to serve three years in prison.

In 2010, Sergey Aleynikov, a former Goldman Sachs programmer, was charged with stealing the bank's confidential code for its high-frequency trading operations when he left the company to join a startup. He was found guilty of theft of trade secrets. A federal appeals court overturned his conviction last year but the Manhattan district attorney charged him again last August with state crimes. If convicted, Aleynikov could face up to four years in prison.

Pescatore said companies can avoid such incidents by cutting off ex-employees' access to corporate accounts and keeping current employees on a "need to know basis" inside the network.

"Quite often the insider has too much access," he said. "But the need to share [company data] trumps the need to know, so problems like this happen."



Atlanta Division

Home • Atlanta • Press Releases • 2009 • International Effort Defeats Major Hacking Ring

International Effort Defeats Major Hacking Ring

Elaborate Scheme Stole over \$9.4 Million from Credit Card Processor

U.S. Attorney's Office
November 10, 2009

Northern District of Georgia
(404) 581-6000

ATLANTA—VIKTOR PLESHCHUK, 28, of St. Petersburg, Russia; SERGEI TŠURIKOV, 25, of Tallinn, Estonia; and OLEG COVELIN, 28, of Chişinău, Moldova, along with an unidentified individual, have been indicted by a federal grand jury on charges of conspiracy to commit wire fraud, wire fraud, conspiracy to commit computer fraud, computer fraud, and aggravated identity theft. IGOR GRUDJJEV, 31, RONALD TSOI, 31, EVELIN TSOI, 20, and MIKHAIL JEVGENOV, 33, each of Tallinn, Estonia, have been indicted by a federal grand jury on charges of access device fraud.

Acting United States Attorney Sally Quillian Yates said of the case, "Last November, in just one day, an American credit card processor was hacked in perhaps the most sophisticated and organized computer fraud attack ever conducted. Today, almost exactly one year later, the leaders of this attack have been charged. This investigation has broken the back of one of the most sophisticated computer hacking rings in the world. This success would not have been possible without the efforts of the victim and unprecedented cooperation from various law enforcement agencies worldwide."

In Washington, D.C., Assistant Attorney General of the Criminal Division Lanny A. Breuer said, "The charges brought against this highly sophisticated international hacking ring were possible only because of unprecedented international cooperation with our law enforcement partners, particularly between the United States and Estonia. Through our close cooperation, both nations have demonstrated our commitment to identifying sophisticated attacks on U.S. financial networks that are directed and operated from overseas and our commitment to bringing the perpetrators to justice."

FBI Atlanta Special Agent in Charge Greg Jones said, "Through the diligent efforts of the victim company and multiple law enforcement agencies within the United States and around the world, the leaders of a technically advanced computer hacking group were identified and indicted in Atlanta, sending a clear message to cyber criminals across the globe. Justice will not stop at international borders, but continue with the ongoing cooperation between the FBI and other agencies such as the Estonian Central Criminal Police and the Netherlands Police Agency."

According to Acting United States Attorney Yates, the charges and other information presented in court: During November, 2008, PLESHCHUK, TŠURIKOV, and COVELIN allegedly obtained unauthorized access into the computer network of "RBS WorldPay," the U.S. payment processing division of the Royal Bank of Scotland Group PLC, located in Atlanta. The indictment alleges that the group used sophisticated hacking techniques to compromise the data encryption that was used by RBS WorldPay to protect customer data on payroll debit cards. Payroll debit cards are used by various companies to pay their employees. By using a payroll debit card, employees are able to withdraw their regular salaries from an ATM.

Once the encryption on the card processing system was compromised, the hacking ring allegedly raised the account limits on compromised accounts, and then provided a network of "cashers" with 44 counterfeit payroll debit cards, which were used to withdraw more than \$9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. The \$9 million loss occurred within a span of less than 12 hours.

The hackers then allegedly sought to destroy data stored on the card processing network in order to conceal their hacking activity. The indictment alleges that the "cashers" were allowed to keep 30 to 50 percent of the stolen funds, but transmitted the bulk of those funds back to TSURIKOV, PLESHCHUK and other co-defendants, using means such as WebMoney accounts and Western Union. Upon discovering the unauthorized activity, RBS WorldPay immediately reported the breach, and has substantially assisted in the investigation.

Throughout the duration of the cashout, PLESHCHUK and TŠURIKOV allegedly monitored the fraudulent ATM withdrawals in real time from within the computer systems of RBS WorldPay. Once the withdrawals were completed, PLESHCHUK and TŠURIKOV allegedly attempted to conceal their activities in the RBS WorldPay computer network by destroying and attempting to destroy data.

TŠURIKOV was not only an alleged hacker, but also distributed fraudulently obtained debit card account numbers and PIN codes to IGOR GRUDJJEV, who, in turn, allegedly distributed the information to defendants RONALD TSOI, EVELIN TSOI, and MIKHAIL JEVGENOV in Estonia.

Atlanta Division Links

Atlanta Home

Contact Us

- Overview
- Territory/Jurisdiction

News and Outreach

- Press Room | Stories
- In Your Community

About Us

- Our People & Capabilities
- What We Investigate
- Our Partnerships
- Atlanta History

Wanted by the FBI - Atlanta

FBI Jobs

CFAA Indictments
§ 1030 (a)(2)
(a)(4)

Together, RONALD TSOI, EVELIN TSOI, and MIKHAIL JEVGENOV allegedly withdrew funds worth approximately \$289,000 in U.S. funds from ATMs in Tallinn, Estonia. Charges based on these transactions are pending in Estonia.

The indictment charges 16 counts. Count one charges PLESHCHUK, TŠURIKOV, COVELIN, and a fourth unidentified individual of conspiracy to commit wire fraud. Counts two through 10 are substantive wire fraud charges brought against PLESHCHUK and TŠURIKOV, aided and abetted by COVELIN and the unidentified hacker, based on the computer commands sent from outside the United States to the computer network of RBS WorldPay in the Northern District of Georgia. Count 11 charges PLESHCHUK, TŠURIKOV, COVELIN, and the fourth individual with conspiracy to commit computer fraud. Counts 13 through 14 are substantive charges of computer fraud against the defendants. Count 15 charges these defendants with aggravated identity theft based on the prepaid payroll card account numbers and associated PIN codes they transferred, possessed, and used without authorization in committing the wire fraud. Count 16 charges RONALD TSOI, EVELIN TSOI, and JEVGENOV, aided and abetted by GRUDJJEV, with access device fraud.

The indictment seeks forfeiture of over \$9.4 million of proceeds of the crimes from the defendants.

PLESHCHUK, TŠURIKOV, COVELIN, and the unidentified defendant each face a maximum sentence of up to 20 years for conspiracy to commit wire fraud and each wire fraud count; up to five years for conspiracy to commit computer fraud; up to five or 10 years for each count of computer fraud; a two-year mandatory minimum for aggravated identity theft; and fines up to \$3.5 million dollars. The charges against GRUDJJEV, the TSOIs, and JEVGENOV carry a maximum of up to 15 years incarceration for each count and a fine of up to \$250,000. In determining the actual sentence, the court will consider the United States Sentencing Guidelines, which are not binding but provide appropriate sentencing ranges for most offenders.

The early detection of fraudulent ATM withdrawal activities in Tallinn, Estonia led to an immediate response by the Estonian Central Criminal Police. Their investigative efforts led to the prompt identification of TŠURIKOV, GRUDJJEV, the TSOIs, and JEVGENOV. TŠURIKOV is presently in custody in Estonia on charges related to access device fraud. The extradition of TŠURIKOV to the United States is currently in process. Access device fraud charges are also pending in Estonia against GRUDJJEV, the TSOIs, and JEVGENOV. Cooperation between the Hong Kong Police Force and the FBI also led to a parallel investigation, resulting in the identification and arrest of two individuals who were responsible for withdrawing RBS WorldPay funds from ATM terminals in Hong Kong. The Netherlands Police Agency National Crime Squad High Tech Crime Unit and the Netherlands National Prosecutor's Office provided key assistance in the investigation.

Members of the public are reminded that the indictment contains only allegations. A defendant is presumed innocent of the charges and it will be the government's burden to prove a defendant's guilt beyond a reasonable doubt at trial.

This case is being investigated by special agents of the Federal Bureau of Investigation. Assistance was provided by international law enforcement partners. The United States Secret Service also participated in the investigation. RBS World Pay immediately reported the crime and has substantially assisted in the investigation.

Assistant United States Attorneys Lawrence R. Sommerfeld and Gerald Sachs, and Senior Counsel Kimberly Kiefer Peretti of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice are prosecuting the case. Office of International Affairs counsel Deborah Gaynus is assisting with extradition matters. Treaty assistance was provided by Office of International Affairs counsels Betsy Burke, Blair Berman, Roman Chaban, Judith Friedman, Deborah Gaynus, Linda McKinney, and Mary McLaren.

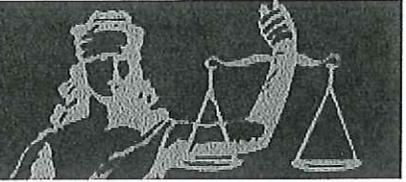
For further information please contact Sally Q. Yates, Acting United States Attorney, or Charysse L. Alexander, Executive Assistant United States Attorney, through Patrick Crosby, Public Affairs Officer, U.S. Attorney's Office, at (404) 581-6016. The Internet address for the HomePage for the U.S. Attorney's Office for the Northern District of Georgia is www.usdoj.gov/usao/gan.

