ELECTRONIC FRONTIER FOUNDATION
PROTECTING RIGHTS AND DEFENDING FREEDOM ON THE ELECTRONIC FRONTIER eff.org

Coders' Rights Project

EFF’s Coders’ Rights Project protects the efforts of programmers and developers engaged in cutting-edge exploration of technology in our world. The work of security and encryption researchers is critical for a safer future, yet many legitimate practitioners face challenges under the Digital Millennium Copyright Act (DMCA), the Computer Fraud and Abuse Act (CFAA), and other computer crime laws from around the world. With education, legal work, and involvement in the community, the Coders’ Rights Project builds upon EFF’s work protecting innovation and the rights of curious tinkerers and hackers pioneering on the digital frontier.

Recent Developments

Defending Against Forced Decryption

Forcing individuals to decrypt the contents of computers can be a violation of Fifth Amendment protections against being compelled to provide testimony against oneself. EFF has filed several amicus briefs explaining this principle to courts, including numerous federal courts and the Supreme Judicial Court of Massachusetts. In these cases, law enforcement sought a court order requiring a suspect to decrypt seized storage and hard drives. We’ve explained that, in the absence of any additional information that shows the suspect had access to and control of the drives and the content inside, the Fifth Amendment protects the suspect from decrypting. In 2012, EFF scored a significant victory when a federal appeals court agreed with us and found a Florida man's constitutional rights were violated when he was imprisoned for refusing to decrypt data on several devices.

Fighting the CFAA in Court

EFF defended Andrew “weev” Auernheimer on appeal, after he was sentenced to 41 months in federal prison in March of 2013 for revealing to media outlets that AT&T had configured its servers to allow the harvesting of iPad owners’ unsecured email addresses. In our brief, we pointed out the multitude of flaws with the case, from the fact that certain “violations” were double-counted to the fact that accessing data on a publicly available site should not be a crime. The CFAA, the United States’ problematic ‘anti-hacking’ law, allows for overly-broad prosecutions and disproportionate penalties, and we hope our legal challenge will help roll back some of its breadth. In 2014, the appeals court found that Auernheimer should not have been prosecuted in New Jersey and overturned his conviction, but did not reach the CFAA issue.

Learn about coders' rights at eff.org/coders

Fighting the CFAA in Congress

EFF isn't just fighting the CFAA in court, though. We have continued to lead a coalition of concerned individuals, organizations, and companies pushing for serious reform. This has included marshaling supporters from tech companies to law professors to researchers explaining how chilling and dangerous the CFAA is. We've previously supported "Aaron's Law," a bill in honor of Aaron Swartz seeking to fix some of the over-criminalization problems with the CFAA, and have pushed for other key reforms. Currently, we are very concerned about the White House's CFAA "modernization" proposals that could actually dramatically increase the scope of CFAA liability and ratchet up penalties for violation. Our coalition stands ready to defeat these misguided proposals if they reach the floor of Congress.

Coders' Rights Around the World

EFF works to defend coders all over the world, urging policymakers not to create legal woes for researchers who expose security flaws. EFF has submitted comments to the European Parliament asking them not to criminalize tools, leave room for unauthorized access for security testing, and protect coders' rights to free expression, and has been closely monitoring legislation in response to the Convention on Cybercrime. EFF is also working to make sure that the United States' implementation of the Wassenaar Arrangement does not impair security researchers' work by controlling the export of the tools they use to do their research or the free flow of information needed to keep the Internet safe.

EFF Resources

Reverse Engineering FAQ

People have always explored and modified the technologies in their lives, and reverse engineering is one expression of this tinkering impulse. Unfortunately, legal regulation of reverse engineering can impact the "freedom to tinker" in a variety of ways. The Reverse Engineering FAQ sets forth some ways that coders can reduce their legal risk. **eff.org/issues/reverse-engineering-faq**

Vulnerability Reporting FAQ

There are many outlets for publicly reporting vulnerabilities, including mailing lists supported by universities and the government. Unfortunately, researchers have received legal threats from vendors and government agencies seeking to stop publication of vulnerability information or "proof of concept" code demonstrating the flaw. The Vulnerability Reporting FAQ sets forth some ways that security researchers can reduce their legal risk when reporting vulnerabilities. **eff.org/vulnerability-reporting-faq**

Grey Hat Guide

A computer security researcher who has inadvertently violated the law during the course of her investigation faces a dilemma when thinking about whether to notify a company about a problem she discovered in one of the company's products. By reporting the security flaw, the researcher reveals that she may have committed unlawful activity, yet withholding information means a potentially serious security flaw may go unremedied. While there are no easy answers for the ethical hacker who has wandered off the straight and narrow into the legal thicket of computer offense laws, EFF's Grey Hat Guide provides useful information on preventing legal troubles arising from security research. **eff.org/grey-hat-guide**