The CFAA: Blocking Competition and Stifling Innovation

- Imagine a tool that lets you view, manage, and use all of your social networks in one screen, avoiding the need to shift from one to the other or the need to check whether you're connected via Facebook, Twitter, or Google+. With your approval, the tool logs you in to your various social networks, seamlessly connects them, and keeps the ads intact. Great innovation, huh? The fact that so many people are working to create novel tools that help us better navigate and live our digital world is what makes the Internet so great.

  But the CFAA, along with similar state computer crime laws, stands as a barrier to such smart innovation. How do we know? It happened.[1] First, the social network argued in court that by allowing users to automate their access, the tool violated its terms of use. With EFF's help, that claim was rejected, but the social network then noted that it had tried to stop the tool by blocking the IP address it came from. The toolmaker, trying to continue to provide his service, jumped to a new IP address to avoid the block. The social network argued, successfully, that moving to a new IP address violated computer crime laws.

  The result? You're not using the tool described above, are you? Innovation lost.

- Imagine a tool that let you automatically place apartment ads from numerous classified ad websites onto an interactive map. That way, you can tell if the "amazing view" is actually looking down on the city dump, or if the Dupont Circle address is actually in outer Georgetown. Again, the CFAA stands in the in two ways.[2] The classified ad website has terms of service that prevent redisplaying content. And if the service tried to avoid a technical block, the CFAA would come into play again.

  The result? You have to hand map each address into a map service, or drive around yourself to find out where the location actually is. Innovation lost again.

- Imagine a mobile app that let you sign in to your accounts on various websites without having to type on the tiny keyboard or navigate a form not designed to render on smaller screens. What a relief! But many websites prevent automated logins both through contractual terms and through technical blocks.

  The result? More squinting, scrolling and typing for you on the tiny device.

- Imagine a tool that allows you to send and receive messages with any of your social networking

[1] 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 try to prosecute the same claim.

[2] http://gigaom.com/2012/07/24/craigslist-sues-competitor-padmapper-over-listings/

friends through a single interface of your choice, rather than having to separately check your messages on gMail, Twitter DM and Facebook Messages. This tool is still a pipe dream, in part because Facebook and Google are battling over your ability to aggregate your contact information into the platform of your choosing.

Facebook started the battle by restricting Google's efforts to import your Friends' addresses into gMail. In return, Google blocked Facebook from using the gMail API to download Google contacts. Facebook then hacked around that restriction by giving users a direct deep link to the download feature. Google responded by saying it was disappointed that Facebook doesn't let its users move their data into Google products. This is a competitive battle, but not one in which the force of federal criminal law has a role. Yet, the CFAA would allow either Google or Facebook to strike back legally, suing the other party for unauthorized access to the other's networks by accessing and exporting user data, even at the user's behest. Facebook could sue Google for trying to scrape your Friends' data, and Google could sue Facebook for hacking around its API block. The existence of the CFAA is a heavy hammer that interferes with healthy competition that keeps companies evolving, and innovating in the user's best interest.

These are just four examples, yet versions of them have occurred over the past couple of years. And it's not counting the innovations that failed to happen once the developers learned of a potential CFAA risk. By blindly handing a sledgehammer of criminal law to violations of terms of use or minor technical workarounds serves as a block on competition and stifles innovation.

The law should support innovation through reverse engineering and interoperability, not hinder it. The law does help in other areas:

- In a series of cases, arising out of computer games and consoles, the courts recognize that the copying of code necessary to build an interoperable computer program constitutes a fair use under copyright law. These cases blocked attempts by companies like Sony and Sega to stop competitors from building interoperable games and consoles.

- Similarly, the DMCA anticircumvention provisions have a specific exception for interoperable programs, 1201(f), which allows reverse engineering even if it circumvents a technological protection measure protecting a copyrighted work. It's not perfect, but it represents Congressional recognition that technological locks can be misused for anticompetitive purposes and the stifling of innovative market ideas.

Computer trespass law should stop computer intrusions, not innovation.