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 you in your effort 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.

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 crime laws like the CFAA when they were young, simply for doing what innovators do: pushing

---

[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).

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,

Mozilla
Internet Infrastructure Coalition (i2Coalition)
Engine Advocacy
Union Square Ventures
O'Reilly Media
Reddit
OpenDNS
Stack Exchange
PadMapper
Floor64
ThoughtWorks
heyzap
Agile Learning Labs
Vuze
#sfbeta
Apportable
Safe Shepard
Framebase
Newsblur
MixRank
Segment.io
ZeroCater
Vidmaker

---

[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.

4Chan
Canvas
Notcot Inc.
The Lewis Charitable Foundation
Get Satisfaction
VigLink
Zemamai
American Library Association
Cheezburger Network
Sibylus Inc. (Rentobo)
Statwing

cc: Members of the House Committee on the Judiciary
*Last updated May 18, 2013