[Accessibility](#) | [eRulemaking](#) | [Freedom of Information Act](#) | [Legal Notices](#) | [Legal Policies and Disclaimers](#) | [Links](#) | [Privacy Policy](#) | [USA.gov](#) | [White House](#)
FBI.gov is an official site of the U.S. government, U.S. Department of Justice

Close

Home » News

PRESS RELEASES



Follow @SDNYNews

Printer Friendly

Three Alleged International Cyber Criminals Responsible For Creating And Distributing Virus That Infected Over One Million Computers And Caused Tens Of Millions Of Dollars In Losses Charged In Manhattan Federal Court

FOR IMMEDIATE RELEASE

Wednesday, January 23, 2013

Gozi Virus Creator, a Russian National, Pled Guilty to Computer Intrusion Charges; Gozi Code-Writer Arrested in Latvia; and Host of Servers That Facilitated and Shielded the Distribution of Gozi and Other Viruses and Malware Arrested in Romania

NASA Computers Among the 40,000 U.S. Computers Infected With Gozi Virus

Preet Bharara, the United States Attorney for the Southern District of New York, Lanny A. Breuer, the Assistant Attorney General of the U.S. Department of Justice's Criminal Division, and George Venizelos, the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced today the unsealing of Indictments against three individuals who played critical roles in creating and distributing the Gozi Virus, one of the most financially destructive computer viruses in history. The Gozi Virus infected over one million computers globally and caused tens of millions of dollars in losses. NIKITA KUZMIN, a Russian national who created the Gozi Virus, was arrested in the U.S. in November 2010 and pled guilty before U.S. District Judge Leonard B. Sand to various computer intrusion and fraud charges in May 2011. DENISS CALOVSKIS, a/k/a "Miami," a Latvian national who allegedly wrote some of the computer code that made the Gozi Virus so effective, was arrested in Latvia in November 2012. MIHAI IONUT PAUNESCU, a/k/a "Virus," a Romanian national who allegedly ran a "bulletproof hosting" service that enabled cyber criminals to distribute the Gozi Virus, the Zeus Trojan and other notorious malware, and conduct other sophisticated cyber crimes, was arrested in Romania in December 2012.

Manhattan U.S. Attorney Preet Bharara said: "In an information-age update on Willie Sutton, these men allegedly ran a modern-day bank robbery ring, and like Sutton, they targeted banks because that's where the money still is. But as we have seen with increasing frequency, cyber criminals' bank heists require neither a mask nor a gun, just a clever program and an Internet connection. This case should serve as a wake-up call to banks and consumers alike, because cybercrime remains one of the greatest threats we face, and it is not going away any time soon."

FBI Assistant Director-in-Charge George Venizelos said: "This long-term investigation uncovered an alleged international cybercrime ring whose far-reaching schemes infected at least one million computers worldwide and 40,000 in the U.S., and resulted in the theft or loss

of tens of millions of dollars. Banking Trojans are to cyber criminals what safe-cracking or acetylene torches are to traditional bank burglars – but far more effective and less detectable. The investigation put an end to the Gozi virus.”

According to the allegations in the Indictments and the Complaint unsealed today in Manhattan federal court:

The Gozi Virus

The Gozi Virus is malicious computer code or “malware” that steals personal bank account information, including usernames and passwords, from the users of affected computers. It was named by private sector information security experts in the U.S. who, in 2007, discovered that previously unrecognized malware was stealing personal bank account information from computers across Europe on a vast scale, while remaining virtually undetectable in the computers it infected. To date, the Gozi Virus has infected over one million victim computers worldwide, among them at least 40,000 computers in the U.S., including computers belonging to the National Aeronautics and Space Administration (“NASA”), as well as computers in Germany, Great Britain, Poland, France, Finland, Italy, Turkey and elsewhere, and it has caused tens of millions of dollars in losses to the individuals, businesses, and government entities whose computers were infected.

The Gozi Virus was distributed to victims’ computers in several different ways. In one method, the virus was disguised as an apparently benign .pdf document which, when opened, secretly installed the Gozi Virus on the victim’s computer. Once installed, the Gozi Virus – which was intentionally designed to be undetectable by anti-virus software – collected data from the infected computer in order to capture personal bank account information including usernames and passwords. That data was then transmitted to various computer servers controlled by the cyber criminals who used the Gozi Virus. These cyber criminals then used the personal bank account information to transfer funds out of the victims’ bank accounts and ultimately into their own personal possession.

The Creation of the Gozi Virus

KUZMIN conceived of the Gozi Virus in 2005 when he created a list of technical specifications for the virus and hired a sophisticated computer programmer (“CC-1”) to write its source code, which is the unique code that enabled the Gozi Virus to operate. Once the Gozi Virus had been coded, KUZMIN began providing it to co-conspirators in exchange for a weekly fee through a business he ran called “76 Service.” Through “76 Service,” KUZMIN made the Gozi Virus available to co-conspirators, allowed them to configure the virus to steal data of their choosing, and stored the stolen data for them. He advertised “76 Service” on one or more Internet forums devoted to cybercrime and other criminal activities. Beginning in 2009, KUZMIN began to sell the Gozi Virus outright to his co-conspirators.

The Refinement of the Gozi Virus

KUZMIN and his co-conspirators regularly paid others to refine, update, and improve the Gozi Virus. For example, CALOVSKIS, a co-conspirator, was hired to develop certain computer code, known as “web injects,” which altered how the webpages of particular banks appeared on infected computers. Specifically, CALOVSKIS’s web injects changed the webpages of banks so that, when a victim used an infected computer to access the webpage, the victim was tricked into divulging additional personal information that cyber criminals would need in order to successfully steal money from the victim’s bank account. One web inject CALOVSKIS designed altered the customer welcome page of a bank so that the victim was prompted to disclose additional personal information – mother’s maiden name, social security number, driver’s

license information, and a PIN code – in order to continue accessing the website.

The Gozi Virus and Bulletproof Hosting Services

Bulletproof hosting” services helped cyber criminals distribute the Gozi Virus with little fear of detection by law enforcement. Bulletproof hosts provided cyber criminals using the Gozi Virus with the critical online infrastructure they needed, such as Internet Protocol (“IP”) addresses and computer servers, in a manner designed to enable them to preserve their anonymity.

PAUNESCU operated a “bulletproof host” that helped cyber criminals distribute the Gozi Virus and commit other cyber crimes, such as distributing malware including the “Zeus Trojan” and the “SpyEye Trojan,” initiating and executing distributed denial of service (“DDoS”) attacks, and transmitting spam. PAUNESCU rented servers and IP addresses from legitimate Internet service providers and then in turn rented them to cyber criminals; provided servers that cyber criminals used as command-and-control servers to conduct DDoS attacks; monitored the IP addresses that he controlled to determine if they appeared on a special list of suspicious or untrustworthy IP addresses; and relocated his customers’ data to different networks and IP addresses, including networks and IP addresses in other countries, to avoid being blocked as a result of private security or law enforcement scrutiny.

* * *

A chart setting forth the names, ages and residences of the defendants, the charges each defendant faces, and the statutory maximum penalty associated with these charges is attached. Extradition proceedings against CAVLOSKIS in Latvia and PAUNESCU in Romania are ongoing.

The case against PAUNESCU is being prosecuted jointly with the Department of Justice’s Computer Crime and Intellectual Property Section (“CCIPS”), which is overseen by Assistant Attorney General Lanny A. Breuer. Mr. Bharara thanked CCIPS for its important partnership in this matter, and he also thanked the Department of Justice’s Office of International Affairs. Mr. Bharara praised the FBI for its outstanding work in the investigation, which he noted is ongoing. He also specially thanked the National Aeronautics and Space Administration Office of Inspector General, the Central Criminal Police Department of the Latvian State Police, the Romanian Intelligence Service, the Romanian Directorate for Combating Organized Crime, the Romanian Directorate for Investigating Organized Crime and Terrorism, and the Romanian Ministry of Justice.

The cases are being handled by the Complex Frauds Unit of the United States Attorney's Office. Assistant United States Attorneys Sarah Lai, Nicole Friedlander, and Thomas G.A. Brown, along with Trial Attorney Carol Sipperly of the Computer Crime and Intellectual Property Section of the Department of Justice on the PAUNESCU case, are in charge of the prosecution.

The charges contained in the Indictments are merely accusations and the defendants are presumed innocent unless and until proven guilty.

13-029

CFAA Indictments

§ 1030 (a)(2)
(a)(4)
(a)(5)(A)
(a)(6)

Defendant	Age and Residence	Charges	Maximum Penalty
NIKITA KUZMIN	Age 25; Moscow, Russia	Conspiracy to commit bank fraud; bank fraud; conspiracy to commit access device fraud; access device fraud; conspiracy to commit computer intrusion; computer intrusion	95 years in pris
DENISS CALOVSKIS	Age 27; Riga, Latvia	Conspiracy to commit bank fraud; conspiracy to commit access device fraud; conspiracy to commit computer intrusion; conspiracy to commit wire fraud; conspiracy to commit aggravated identity theft	67 years in pris
MIHAI IONUT PAUNESCU	Age 28; Bucharest, Romania	Conspiracy to commit computer intrusion; conspiracy to commit bank fraud; conspiracy to commit wire fraud	60 years in pris

[Return to Top](#)

The New York Times Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers here or use the "Reprints" tool that appears next to any article. Visit www.nytreprints.com for samples and additional information. Order a reprint of this article now.



