Los Angeles Times

Cyber security run amok

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

By The Times editorial board

March 28, 2013

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.

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 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.

techdirt

Rather Than Fix The CFAA, House Judiciary Committee Planning To Make It Worse... Way Worse

by Mike Masnick, Mon, Mar 25th 2013

So, you know all that talk about things like **Aaron's Law** and how Congress needs to **fix** the CFAA? Apparently, the House Judiciary Committee has decided to raise a giant middle finger to folks who are concerned about abuses of the CFAA. Over the weekend, they began circulating a "draft" of a "cyber-security" bill that is so bad that it almost feels like the Judiciary Committee is doing it on purpose as a dig at online activists who have fought back against things like SOPA, CISPA and the CFAA. Rather than fix the CFAA, it expands it. Rather than rein in the worst parts of the bill, it makes them worse. And, from what we've heard, the goal is to try to push this through quickly, with a big effort underway for a "cyberweek" in the middle of April that will force through a bunch of related bills. You can **see the draft of the bill here** (or embedded below. Let's go through some of the pieces.

Adds computer crimes as a form of racketeering

The bill adds to the current **definition of "racketeering activity"** so that it would now link back to the CFAA, such that if you are found to violate the CFAA as part of an activity that involves a variety of other crimes, you can now *also* be charged with racketeering. More specifically, if you look at that long list of related statutes in the definition to 18 USC 1961 (1), it will also include: "'section 1030 (relating to fraud and related activity in connection with computers)." Basically, this just gives the DOJ yet another tool to use against "computer criminals" when they want to bring the hammer down on someone they don't like. Not only could you be charged with computer fraud, but now racketeering as well. Because, you know, all you hackers are just like the Mob.

Expanding the ways in which you could be guilty of the CFAA -- including making you just as guilty if you plan to "violate" the CFAA than if you actually did so

Section 103 of the proposed bill makes a bunch of "changes" to the CFAA, almost all of which*expand* the CFAA, rather than limit it. For example, they make a small change to subsection (b) in**18 USC 1030** (the CFAA) such that it will now read:

Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided for the completed offense in subsection (c) of this section.

All they did was add the "for the completed offense," to that sentence. That may seem like a minor change at first, but it would now mean that they can claim that anyone who talked about doing something ("conspires to commit") that violates the CFAA *shall* now be punished the same as if they had "completed" the offense. And, considering just how broad the CFAA is,

think about how ridiculous that might become. Now if you talk with others about the possibility of violating a terms of service -- say, talking to your 12 year old child about helping them sign up for Facebook even though the site requires you to be 13 -- you may have *already* committed a felony that can get you years in jail. That seems fair, right?

Ratchets up many of the punishments

They change around a bunch of the "penalties" that you can get for various CFAA infractions, shaking up a variety of things and basically raising the maximum sentences available for certain infractions.

A very, very minor adjustment to limit "exceeding authorized access."

~~This one is a very, very tiny step in the right direction, but just barely. Under the old CFAA, "accessing a computer without authorization" and "exceeding authorized access" were lumped together as a a form of breaking the law. The new bill keeps the basic terms of accessing a computer without authorization the same and just ever so slightly trims back the "crime" of exceeding authorized access. Now, to violate the law by "exceeding" authorized access, you'd have to get access to "information from any protected computer" (or financial institution or US gov't agency)~~ **~~and~~** ~~the "value" of that info would need to be over $5,000 (who determines that?)~~ **~~and~~** ~~the access had to have been "committed for purposes of obtaining sensitive or non-public information of an entity or another individual (including such information in 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"~~ **~~and~~** ~~was committed "in furtherance of any criminal act."~~

~~While it's good to see them ever so slightly roll back the issue of "exceeding authorized access," it still seems broad enough that all sorts of activities that shouldn't be seen as criminal would easily get lumped in here by aggressive prosecutors.~~ Rather than "streamlining" the bill and getting rid of the ridiculous "exceeds authorized access" trigger -- as folks like **Orin Kerr have suggested** -- this tends to just muddle matters even more.

