In Memory of Aaron Swartz: Reboot Draconian Computer Crime Law

In the wake of social justice activist Aaron Swartz’s tragic death, EFF has been working with a coalition of legislative staffers and experts on the Computer Fraud and Abuse Act (CFAA), the infamously problematic U.S. anti-hacking law, to finalize a proposal for changes that would make major improvements to it. We've written a series of blogposts outlining our ideas as they’ve developed and expanded upon Rep. Zoe Lofgren’s terrific start for Aaron’s Law. Below we outline three critical fixes for the CFAA that must be addressed immediately.

No Criminal Exposure for Violating Private Agreements or Duties

Violations of contractual obligations like a website's terms of service must not be the basis for criminal charges. The original "Aaron’s Law" proposal from Rep. Zoe Lofgren focused exclusively on this issue, and was based on a bi-partisan bill first introduced by Senators Franken, Lee and Grassley. In two recent cases, federal circuit courts have decided that simple violations of computer use policies and duties of loyalty are not criminal activities. Rep. Lofgren has asked for those holdings to be codified into law, and we agree.

Put simply, there should be no criminal penalties for violating the fine print written by a website or service. Users may face civil liability for violating those terms, or even criminal liability if they go on to do worse things like destroy data. But it is dangerous for a private one-sided contract to be enforceable upon punishment of severe criminal penalties at a prosecutor’s whim.

If You’re Allowed to Access Information, Doing it in an Innovative Way Shouldn't Be a Crime

As the CFAA is written today, users can expose themselves to criminal liability if they are authorized to access data, but do so while engaging in commonplace "circumvention" techniques like changing IP addresses, MAC addresses, or browser User Agent headers. But these "circumvention" activities can have great benefits: they can help protect privacy, ensure anonymity, and aid in testing security. Furthermore, technical barriers are sometimes put into place not to protect data or computers from intrusion at all. Quite often they are an accidental result of misconfigured servers or network equipment.1

Apart from these accidents, technological barriers increasingly serve purposes far removed from preventing computer intrusion, such as giving people in one location a better price than people in another and blocking competitors from seeing information otherwise available to the general public. EFF’s proposal would clarify that if access to data is already authorized, gaining that access in a novel or automated way is not a crime.

(Continued on reverse)
Make Penalties Proportionate to Offenses

As a general principle, minor violations of the CFAA should be punishable with minor penalties. As the law is currently written, first-time offenses can be too easily charged as felonies instead of misdemeanors. Our proposal would fix that.

Furthermore, several sections of the CFAA are redundant with other parts of the law, which lets prosecutors "double dip" to pursue multiple offenses based on the same behavior. And the stiff penalties for "repeat" offenses can be used to dole out harsher punishment for multiple convictions based on the same conduct. Our proposal would ensure that prosecutors can't count the same actions more than once to ratchet up the pressure for a plea bargain by threatening a defendant with decades of jail time.

We encourage you to take action today.

Tell Congress that we need to fix computer crime law at eff.org/Aarons-Law or scan the QR code to go directly to EFF’s Action Center tool.

Learn more about EFF’s CFAA reform proposals at eff.org/CFAA.