March 13, 2012

New Interest in Hacking as Threat to Security

By MICHAEL S. SCHMIDT

WASHINGTON — During the five-month period between October and February, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories and databases, according to the Department of Homeland Security, compared with 11 over the same period a year ago.

None of the attacks caused significant damage, but they were part of a spike in hacking attacks on networks and computers of all kinds over the same period. The department recorded more than 50,000 incidents since October, about 10,000 more than in the same period a year earlier, with an incident defined as any intrusion or attempted intrusion on a computer network.

The increase has prompted a new interest in cybersecurity on Capitol Hill, where lawmakers are being prodded by the Obama administration to advance legislation that could require new standards at facilities where a breach could cause significant casualties or economic damage.

It is not clear whether the higher numbers were due to increased reporting amid a wave of high-profile hacking, including the arrest last week of several members of the group Anonymous, or an actual increase in attacks.

James A. Lewis, a senior fellow and a specialist in computer security issues at the Center for Strategic and International Studies, a policy group in Washington, said that as hacking awareness had increased, attacks had become more common. He said that the attacks on the nation's infrastructure were particularly jarring.

"Some of this is heightened awareness because everyone is babbling about it," he said of the reported rise in computer attacks. "But much of it is because the technology has improved and the hackers have gotten better and people and countries are probing around more like the Russians and Chinese have."

He added: "We hit rock bottom on this in 2010. Then we hit rock bottom in 2011. And we are

still at rock bottom. We were vulnerable before and now we're just more vulnerable. You can destroy physical infrastructure with a cyberattack just like you could with a bomb.”

The legislation the administration is pressing Congress to pass would give the federal government greater authority to regulate the security used by companies that run the nation's infrastructure. It would give the Homeland Security Department the authority to enforce minimum standards on companies whose service or product would lead to mass casualties, evacuations or major economic damage if crippled by hackers.

The bill the administration backs is sponsored by Senators Joseph I. Lieberman, independent of Connecticut, and Susan Collins, Republican of Maine. It has bipartisan support, and its prospects appear good. Senator John McCain, Republican of Arizona, is sponsoring a more business-friendly bill that emphasizes the sharing of information and has fewer requirements for companies.

Last week on Capitol Hill, Janet Napolitano, the secretary of Homeland Security; Robert S. Mueller III, the director of the Federal Bureau of Investigation; and Gen. Martin E. Dempsey, the chairman of the Joint Chiefs of Staff, made their pitch to roughly four dozen senators about why they should pass the Lieberman-Collins bill.

At a closed-door briefing, the senators were shown how a power company employee could derail the New York City electrical grid by clicking on an e-mail attachment sent by a hacker, and how an attack during a heat wave could have a cascading impact that would lead to deaths and cost the nation billions of dollars.

“I think General Dempsey said it best when he said that prior to 9/11, there were all kinds of information out there that a catastrophic attack was looming,” Ms. Napolitano said in an interview. “The information on a cyberattack is at that same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something.”

General Dempsey told the senators that he had skipped a meeting of the National Security Council on Iran to attend the briefing because he was so concerned about a cyberattack, according to a person who had been told details of the meeting. A spokesman for General Dempsey said the chairman had “sent his vice chairman to the meeting on Iran so that he could attend the Senate meeting and emphasize his concern about cybersecurity.”

“His point was about his presence at the cyber exercise rather than a value judgment on the ‘threat,’ ” the spokesman, Col. David Lapan, said.

Experts say one of the biggest problems is that no part of the government has complete authority over the issue. The Central Intelligence Agency and the National Security Agency

give the government intelligence on potential attacks, and the F.B.I. prosecutes hackers who break the law. The Department of Homeland Security receives reports about security breaches but has no authority to compel business to improve their security.

“Nobody does critical infrastructure of the dot-com space where America now relies on faith healing and snake oil for protection,” Mr. Lewis said. “The administration wants it to be the Department of Homeland Security, but the department needs additional authorities to be effective.”

National security threat: hacking the smart grid

Sylvie Barak

4/5/2012 8:19 AM EDT

SAN JOSE, Calif.--The nation's smart grid is constantly under threat of real attack and potentially no amount of investment in securing it will help, according to a white hat security expert.

Speaking at DesignWEST panel on hacking the smart grid, senior research engineer Joe Loomis blasted through the buzz on smart grid and smarter energy technology, exposing the risks of hacking and full scale cyber warfare and the crippling effects it could have on national infrastructure.

"It's critical infrastructure and society depends on it, making it a prime target for attack," said Loomis. Indeed, as smart grid technology develops year by year, so too do the opportunities for hackers with malicious intentions on national infrastructure.

Loomis pointed to the recent Stuxnet computer worm discovered in June 2010, which took out a large portion of Iran's nuclear centrifuge control and disrupted the delivery of nuclear fuel with its payload. That worm, whose origins are still not officially known, exploited multiple zero-day vulnerabilities, said Loomis, spreading quickly across the world and even ending up in a few systems in the United States, despite Iran being the clear target.

"What made Stuxnet more scary than anything else is the order of magnitude of sophistication over everything that came before it," said Loomis adding that the success of the worm was proof of concept that cyber warfare was real and dangerous.

"The collateral infections are the scariest part," said Loomis, claiming that analysis of Stuxnet pointed to it having been developed by over 40 engineers, though no country or group takes responsibility for it.

A similar worm, DuQu, was discovered more recently in September 2011 and is thought to have been developed the same team that created Stuxnet, though its purpose is apparently different, with DuQu having been designed to capture system information and keystrokes which could enable a future Stuxnet-like attack.

"People are actively pursuing cyber warfare as an attack method," said Loomis, pointing out that the smart grid was a prime target for such an attack.

"Before, if someone wanted to shut off power to my home, the electricity company would have to send someone around, physically, to cut me off. Now, it's all being networked and can be shut off remotely, which creates a dangerous risk," he said.

With \$3.4 billion in stimulus funds having been funneled into smart-grid technologies by the U.S.

government, more and more American households and businesses are getting connected up to smart meters, with over 60 million predicted to be deployed this year alone.

That's a scary prospect according to Loomis who claims there are already "multiple credible threats" out there.

"They could turn off our power if they wanted to," he said.

The most difficult thing, said Loomis, was for individuals and firms to evaluate the risks and invest in protection accordingly. "These are systems that were never designed to be secured," he said, noting that any investment may also ultimately prove worthless.

"No system is 100 percent secure," he said. "Given enough time and access, you can reverse engineer the whole thing."

Loomis added that even if the country, or individual businesses spent a great deal of money to secure the power infrastructure, it would still be open to compromise, and that it was thus up to every individual to determine how much money they wanted to spend on trying to plug up the security holes.

"I tell clients they should judge it on a case by case situation," he said, recommending that people lobby for better standards and repeatedly test their systems for cracks.

"There are plenty of open source tools available that are ideal for protocol testing," he said.

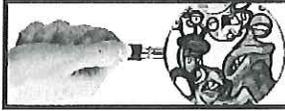
The Hacker News™

Security in a serious way

+326,243

78,635
Follow

117,815
Like 118k



And find out where your vulnerabilities may be lurking.

nCircle®
purecloud.ncircle.com

Subscribe News Updates

Related Ads: Mobile Security, Hacking Security, Ethical Hacking, Network Security

Intelligence and National Security Alliance (INSA) hacked

Share 17

Like 157

Tweet 87

9

9

Posted by: Mohit Kumar on Sunday, September 18, 2011

Follow Us

Like 118k

Follow

CIA - Intelligence Degree

www.AMU.APUS.edu/Intelligence

Earn an intelligence degree online at American Military University.



Intelligence and National Security Alliance (INSA) hacked

On



The Hacker News on

Follow

+353,073

And find out where your vulnerabilities may be lurking.

nCircle® purecloud.ncircle.com

Popular News this Week



World's biggest DDoS attack that Almost Broke the Internet



Russian underground vSkimmer Botnet targeting payment world



Hacker uses Evernote account as Command-and-Control Server

Like

Wednesday, 48 hours after releasing a policy paper on cybersecurity, the top trade association for intelligence contractors got a first-hand lesson on the subject: they discovered that their website was hacked.

Cryptome, a site affiliated with the hacker collective Anonymous, published the membership emails and phone numbers and in some cases home addresses for the members of the Intelligence and National Security Alliance (INSA). By clicking on a link titled, "INSA Nest of Official and Corporate Spies," anyone can find contact information for senior officials at the NSA, FBI, and CIA, as well as top national security contracting firms like Booz Allen Hamilton.

The apparent cyberattack on the Intelligence and National Security Alliance, or INSA, is the latest example of the ability of hackers to penetrate the computer systems of government agencies and private companies — including those that pride themselves on their savvy and expertise in cybersecurity.

INSA is only the latest example of how the intelligence community and its affiliated contractors have been

hacked by increasingly brazen hackers. On July 11, Anonymous published some 90,000 emails and login credentials for U.S. military officers after breaking into the servers of Booz Allen Hamilton. The group published the data on a website called Pirate Bay and announced on Twitter that July 11 was "Military Meltdown Monday." The month before, another group of hackers called "LulzSec" (who claim to have since disbanded) published internal files from the FBI and claimed to briefly disable the CIA's public website.