Update*: On second look, it turns out that this initial analysis was wrong. This part is worse too! More* ***details here****, but basically all those "and" statements are actually "or" which actually push back on how the courts have interpreted the CFAA... and make it worse*

And... at the same time, they do something else to make "exceeding unauthorized access" worse. Which brings us to:

Expanding **the definition of "exceeding authorized access" in a very dangerous way**

That's because the new bill says that you can exceed authorized access: "even if the accesser may be entitled to obtain or alter the same information in the computer for other purposes." Yes, read that again. Even if you are *allowed* to obtain info via your authorization on your computer, they're now saying that if you use that information in a way that runs afoul of the info above, you can be found to have exceeded authorized access.

Make it easier for the federal government to seize and forfeit anything

We've seen how federal seizure and forfeiture laws are frequently abused to seize goods, which the government claims are used in the commission of a crime (even if they never charge anyone for the crime). And we've seen, with cases like the **Dajaz1 case**, how the government will use such tools to take and censor websites on no actual basis. And now the CFAA will make it even easier for the government to do such things. It amends the existing sections to basically expand what can be forfeited, because it's not like the government hasn't abused that one before...

The rest of the bill deals with two other things: first a section on "cybersecurity" which includes punishment for those damaging "critical infrastructure" computers, another section that tells the courts to figure out how secure their computers are, and finally a part that creates a "National Cyber Investigative Joint Task Force," to be led by the FBI, because they're an unbiased party.

The final part of the bill relates to "breach notifications." A number of states already have various laws in place that require companies and websites that have data breaches to inform impacted users. This creates a federal law that supersedes those state laws. You can read the details, but basically companies will have to let people (and other companies) know of such breaches within a short period of time -- unless there are law enforcement or national security reasons to delay such notification. It also requires companies to tell the FBI or Secret Service of certain kinds of breaches. If companies *don't* do this, they can be fined between $500,000 and $1 million -- but only by the DOJ (i.e., individuals or companies can't go after organizations for screwing this up).

Those last two sections are really somewhat unrelated to the rest of the CFAA parts. But the CFAA parts are troubling. Rather than fixing the law, they're expanding it so that computer "crimes" can be hit with racketeering charges, and expanding the general language and punishments for part of the bill. This is not a good thing. The fact that this is being passed around by the House Judiciary Committee suggests that it's likely to be backed by HJC chair Bob Goodlatte, which is unfortunate. You would have hoped that Goodlatte and others on the HJC would recognize that now is the time to fix the CFAA, not to make it worse.

The Volokh Conspiracy

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

Orin Kerr • March 25, 2013 5:30 pm

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.

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 authorziation."

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.

House Judiciary Committee's Draft Computer Crime Bill Rehashes Old Proposals, Makes them Worse

by Andrew McDiarmid

March 27, 2013

The House Judiciary committee is reportedly circulating a discussion draft that would amend the Computer Fraud and Abuse Act (CFAA) in precisely the wrong direction.

In the wake of the tragic death of activist Aaron Swartz, US Internet freedom advocates have devoted much time and energy to pushing sensible reforms to narrow the scope of the CFAA, under which Swartz was being aggressively prosecuted at the time of his death. This draft flies in the face of those efforts, as it would dramatically enhance the already heavy penalties for violations of what Internet scholar Tim Wu recently called "the Worst Law in Technology," while appearing to expressly overturn existing case law to say that violating terms of service or other agreements can indeed be prosecuted as a felony.
Orin Kerr at the Volokh Conspiracy points out that much of the proposal is a rehash of 2011 Administration recommendations to expand the law and criticizes the breadth of the draft's treatment of what it means to "exceed authorize access" to a computer.
Mike Masnick at Techdirt, another vocal critic of the law and how it has been prosecuted, put up a post on Monday that walks through the draft's problems, and noted conservative security policy expert Paul Rosenzweig has blogged critically about the draft at Lawfare, noting that it "seems to answer most of what the Department of Justice wants with very little for the Internet online community in return."