"Due to the nature of our business, INSA takes security very seriously," McCarthy said in a statement. "We are outraged that someone finds it sporting to make private organizational data public, but we are not naïve. It is not a coincidence that this incident happened just two days after INSA's Cybersecurity Council released a report documenting the need for government and the private sector to begin to work together to solve our nations cyber security vulnerabilities."

DDoS Attacks

radware.com/DDoS_Attacks

DDoS Attacks Cost You Time & Money Free DDoS Attack White Paper



AdChoices

Follow Us Like 118k Follow

Posted in Categories: Defacements , Hacker News , how to join anonymous , News

You might also like



How Hackers can Track your Mobile phone with a cheap setup ?



Hacking Facebook Passwords like changing your own Password



Jailed cyber criminal hacked into prison computer system from Jail



Facebook hacked in Zero-Day Attack



26 Underground Hacking Exploit Kits available for Download I



JavaScript hole in Facebook I

Recommended by

Author Info



Mohit Kumar aka 'Unix Root' is Founder and Editor-in-chief of 'The Hacker News'. He is a Security Researcher and Analyst, with experience in various aspects of Information Security. Other than this : He is an Internet Activist, Strong supporter of Anonymous & Wikileaks. Follow him @ Twitter | LinkedIn | Google | Email | Facebook Profile



Hacking Facebook Passwords like changing your own Password



Java enabled browsers are highly vulnerable



Anonymous hacktivist Barrett Brown's Mother faces Prison for hiding Evidences



Smartphones cache poses huge risk for Cloud Storage Security



How Hackers can Track your Mobile phone with a cheap setup ?



Human Rights Activists targeted with new Android malware

Tech Blog Updates

Hacker reported security holes in BSNL Haryana state Intranet portal

Exploit Database website Inj3ct0r defaced

BBC Twitter Account Hacked by Syrian Electronic Army

Anonymous threatens to dump credit card details of many from law enforcement

Reuters editor Matthew Keys charged with aiding Anonymous hackers

Most Frequently Used Unix-Linux Command Reference

Sudo Local Authentication Bypass Vulnerability when clock is reset

Security and Pentest Tools

The Social-Engineer Toolkit (SET) v4.7 released

Biggest password cracking wordlist with millions of words

Phrozen Keylogger Lite v1.0 download

Pentoo 2013.0 RC1.1 Released

Snort 2.9.4.1 - Network intrusion detection system

Recon-ng : Web Reconnaissance framework for Penetration testers

Unhide Forensic Tool, Find hidden processes and ports

2 comments

☆ 3

Mobile version for this page 



Leave a message...

Best Community

Share  



EpicWin · 2 years ago
Was hacked by a Macedonian hacker..annon had nothing to do with this.

0 ·  Reply ·  Share



Bobby C · 2 years ago
Bitch slapped

0 ·  Reply ·  Share



ALSO ON THE HACKERS NEWS

What's this?

World's biggest DDoS attack that Almost Broke the Internet - Hacking News

6 comments · 3 days ago



LOL — This notice is pure marketing from CloudFlare and you are promoting it.

Java enabled browsers are highly vulnerable - Hacking News

5 comments · 5 days ago



Daniel — "All this doesn't mean that Java is an insecure language or platform, or that web sites built on Java EE are any less secure than other platforms." So you just ...

Smartphones cache poses huge risk for Cloud Storage - Hacking News

4 comments · 5 days ago



Nola IT — Full device encryption may at least secure any remaining data. For example Windows Phone 8 encrypts the entire device by default - 'out of the box' full device ...

Download Kali Linux, from the creators of BackTrack - Hacking News

25 comments · 19 days ago



Pankaj — 'Kali' in Hindi language means 'Black'.

 Comment feed  Subscribe via email

[Related Ads](#) [Cyber Security](#) [Cloud Security](#) [IT Security](#) [Security Awareness](#)

© 2010-2012 by 'The Hacker News'. All rights reserved

[About Us](#) | [Advertise with us](#) | [Privacy Policy](#) | [DMCA](#) | [The Hackers Conference](#) | [Submit News](#) | [Authors](#) | [Contact Us](#)

The New York Times

March 28, 2013

Cyberattacks Seem Meant to Destroy, Not Just Disrupt

By NICOLE PERLROTH and DAVID E. SANGER

American Express customers trying to gain access to their online accounts Thursday were met with blank screens or an ominous ancient type face. The company confirmed that its Web site had come under attack.

The assault, which took American Express offline for two hours, was the latest in an intensifying campaign of unusually powerful attacks on American financial institutions that began last September and have taken dozens of them offline intermittently, costing millions of dollars.

JPMorgan Chase was taken offline by a similar attack this month. And last week, a separate, aggressive attack incapacitated 32,000 computers at South Korea's banks and television networks.

The culprits of these attacks, officials and experts say, appear intent on disabling financial transactions and operations.

Corporate leaders have long feared online attacks aimed at financial fraud or economic espionage, but now a new threat has taken hold: attackers, possibly with state backing, who seem bent on destruction.

"The attacks have changed from espionage to destruction," said Alan Paller, director of research at the SANS Institute, a cybersecurity training organization. "Nations are actively testing how far they can go before we will respond."

Security experts who studied the attacks said that it was part of the same campaign that took down the Web sites of JPMorgan Chase, Wells Fargo, Bank of America and others over the last six months. A group that calls itself the Izz ad-Din al-Qassam Cyber Fighters has claimed responsibility for those attacks.

The group says it is retaliating for an anti-Islamic video posted on YouTube last fall. But American intelligence officials and industry investigators say they believe the group is a convenient cover for Iran. Just how tight the connection is — or whether the group is acting on direct orders from the Iranian government — is unclear. Government officials and bank

executives have failed to produce a smoking gun.

North Korea is considered the most likely source of the attacks on South Korea, though investigators are struggling to follow the digital trail, a process that could take months. The North Korean government of Kim Jong-un has openly declared that it is seeking online targets in its neighbor to the south to exact economic damage.

Representatives of American Express confirmed that the company was under attack Thursday, but said that there was no evidence that customer data had been compromised. A representative of the Federal Bureau of Investigation did not respond to a request for comment on the American Express attack.

Spokesmen for JPMorgan Chase said they would not talk about the recent attack there, its origins or its consequences. JPMorgan has openly acknowledged previous denial of service attacks. But the size and severity of the most recent one apparently led it to reconsider.

The Obama administration has publicly urged companies to be more transparent about attacks, but often security experts and lawyers give the opposite advice.

The largest contingent of instigators of attacks in the private sector, government officials and researchers say, remains Chinese hackers intent on stealing corporate secrets.

The American and South Korean attacks underscore a growing fear that the two countries most worrisome to banks, oil producers and governments may be Iran and North Korea, not because of their skill but because of their brazenness. Neither country is considered a superstar in this area. The appeal of digital weapons is similar to that of nuclear capability: it is a way for an outgunned, outfinanced nation to even the playing field. "These countries are pursuing cyberweapons the same way they are pursuing nuclear weapons," said James A. Lewis, a computer security expert at the Center for Strategic and International Studies in Washington. "It's primitive; it's not top of the line, but it's good enough and they are committed to getting it."

American officials are currently weighing their response options, but the issues involved are complex. At a meeting of banking executives, regulators and representatives from the departments of Homeland Security and Treasury last December, some pressed the United States to hit back at the hackers, while others argued that doing so would only lead to more aggressive attacks, according to two people who attended the meeting.

The difficulty of deterring such attacks was also the focus of a White House meeting this month with Mr. Obama and business leaders, including the chief executives Jamie Dimon of JPMorgan Chase; Brian T. Moynihan of Bank of America; Rex W. Tillerson of Exxon Mobil;

Randall L. Stephenson of AT&T and others.

Mr. Obama's goal was to erode the business community's intense opposition to federal legislation that would give the government oversight of how companies protect "critical infrastructure," like banking systems and energy and cellphone networks. That opposition killed a bill last year, prompting Mr. Obama to sign an executive order promoting increased information-sharing with businesses.

"But I think we heard a new tone at this latest meeting," an Obama aide said later. "Six months of unrelenting attacks have changed some views."

Mr. Lewis, the computer security expert, agreed. "The Iranian attacks have tilted private sector opinion," he said. "Hence the muted reaction to the executive order versus squeals of outrage. Companies are much more concerned about this and much more willing to see a government role."

Neither Iran nor North Korea has shown anywhere near the subtlety and technique in online offensive skills that the United States and Israel demonstrated with Olympic Games, the ostensible effort to disable Iran's nuclear enrichment plants with an online weapon that destabilized hundreds of centrifuges, destroying many of them. But after descriptions of that operation became public in the summer of 2010, Iran announced the creation of its own Cyber Corps.

North Korea has had hackers for years, some of whom are believed to be operating from, or through, China. Neither North Korea nor Iran is as focused on stealing data as they are determined to destroy it, experts contend.

When hackers believed by American intelligence officials to be Iranians hit the world's largest oil producer, Saudi Aramco, last year, they did not just erase data on 30,000 Aramco computers; they replaced the data with an image of a burning American flag. In the assault on South Korea last week, some affected computers displayed an ominous image of skulls.

"This attack is as much a cyber-rampage as it is a cyberattack," Rob Rachwald, a research director at FireEye, a computer security firm, said of the South Korea attacks.

In the past, such assaults typically occurred through a denial-of-service attack, in which hackers flood their target with Web traffic from networks of infected computers until it is overwhelmed and shuts down. One such case was a 2007 Russian attack on Estonia that affected its banks, the Parliament, ministries, newspapers and broadcasters.

With their campaign against American financial institutions, the hackers suspected of being

Iranian have taken that kind of attack to the next level. Instead of using individual personal computers to fire Web traffic at each bank, they infected powerful, commercial data centers with sophisticated malware and directed them to simultaneously fire at each bank, giving them the horsepower to inflict a huge attack.

As a result, the hackers were able to take down the consumer banking sites of American Express, JPMorgan Chase, Bank of America, Wells Fargo and other banks with exponentially more traffic than hit Estonia in 2007.

In the attack on Saudi Aramco last year, the culprits did not mount that type of assault. Instead, they created malware designed for the greatest impact, coded to spread to as many computers as possible.

Likewise, the attacks last week on South Korean banks and broadcasters were far more sophisticated than coordinated denial-of-service attacks in 2009 that briefly took down the Web sites of South Korea's president and its Defense Ministry. Such attacks were annoyances; they largely did not affect operations.

This time around in South Korea, however, the attackers engineered malware that could evade popular South Korean antivirus products, spread it to as many computer systems as possible, and inserted a "time bomb" to take out all the systems at once for greatest impact.

The biggest concern, Mr. Lewis said: "We don't know how they make decisions. When you add erratic decision making, then you really have something to worry about."

» Print

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.

DuPont says paint secrets stolen, sold to China

Wed, Apr 6 2011

By Ernest Scheyder

NEW YORK (Reuters) - Chemicals giant DuPont (DD.N: [Quote](#), [Profile](#), [Research](#), [Stock Buzz](#)) sued a California company on Wednesday, alleging it sold proprietary information on a lucrative line of specialty paint to Chinese rivals.

USA Performance Technology Inc somehow obtained secret materials on how DuPont produces titanium dioxide, a popular pigment used to make paints for cars, plastics and paper, DuPont said in a filing with the U.S. District Court, Northern District of California.

In the suit, DuPont said the defendants were "in the process of providing or have provided" specific details on its titanium dioxide production process to one or more of DuPont's competitors in China.

DuPont said it does not know how the trade secrets were stolen from its facilities.

"The investigation is ongoing," DuPont spokesman Dan Turner said.

A call to Oakland-based USA Performance was not immediately returned.

DuPont wants USA Performance, as well as employees Walter Liew and John Liu, to pay "an amount equal to double actual damages" as well as other fees.

DuPont declined to say the final amount it is ultimately seeking.

DuPont is the world's largest producer of the material, also known as TiO₂. Ford Motor Co (F.N: [Quote](#), [Profile](#), [Research](#), [Stock Buzz](#)) is one of DuPont's biggest TiO₂ customers. Texas-based Huntsman Corp (HUN.N: [Quote](#), [Profile](#), [Research](#), [Stock Buzz](#)) is a rival.

DuPont does not break out sales figures for individual products, but in 2010 the unit that contains TiO₂ reported revenue of \$6.32 billion.

DuPont shares fell 0.3 percent to \$55.87 in post-market trading.

The case is E.I. Du Pont De Nemours and Company v. USA Performance Technology Inc, U.S. District Court, Northern District of California.

(Reporting by Ernest Scheyder; editing by Andre Grenon)



© Thomson Reuters 2011. All rights reserved. Users may download and print extracts of content from this website for their own personal and non-commercial use only. Republication or redistribution of Thomson Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Thomson Reuters. Thomson Reuters and its logo are registered trademarks or trademarks of the Thomson Reuters group of companies around the world.

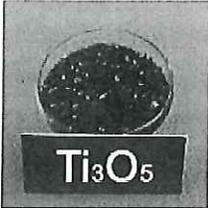
Thomson Reuters journalists are subject to an Editorial Handbook which requires fair presentation and disclosure of relevant interests.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.

Global Security, Privacy, & Risk Management

Dupont's Titanium Oxide Color Recipe- Stolen for Chinese Advantage

Posted on March 10, 2012 by Chris Mark



Many mistakenly believe that only “high tech” secrets and intellectual property are targets for intellectual property theft. In a clear example of how any propriety secret can be considered a target, a scientist (Tse Chao) who worked for Dupont from 1966-2002 (36 years!) pleaded guilty in Federal court on Thursday to committing espionage for a company controlled by the Chinese government. Mr. Chao testified that he provided confidential information to Chines controlled Pangang Group. What did he steal? Among other things, the recipe for Dupont's Titanium Dioxide. What is TD used in? Titanium Dioxide is the ingredient in many white products that makes the products white. Products such as paint, toothpaste, and Oreo cookie filling! Stealing the ingredients to Oreos shows just how low cyberthieves will go! According to court documents: *“DuPont's chlorine-based process was eagerly sought by China, which used a less efficient and more environmentally harmful production method”*

I have worked with a number of large companies who, when asked why they did not protect trade secrets, replied that they did not believe their industry or type of product was of interest. Make no mistake. If your company has a unique process, technology, or product, it IS of interest to many companies. Unfortunately, the US Government has released reports that state that China is sponsoring much of the US and European cyber espionage.

photo from: <http://www.titaniumexposed.com>

Share this:



Like this:



Be the first to like this.

This entry was posted in [Industry News](#), [InfoSec & Privacy](#), [Risk & Risk Management](#) and tagged [Chris Mark](#), [corporate espionage](#), [cyberespionage](#), [cybersecurity](#), [Dupont](#), [InfoSec](#), [mark consulting group](#), [San Francisco Chronicle](#), [security](#). Bookmark the [permalink](#).

Global Security, Privacy, & Risk Management

Theme: [Twenty Ten](#) Blog at [WordPress.com](#).



ADFA hack a national security failure, expert finds

December 12th, 2012 in Technology / Internet



[Enlarge](#)

Hackers have accessed personal details on thousands of Australia's future military leaders.
Credit: AAP
Image/Alan Porritt

A hacker has accessed personal details on thousands of Australia's future military leaders, a situation one expert

has described as a national security failure.

According to [media reports](#), a single hacker from the Anonymous group, calling himself Darwinare, released online the names, birthdays and passwords of 20,000 staff and students from a university database at the Australian Defence Force Academy.

The hacker is reported as saying it took three minutes and that his only motivation was boredom.

The University of New South Wales, which runs the campus, emailed all staff and students after the hack occurred on November 15 to say that identification numbers, birthdays, passwords had been stolen.

"We believe that the impact on you will be minimal," the email said.

"Email alias information may be used for targeted SPAM, phishing and other sort of email attacks on students. You should be especially vigilant in dealing with any suspicious emails."

"Student name and birthday information may be used for attempts at identity theft and again this requires additional [vigilance](#)."

A spokesperson for the Department of Defence said UNSW had taken "steps to mitigate the impact

of the data breach and reduce the possibility of further data breaches."

"The university also worked with Defence to ensure former military students and staff were made aware of the breach," the spokesperson said in an email.

Mark Gregory, Senior Lecturer in Electrical and Computer Engineering at RMIT University, described the situation as mind-boggling.

"This, in my view, is a national security failure and should be treated as such," he said.

Dr Gregory is a retired army captain and it is his own alma mater that has been hacked.

"What's even more frightening is that they have now have access to private information on the people who are going to be our future military leaders in years to come," he said.

"Defence spends vast sums protecting every aspect of the organisation. Defence contractors also spend considerable sums achieving security clearance. Yet here we have a massive security failure by an organisation that receives considerable Defence funding. For Defence not to be checking that adequate security is in place at ADFA is, in my view, something that people should face the sack for," he said.

Dr Gregory said it was not yet clear how Darwinaire accessed the database but said the hacker may have used a brute force attack, where all possibilities are systematically checked until the right password information is found.

Another possibility is that the hacker broke through the university's firewall to access the administrative system directly or access a computer that can tap into the administrative system.

"The administrative systems should only be able to be accessed on the internal network from secure private subnets and never from the external internet. The administrative systems should be partitioned off so only certain people on certain internal networks have access," said Dr Gregory, adding that the administrative systems should have required two-step authentication—such as the sms passcodes or tokens used by online banks—to verify the security clearance of everyone trying to access the system.

"For most universities and other organisations, it's standard practice that these kinds of administrative systems can't be accessed from outside even through the use of VPNs or remote control of desktops. It slows things down but it's absolutely necessary to ensure security is maintained."

Jason But from the Centre for Advanced Internet Architectures at Swinburne University of Technology said a security system is only as strong as its weakest link.

"No reports have emerged as to how the hacker has accessed the ADFA systems, so we can only speculate as to where the weak link is. It is possible that more secure systems were accessed via less secure systems where the hacker has bypassed the stronger levels of security commonly applied to shield secure systems from generic Internet access," he said.

"While I can understand the political implications, it is disturbing how much this attack is being downplayed. To claim that only historical passwords were stolen is naive in assuming that most people regularly change their passwords in a routine manner. Coupled with the fact that passwords are regularly reused across multiple systems, this list could provide an avenue of attack into

unrelated systems where users share common accounts."

The potential for identity theft was also being downplayed, Dr But said.

"The information which has been stolen can now be used to fish for further information, making ADFA users more vulnerable to future attacks. One would expect that organisations such as ADFA would have a higher priority on security of their computer and data systems."

The speed with which the hacker claimed to be able to access the data was also disturbing, he said.

Provided by The Conversation

This story is published courtesy of the The Conversation (under Creative Commons-Attribution/No derivatives).