One dangerous addition to the proposal since similar language was last introduced by Senator Patrick Leahy last summer is the stark reversal of language first introduced by Senators Grassley, Franken, and Lee to greatly limit the law's application to terms-of-service and other contractual violations. In place of that language, the current House draft says that a person can exceed authorized access in violation of the statute "even if the accesser may be entitled to obtain or alter the same information in the computer for other purposes." This is in direct conflict with current case law on ToS violations and the CFAA, and is especially shocking in light of the longstanding bipartisan effort to get ToS violations out of the statute once and for all.

As CDT wrote in its analysis of the initial White House proposal in 2011, it does not make sense to consider expanding and enhancing penalties under the CFAA without first sensibly narrowing its scope, lest every American on the Internet risk felony charges for even minor ToS violations.

Indeed, given the heavy penalties already possible under existing law, there are plenty of reasons to question whether penalty-enhancement is necessary at all.

Representative Lofgren's office has been working with a coalition of groups including CDT, EFF, ACLU, and the Reddit community to develop just such a proposal to narrow the scope of the CFAA. We are hopeful that her work and that of the Internet advocacy community will convince the Committee to stop and rethink its approach, since the bill it is floating is exactly the opposite of the computer crime bill that we need right now.

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

Congress' New CFAA Draft Could Have Put Aaron Swartz in Jail For Decades Longer Than the Original Charges

MARCH 27, 2013 | BY TREVOR TIMM

Law professor and historian Tim Wu has called the Computer Fraud and Abuse Act (CFAA) the "worst law in technology." The Ninth Circuit Court of Appeals has described the government's interpretation of it "expansive," "broad," and "sweeping." And Orin Kerr, former federal prosecutor and law professor, has detailed how the government could use it to put "any Internet user they want [in jail]."

So it's pretty surprising to see that now, instead of reining in the CFAA's dangerous reach, the House Judiciary Committee is floating a proposal to dramatically *expand* it and is reportedly planning to rush it to the floor of Congress during its April "cyber" week.

The CFAA, of course, is also the computer trespass law that prosecutors misused to hound the late activist and Internet pioneer Aaron Swartz. Aaron's tragic death resulted in outrage across the political spectrum and led to calls for real reform that would bring the law back to its reasonable purpose of criminalizing malicious computer intrusions, rather than handing out draconian penalties for minor infractions and turning terms of service violations into criminal acts.

So why is the House Judiciary Committee floating a proposal that goes so clearly against the public opinion? Their reasoning is almost hard to fathom.

Techdirt's Mike Masnick posted a new draft and analysis of the CFAA expansion bill on Monday. The changes are nothing short of outrageous and should brand supporters in Congress as out of touch and downright hostile to the Internet. Users concerned about Internet rights should contact their representatives immediately.

Perhaps the most disturbing aspect: instead of reducing the penalties for crimes that don't cause much economic damage, it dramatically increases them. For example, Aaron faced four charges under section (a)(4) of the CFAA, which had a maximum sentence of five years each. EFF, Orin Kerr and many others have proposed removing (a)(4) entirely since it creates double penalties for the same behavior criminalized elsewhere in the law. What does the new draft do? It increases the maximum under (a)(4) to twenty years *for each charge*. As Internet law scholar James Grimmelmann remarked Monday, the thought of Aaron facing *more* time is "simply obscene."

The new draft also now turns CFAA violations into a “racketeering” offense, adding yet another layer of charges the DOJ can add to the charge sheet of a hacker it doesn’t like. It also adds a broad conspiracy charge that carries the same penalty for actually committing an offense. Essentially, *talking* about committing computer crimes without actually doing so can land you in prison.

Most troublingly for innovation and for user empowerment, the bill “clarifies” its definition of “exceeding authorized access” to include accessing information for an “impermissible purpose”—even if you have permission to access the information in the first place. That codifies the misguided idea that any terms of service violation is indeed a crime, effectively undoing good rulings in the 9th and 4th Circuits.