"ADFA hack a national security failure, expert finds." December 12th, 2012. <http://phys.org/news/2012-12-adfa-hack-national-failure-expert.html>

The New York Times

March 24, 2013

Luring Young Web Warriors Is Priority. It's Also a Game.

By NICOLE PERLROTH

WASHINGTON — In the eighth grade, Arlan Jaska figured out how to write a simple script that could switch his keyboard's Caps Lock key on and off 6,000 times a minute. When friends weren't looking, he slipped his program onto their computers. It was all fun and games until the program spread to his middle school.

"They called my parents and told my dad I was hacking their computers," Mr. Jaska, 17 years old, recalled. He was grounded and got detention. And he is just the type the Department of Homeland Security is looking for.

The secretary of that agency, Janet Napolitano, knows she has a problem that will only worsen. Foreign hackers have been attacking her agency's computer systems. They have also been busy trying to siphon the nation's wealth and steal valuable trade secrets. And they have begun probing the nation's infrastructure — the power grid, and water and transportation systems.

So she needs her own hackers — 600, the agency estimates. But potential recruits with the right skills have too often been heading for business, and those who do choose government work often go to the National Security Agency, where they work on offensive digital strategies. At Homeland Security, the emphasis is on keeping hackers out, or playing defense.

"We have to show them how cool and exciting this is," said Ed Skoudis, one of the nation's top computer security trainers. "And we have to show them that applying these skills to the public sector is important."

One answer? Start young, and make it a game, even a contest.

This month, Mr. Jaska and his classmate Collin Berman took top spots at the Virginia Governor's Cup Cyber Challenge, a veritable smackdown of hacking for high school students that was the brainchild of Alan Paller, a security expert, and others in the field.

With military exercises like NetWars, the competition, the first in a series, had more the feel of a video game. Mr. Paller helped create Cyber Aces, the nonprofit group that was host of the competition, to help Homeland Security, and likens the agency's need for hackers to the

shortage of fighter pilots during World War II.

The job calls for a certain maverick attitude. “I like to break things,” Mr. Berman, 18, said. “I always want to know, ‘How can I change this so it does something else?’ ”

It’s a far different pursuit — and a higher-minded one, enlightened hackers will say — than simply defacing Web sites.

“You want people who ask: How do things work? But the very best ones turn it around,” said Mr. Paller, director of research at the SANS Institute, a computer security training organization.

It’s no coincidence that the idea of using competitions came, in part, from China, where the People’s Liberation Army runs challenges every spring to identify its next generation of digital warriors.

Tan Dailin, a graduate student, won several of the events in 2005. Soon afterward he put his skills to work and was caught breaking into the Pentagon’s network and sending reams of documents back to servers in China.

“We have no program like that in the United States — nothing,” Mr. Paller said. “No one is even teaching this in schools. If we don’t solve this problem, we’re in trouble.”

At Northern Virginia’s acclaimed Thomas Jefferson High School for Science and Technology, which both Mr. Jaska and Mr. Berman attend, there are five computer science teachers, but none focused on security.

When eight students expressed interest in starting a security club, they had to persuade a Raytheon employee to meet with them once a week. (One idea for a name, the Hacking Club, didn’t last.

“We don’t want people who are going to go around defacing sites,” Mr. Berman said. They recently rebranded from the Cybersecurity Club to the Computer Security Club. The group dropped the “Cyber” because “it sounds like you’re trying to be cool but you’re not,” clarified Mr. Jaska.)

Mr. Jaska and Mr. Berman heard about the Virginia competition through their school. To qualify, they had to identify bad passwords and clean up security settings — a long way from a Caps Lock program.

Some 700 students from 110 Virginia high schools applied, but only 40, including Mr. Jaska and Mr. Berman, made the cut.

So, three weeks ago, the pair traveled to the Governor's Cup Cyber Challenge at George Mason University.

There, they found something they rarely encounter in high school — a thriving community of like-minded teenagers, the best and brightest of a highly specialized task.

“For some of the kids, who tended to be a little bit loners, this was the first time they had a peer group,” Mr. Paller said. “They were having excited conversations about arcane technical issues — something they never get to do — and their parents exalted in it.”

The students faced the same five-level test that the military uses to test its own security experts. They earned points for cracking passwords, flagging vulnerabilities and breaking into a Web site administrator's account where, had they changed any settings or defaced a site, they would have been eliminated. Their scores were displayed in real time on a leader board.

After several hours, the winners were announced. A third of the students had made it to Level 3 — a level that Rear Adm. Gib Godwin, chairman of the Governor's Cup, said typically requires someone with seven to 10 years of experience to achieve. Mr. Jaska won, earning a \$5,000 scholarship. Mr. Berman won \$1,500 for third place.

The idea for such competitions is nothing new. For years, a hacking conference called DefCon has hosted games like Capture the Flag in which teams earn points for hacking into each other's computers. The Air Force started a Cyber Patriot competition in which hackers defend against a “Red Team” trying to steal data. And the Defense Department has its own Digital Forensics Challenge. But none of these was meant for individual high school students.

“The goal is to create a continuum, similar to the way kids go to junior high, high school, college and get their Ph.D.,” Admiral Godwin said. “We want to create the same flow for kids in the cyber domain.”

This summer, Mr. Jaska is hoping to be an intern at Northrop Grumman. Mr. Berman is considering an internship at Homeland Security. But Ms. Napolitano still has some convincing to do.

But asked about their dream job, both said they wanted to work in the private sector. “The problem with going into the government is you're going to make a lot less,” said Mr. Berman.

“Everything's slower, there's budget cuts and bureaucracy everywhere and you can't talk about what you do,” Mr. Jaska added. “It just doesn't seem like as much fun.”

This article has been revised to reflect the following correction:

Correction: April 1, 2013

Because of an editing error, an article last Monday about efforts to identify online security talent through competitions for high school hackers misstated the availability of such contests for such students. Cybersecurity competitions for teams of high school students are sponsored by the Defense Department's Digital Forensics Challenge, the Air Force Association and other cybersecurity organizations; it is not the case that no contests are available for high school students to face off against each other.

MONDAY, MAR 25, 2013 1:30 PM UTC

Government uses video games to recruit teen hackers

Taking a cue from China, U.S. agencies seek out the next generation of cyberdefense workers young

BY NATASHA LENNARD



(Credit: Shutterstock/YanLev)

It's no news that the U.S. government is targeting young hackers — but their interest is not just prosecution. As the New York Times noted Sunday, the Department of Homeland Security — following in the footsteps of the National Security Agency — is using computer game competitions to scout high-school hackers as possible recruits to their cyberdefense ranks.

The Times noted that, “the idea of using competitions came, in part, from China, where the People’s Liberation Army runs challenges every spring to identify its next generation of digital warriors.” This is just another arena in which the cat-and-mouse cyberwar between the U.S. and China

(usually with the U.S. intelligence community at the forefront) is taking shape.

Via the Times:

“We have to show them how cool and exciting this is,” said Ed Skoudis, one of the nation’s top computer security trainers. “And we have to show them that applying these skills to the public sector is important.”

One answer? Start young, and make it a game, even a contest.

This month, Mr. Jaska and his classmate Collin Berman took top spots at the Virginia Governor’s Cup Cyber Challenge, a veritable smackdown of hacking for high school students that was the brainchild of Alan Paller, a security expert, and others in the field.

With military exercises like NetWars, the competition had more the feel of a video game. Mr. Paller helped create the competition, the first in a series, to help Homeland Security, and likens the agency’s need for hackers to the shortage of fighter pilots during World War II.

The high-school hacking competitions align too with federal efforts to promote “civic hacking,” as with its upcoming Civic Hacking Day, on which technologists are invited to create public-use applications using government data. As I noted on the announcement of the June 1. National Day of Civic Hacking, such an effort, “couched in all-American rhetoric and imagery (Rosie the Riveter adorns the event Web page), sits ill at a time when the government continues to persecute hacktivists and open-data activists.” Troubling lines have been drawn: good hackers work for the government, others will be prosecuted.

Natasha Lennard is an assistant news editor at Salon, covering non-electoral politics, general news and rabble-rousing. Follow her on Twitter @natashalennard, email nlennard@salon.com.