The CFAA already reaches computer intrusions, serious denial of service attacks, password misuse and attacks on national security computers. Those provisions are important. The Department of Justice has more than enough tools it needs to go after real criminals using this law and a host of others—including criminal copyright, trade secrets, identity theft and other laws. It should use those tools rather than coming back to Congress for more, especially now that it's just been caught misusing the law so egregiously in Aaron’s case.

Quite simply, this bill is a nightmare for Internet users' rights. That the House Judiciary Committee would introduce it in the wake of Aaron’s death demonstrates just how out of step they are.

Law professor Orin Kerr agrees, concluding the proposed bill’s language is a “a step backward, not a step forward” and says its meant “to give DOJ what it wants, not to amend the CFAA in a way that would narrow it.”

One thing is clear: Congress is not going to fix the CFAA without an enormous, sustained effort from regular folks to implore them to fix it. In fact, this proposal shows that if we stand silent, they are likely to make it worse. Let’s remind Congress about the last time they decided to go against the wishes of Internet users across the country—CFAA could be SOPA II.

Call your member of Congress and tell them that representing **you** means that they will work to fix the CFAA, not make it worse. Tell them that the CFAA already carries incredibly harsh penalties for conduct that would be considered a minor crime, or no crime *at all,* in the physical world. Tell them that the law meant for real criminals, should not also engulf activists, security researchers, innovators, and entrepreneurs.

In the name of Aaron—and the next person to face an overreaching prosecutor harboring a grudge—implore them to fix the CFAA.

For Immediate Release: **Contact:** Nathan White (269)267-0580

Egregious DOJ Overreach Underscores Urgent Need for Reform of Computer Laws

Washington D.C. (March 19, 2013) – As more of America's activists and innovators face harsh prison sentences, David Segal, Executive Director of Demand Progress, today called upon Congress to take swift action to amend a decades-old law which criminalizes routine computer use. The Computer Fraud and Abuse Act (CFAA) was written in 1984 and as applied today would have put Bill Gates and Steve Jobs in jail for their innovation.

"The Computer Fraud and Abuse Act, as it exists today, could be used to arrest almost anyone who uses a computer in the United States. Check your personal email on your work computer and you become a felon," said David Segal.

George Washington Law Professor Orin Kerr recently testified before Congress that the law is so vague it may be unconstitutional; myriad other legal scholars concur. Officials with the Department of Justice (DOJ) have countered that the law is only used to prosecute egregious violations. However, recent prosecutions conducted by the Department of Justice prove otherwise. Increasingly the law is used to bully computer users for minor infractions.

- Aaron Swartz, a widely-respected computer programmer and political activist, faced up to more than 35 years in prison for allegedly violating the CFAA. Prosecution alleged that Swartz illegally downloaded academic articles from JSTOR on MIT's campus by using a computer program to automate the downloading process. Critics have accused the Department of Justice of prosecuting Swartz for the equivalent of checking too many books out of the library. Swartz had a legal right to access JSTOR documents and JSTOR declined to participate in Swartz's prosecution. After two years of being denied his right to defend himself in court, Swartz took his own life on January 11, 2013.

- Yesterday, a 26-year-old computer user was sentenced to 41 months of prison time plus three years of supervised release for revealing a privacy vulnerability in a widely used consumer product. Andrew Auernheimer was charged with identity fraud and accessing a computer without authorization. The penalty means that a bright, young mind will forever be identified as a criminal. His prosecution has also chilled the software development community who saw his actions as routine security research.

- Mathew Keys, a Reuters deputy social media editor, is another 26-year-old with a bright future being stymied by overzealous enforcement of an out-of-date law. Keys recently provided a username and password for the purposes of cyber graffiti. Individuals used the unauthorized access to change the title of a Reuters headline for about an hour. For this infraction, Keys is facing penalties up to $250,000 and five to ten years in prison.

"A clear pattern is emerging as more people pay attention to the DOJ's use and abuse of the CFAA in the wake of Aaron's suicide. Some of these prosecutions should never have been allowed to move forward, while others demonstrate egregious disproportionality between the alleged crime and the punishment being sought. DOJ has made it clear that it can't control itself: It's time for Congress to rein them in," said David Segal.

###

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.