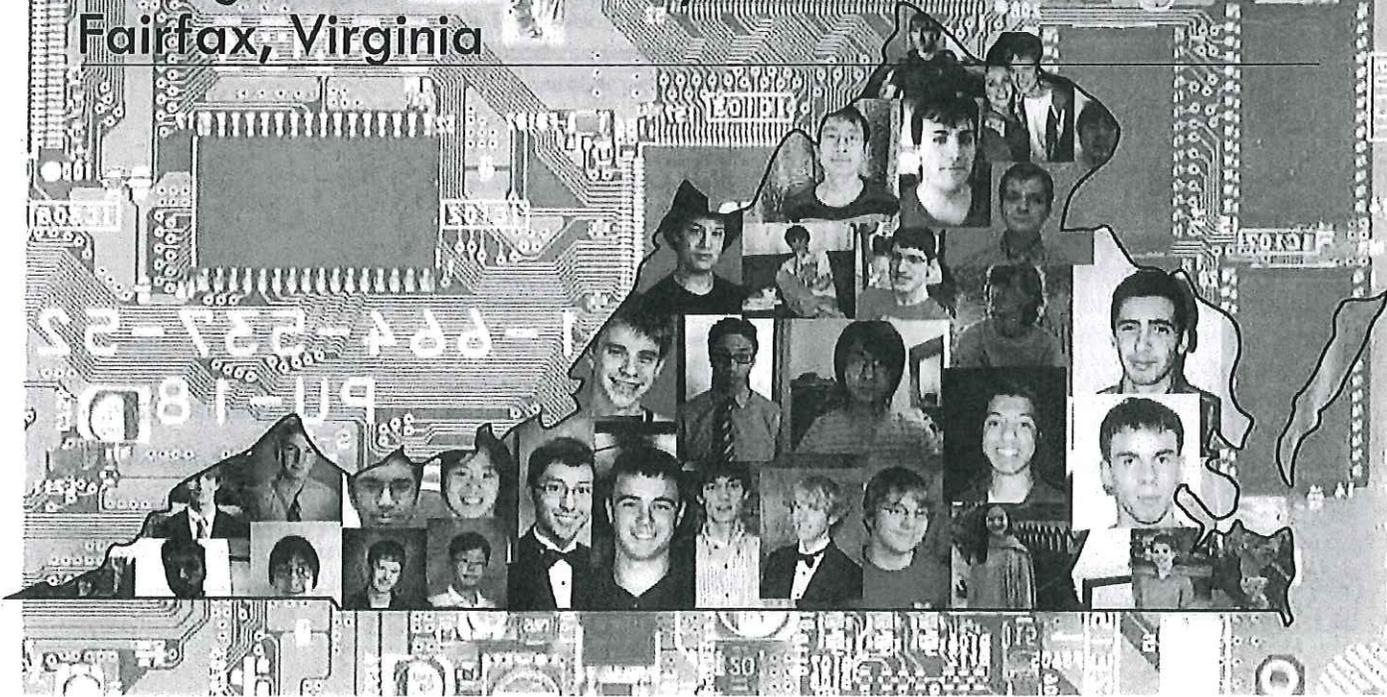
Copyright © 2011 Salon.com. All rights reserved.



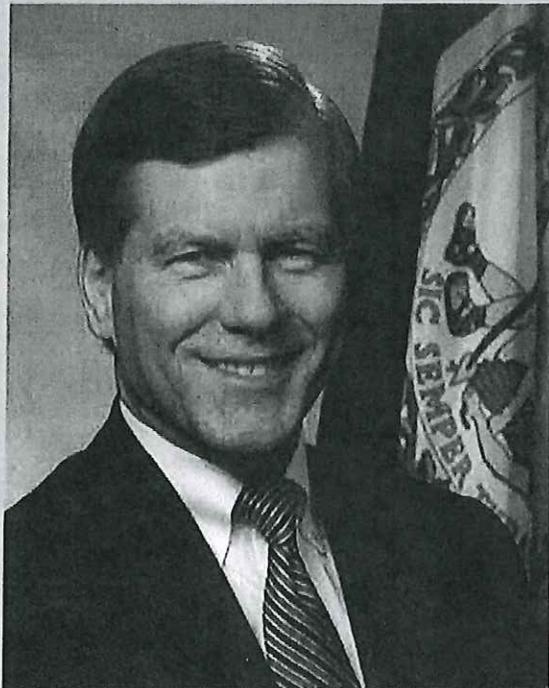
Virginia Governor's Cup Cyber Challenge

George Mason University
Fairfax, Virginia

March 1-2, 2013



Welcome to the first annual Governor's Cup Cyber Challenge!



You all should be very proud of what you have accomplished to be here. You all are the top-40 students, having competed against over 700 other Commonwealth students to earn your spots here this weekend!

I am very proud of your success and I know you all will continue to play a large role in Virginia's future!

I wish you all the best of luck this weekend!

Sincerely,
Governor Bob McDonnell

Welcome to the inaugural Virginia Governor's Cup Cyber Challenge. Congratulations to the students who've come from across the Commonwealth to compete over the next two days. Your knowledge, skills and intellect have earned you distinction as one Virginia's top talents in cybersecurity.

The mission of the Cyber Aces Foundation is to identify, enable and encourage Americans with high aptitude for technical achievement in information security to discover their talents, develop their passion and determine where their talent can be nurtured so they can make a major contribution to the physical and economic security of the United States.

The Governor's Cup Cyber Challenge will help fill the critical shortage of talent in cybersecurity. It's part competition, part conversation and part learning. We're thrilled to be in Virginia to launch our first Governor's Cup Cyber Challenge.

This event would not be possible without the generous support of Governor Robert F. McDonnell, members of his administration and members of our Virginia Advisory Committee. I'd also like to thank George Mason University for their hospitality and making the resources of this beautiful campus available. I'd like to say a special thank you to the teachers, administrators, parents, family members, and friends who volunteered their time and effort. Finally, I'd like to thank our sponsor, the SANS Institute, for their guidance and support.

Enjoy the competition.

Cordially,
David Brown
Executive Director, CyberAces

The Cyber Aces Foundation would like to thank the Virginia Governor's Cup Cyber Challenge Advisory Committee.

Mason Brown, Director, SANS Institute

Sharon Caraballo, Associate Dean for Undergraduate Programs, George Mason University

Karen Evans, National Director, US Cyber Challenge

J.B. "Gib" Godwin, Committee Chair, President, BriteWerx, Inc.

Dick Held - Society of Former FBI Agents

Cameron Kilberg, Assistant Secretary and Senior Policy Advisor, Office of Virginia's Secretary of Technology

Alan Paller, Director Research, SANS Institute

Sonny Sandelius, Cyber Aces Foundation

Ed Skoudis, Counter Hack Challenges

Tim Medin, Counter Hack Challenges
Pat Watson - Society of Former FBI Agents

Future 40

More than 700 high school students registered to be a part of the CyberAces Foundation's first ever Virginia Governor's Cup Cyber Challenge to determine the best young cyber talents in the Commonwealth. After a series of online workshops and tests, the 40 highest scoring entrants have been chosen to compete for top honors, scholarships and internships at George Mason University's Fairfax Campus on March 1 and 2. Meet these bright young minds and cyber-defenders of the future across the following seven pages.

Nathan Allen

"Just about any piece of technology" sparks Nathan's interest. The 16-year-old Emporia resident and Greensville County High junior was introduced to computers by his mother, who works as a network engineer. Nathan, who keeps his bedroom in a state of "organized chaos," says if he was stranded on a deserted island and could eat only one item, it would be rabbit.



Anirudh Bagde

"If all technology is included," the one thing 16-year-old Chantilly resident Anirudh says he couldn't live without would be "electricity." The Chantilly High School junior also says that his laptop is his most important technological possession.



Jeffrey Banghart

Jeffrey, 15, is one of two Banghart siblings in the competition. Like his brother, the Oakton High School freshman says his father is his hero in the industry, as he has exposed Jeffrey to cybersecurity since he was very young. In the future, Jeffrey says, the field needs to evolve to "focus more on prevention" to ensure people's resources remain safe.



Stephen Banghart

Stephen says his hero in the tech industry is his father, who has been working with technology since before the 18-year-old Herdon resident and Oakton High School senior was born. Stephen says the one piece of technology he couldn't live without is the microphone. "The ability to hear and store the voices of other human beings has allowed the internet to become a viable communication medium," he says.



Collin Berman

McLean local and Thomas Jefferson High School for Science and Technology (TJHSST) senior Collin, 18, got into cyber technology when he started using a Linux machine regularly. When he gets a new piece of technology, he likes to see what makes it tick - like when he got an android smartphone for Christmas and decided he needed to learn Dalvik bytecode.



Bruce Blair

Virginia Beach's Bruce, a 16-year-old junior at Princess Anne High School, has video proof of his introduction to computers - at only a few days old, his father taught him how to press buttons on the keyboard. Now, Bruce is so hooked that he sacrificed his own bedroom to convert the space to a server room/office, which now houses nine server boxes and countless video game maps and programming diagrams. He now shares a bedroom with his younger brother.



Tyler Booth

Tyler was introduced to the cyber tech industry by an uncle, who worked for the NSA. The 19-year-old Covington resident and Allegheny High School senior stresses the vulnerability the future will bring - "the more tech we install, the more holes there will be." One reason for those holes, he says, is "the human element," which is a major factor in security breaches. For this reason, he looks up to men like Dave Kennedy, founder of TrustedSEC, who try to minimize this vulnerability.



Cole Bradley

Like many teenagers, 18-year-old Cole, an Allegheny High School senior and Covington resident, spends much of his time on the internet. Unlike many, though, Cole uses the time he spends there learning and keeping up to date with the rapidly changing cyber technology field. Eventually, Cole believes, everything will be stored electronically - "from medical records to classified government documents." For this reason, he says, "the industry will be booming" for those with the know-how.



Jack Bowden

Jack became interested in cyber technology when he began to play online multiplayer video games on his PC. The 17-year-old Williamsburg resident and Bruton High School senior now uses his skills daily to design web pages, script code and operate gaming servers to play on with his friends. A rule Jack has learned to live by is to keep his laptop "in tip-top shape" at all times.



CAUTION-REPLACE IC LINKS-NO NARLES-LECTOR

SONY CXD8561HQ 1996 Sony Catalogue

SONY

Spencer Chen

Roanoke's Spencer appreciates the internet for its ability to "broaden the horizons of communication." The 16-year-old Roanoke Valley Governor's School junior also highly values efficiency, making everyday gadgets like utility knives and cell phones interesting items, in his eyes.



Selena Feng

Selena, a 14-year-old Albemarle High School Freshman, was introduced to cyber technology by the media, movies and magazine articles. The Crozet resident says she could not live without the internet, due to its wide range of applications. As the complexity of cyber-attacks increases, she says, "it will be necessary to develop more advanced technologies to protect people and information."



Corwin de Boor

Corwin is a well-rounded student. Almost everything sparks the 15-year-old Arlington local's interest, except history. The TJHSST sophomore says he could live without his technological gadgets, but getting through his classes would be very hard. While Corwin admits to not being knowledgeable enough in the cybersecurity field to know where it's headed, he does have one hope: "that it doesn't degenerate into war."



Ben Humphries

Clifton Forge's Ben is 17 years old and a senior at Allegheny High School. He wouldn't even be interested in technology if it wasn't for his iPhone. The older of two siblings, Ben is a huge Indianapolis Colts fan with a bedroom to prove it - he says it's "completely decked out in Colts stuff."



CJ Gardner

CJ says his father introduced him to computers at a very early age, beginning a lifestyle of "tinkering." Now the 17-year-old Vienna resident tests his skills at George C. Marshall High School's Cyber Security Club. Given technology's fast advancement rate, CJ believes that a large part of cybersecurity's future will deal with securing new devices.



Arlan Jaska

Because computer code is being written faster than it can be reviewed, TJHSST senior Arlan says, "numerous insecurities with software" are popping up everywhere. The 17-year-old McLean resident is interestedly awaiting Google's 'Project Glass' augmented reality head-mounted display and believes the future will bring "reduced physical interaction with computers." Instead of pushing buttons, "the computer will know what buttons we want to push."



Ryan Kelly

Fairfax Station's Ryan, 17, is the middle child in a family of three. A junior at Lake Braddock Secondary School, Ryan says he was introduced to the cybersecurity field by his programming teacher. Of all of his electronic gadgets, Ryan says the one thing he couldn't live without is his cell phone, because it connects him to all his friends.



John Kim

John, 13, was introduced to the cybersecurity field by a close friend, who he calls a "computer whiz." From there, his digital input technologies teacher at Lake Braddock Secondary School honed his interest. His true passion, however, lies in making, testing and programming robots. In the future, John hopes to see "an efficient society, not completely dependent on, but rather supplemented and facilitated by computers."



Angela Li

Angela hopes that more girls get involved with computer science. The 16-year-old Western Albemarle High School junior recently connected with a female former IBM employee who is trying to form a group for girls interested in technology in the Charlottesville region, where Angela lives. Angela is interested in apps and "would love to learn about app development."



Jack Lynch

Jack is no stranger to cyber technology competitions. The 16-year-old Vienna resident and George C. Marshall High school junior competed in Cyber Patriot IV last year, where his team made it to the national finals. Jack is interested in Smart watches, 3-D printers and virtual reality.



CAUTION-REPLACE IC LINK AS MARKED

SONY
© Sony Computer Entertainment Inc.
KDB8606Q
LFB00057
WK94589
NNG 9718 AA
HONG KONG

CCP2E50

CCP2E20 CCP2E20

-52

Nevin Mascarenhas

The youngest of three, Springfield junior Nevin is a self-starter in the information industry. "I was interested in how computers work at age 7, so I looked it up," Nevin says. Now, he relies on his HTC Vivid mobile phone to keep him connected to the technological world while on the go. In the future, Nevis says, "technology will be integrated into almost everything we do."



Dorian Nicu

Dorian, 17 and a junior at Warwick High School, says computers have held his interest since he first used one. In fact, the Newport News resident says the one piece of technology he couldn't possibly live without is his laptop, which has "everything that [he] need[s] in terms of technology." In the future, Dorian believes that things we have seen in science fiction movies will become a reality.



Andrew Pham

Andrew Pham is nothing if not practical. His favorite piece of technology, he says, is the refrigerator. Without it, he says, he "would slowly die of starvation." The 15-year-old Fairfax resident and W.T. Woodson High School sophomore first learned to program in Lua before transitioning to C and C++. Andrew is currently the lead and only programmer of his high school's robotics team.



Eric Sun

"As long as people want to get to protected data, there will always have to be new ways to defend that data," says Eric, a Springfield local and TJHSST sophomore. For this reason, he counts among his heroes in the industry "the hackers who keep finding ways around current security techniques and pushing the industry forward."



Osaze Shears

Appomattox Regional Governor's School for the Arts and Technology junior Osaze, 16, found that "computers were the coolest thing in the world" when he got his first PC in seventh grade. Osaze believes that it is our job, as a whole, to prevent attacks on the safety and security of both personal computers and world networks. When he isn't contemplating these deep issues, he enjoys Chick-fil-a's spicy chicken sandwich and "amazing lemonade."



SONY
LABORATORY
EXPERIMENTAL
@Sony.com

Nikita Torosyan

was introduced to the cyber tech industry through his father, who he calls his hero in the industry. One of three siblings from Gainesville, the Governor's School at Innovation Park junior believes that automation is the future of the industry, but remains skeptical. "In the world of actual cyber security and such, everything will become automatic and eventually every loophole will be fixed... maybe."



Mathew Velasquez

Moseley resident and Cosby High School senior Mathew, 17, is the middle child in a family of three. Above his bed hangs a large, impressionist painting of Einstein amidst his own artwork. Mathew began experimenting with computer game creation software at nine years old and quickly followed that with more general applications, such as C++ and Java. In the future, Mathew believes, "neural networks will become advanced enough to simulate computer intelligence" resulting in some "confusing ethical dilemmas about what constitutes sapience."



Zach Wade

As more and more of our computing and lives move to the cloud, 16-year-old TJHSST sophomore Zach says, hackers will soon be "capable of destroying a person's entire life," making the future of cybersecurity incredibly important. Zach is a "huge fan of Google" and is interested in project ranging from Google Glass to Leap Motion.



Brandon Walker

"Doing robotics after school has really pushed me to begin working with the hardware aspects of computing," 14-year-old Forest Park High School freshman Brandon says. He also says he would be at a "great loss" without his phone, as the accessibility and creativity a hand-held provides is amazing. The Woodbridge resident lists "the many that make up the communities and develop open-sourced ideas" as his heroes.



SONY
OX18555
1998 Sony Corp
Entertainment
JANU 9712

SONY
© Sony Computer
Entertainment Inc.
CXDB606Q
L9B0057
WK94589
NNG 9718 AA
HONG KONG

CAUTION-REPLACE LINK-95 MARKER

CCP2E20

CCP2E20 CCP2E20

Eric Wang

Eric, a Lake Braddock Secondary School eighth grader, was introduced to cyber technology at the age of seven, when his father showed him how to make a program on C#.net. For this reason, the 14-year-old calls his father his hero in the industry. When he isn't on his computer doing homework, chatting with my friends, playing games, watching videos or programming, he is practicing on the piano in his room.



Caleb Webber

Currently a junior at Prince George High School, Caleb got into programming and social engineering in the eighth grade. Starting with Visual Basic, Caleb quickly turned to Python and now studies Java and C++. Caleb is deeply interested in both cybersecurity and programming and lists Kevin Mitnick, Dennis Ritchie, Aaron Swartz and Linus Torvalds among his industry heroes.



Chris Yi

"We, as a nation and relative to other nations, are moving forward too slowly" in terms of cyber security, the Woodbridge resident and Forest Park High School senior says. In the future, the 18 year old pessimistically believes, the U.S. may end up outsourcing these important positions to others countries, who are "leagues ahead of the United States in terms of technological advancement."



David Young

A self-starter in the cyber tech field, the Forest Park High School senior says he picked up the hobby while "bored one summer." The 17-year-old Dumfries resident enjoys video games and programming and believes one day, artificial intelligence will "make technology jobs that deal with menial tasks obsolete."

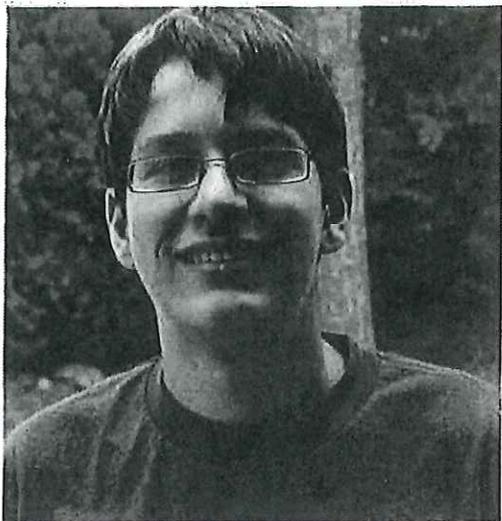


Justin Yirka

Justin, a junior at Garfield Senior High School, believes the future of the cyber technology industry is "impossible to predict," though it's sure to be "amazing." While his interest in computers has grown over time and he could not live without his laptop, Justin also enjoys building model rockets and playing paintball.



Choosing not to respond to the provided questionnaire were Caleb Spence, Geordon Worley, Joseph Mehl, Weyland Chiang, Jacob Jernigan, Kashish Jagga and Joshua Geise.

**Caleb Spence,**

A sophomore at Appomattox Regional Governor's School, has learned his impressive cyber skills from reading Bruce Schneier's blog, watching DEFCON videos, and engaging his school's IT department. He believes user education is an important topic that needs to be addressed to strengthen our nation's cyber security.