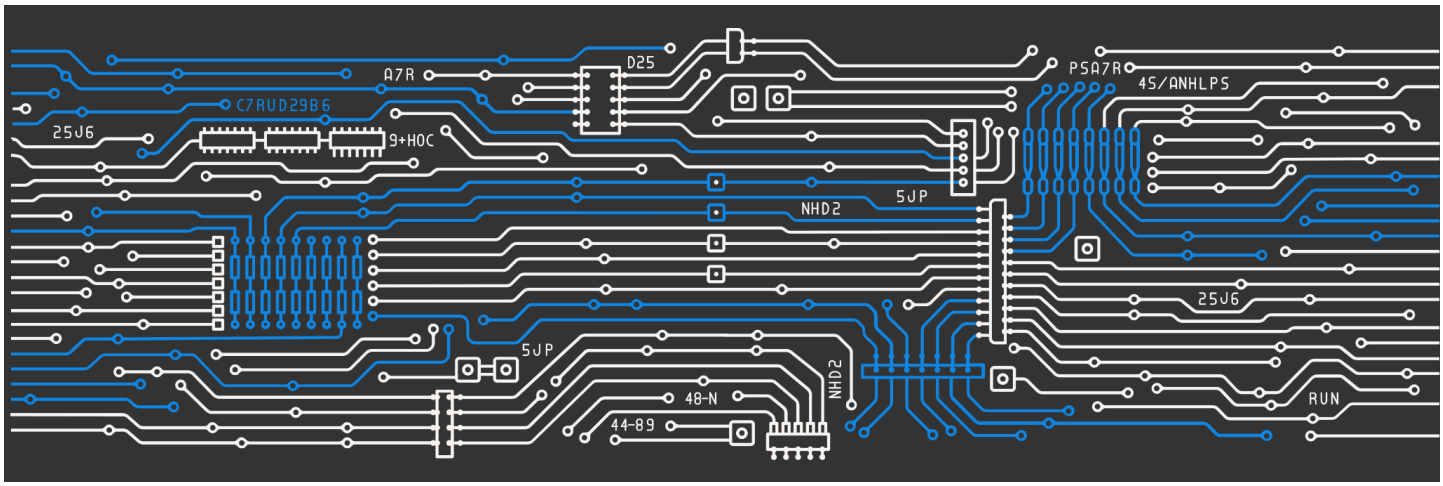
OPEN TECHNOLOGY INSTITUTE

Cybersecurity Research Should Not Be a Crime

Nat Meysenburg



The exponential growth of both cyber attacks and the number of connected devices illustrates two trends. There are already a lot of vulnerable pieces of tech out there, and with so much new tech it is likely that more vulnerabilities are introduced every day. Understanding the scope of current cyber threats will require vulnerability research on all manner of connected tech. Growth in the number of researchers in the field is currently held back by fears of civil liability and felony prosecution rooted in the Computer Fraud and Abuse Act of 1986 (CFAA) and the Digital Millennium Copyright Act (DMCA)—a pair of tech laws written in the 1980s and 90s.

Unambiguous protections for good-faith security research are needed. Congress must take legislative action, updating federal law to expand protections and clarify protections for good-faith security research.

Congress must update the Digital Millennium Copyright Act to create a permanent exemption for legitimate security research. Section 1201 of the Digital Millennium Copyright Act creates the existing process for requesting and granting temporary exemptions every three years. This section should be rewritten to create a research exemption that is clear, robust, and permanent.

Congress must update the Computer Fraud and Abuse Act to create a permanent exemption for legitimate security research. The Computer Fraud and Abuse Act should similarly be updated to include a clear and permanent exemption for those engaged in good-faith security research.

Congress must update the Computer Fraud and Abuse Act to have a more clear test for civil claims. Under the current law, a company can sue someone based on an alleged CFAA violation in the absence of that alleged violation being criminally prosecuted and only having to claim five-thousand dollars worth of damage. The law should be updated in a way that leaves a right to civil action but clarifies the collection of harms required to constitute a valid civil claim.

The Government should increase the speed at which it sets up vulnerability disclosure programs, and make them visible. Many formal vulnerability disclosure programs have been implemented by government agencies, including 18f, and CISA, who mandated that agencies begin setting them up. These processes create avenues for researchers to responsibly disclose any vulnerabilities they might find in public-facing government tech. As CISA noted in its directive: "Vulnerability disclosure policies enhance the resiliency of the government's online services by encouraging meaningful collaboration between federal agencies and the public." Expanding the use of such programs, and making them easy to find and understand, would serve as a model for how such programs could work at other levels of government, as well as at companies and other organizations.

The Government should incentivize more companies to implement their own responsible disclosure programs. When companies create programs that allow researchers to conduct good-faith research and create avenues for them to disclose their findings, they are able to benefit from the talent and expertise of independent security researchers. These programs should include best practices, including those required by CISA of federal agencies, and include a commitment not to pursue legal action against individuals who are legitimate researchers seeking to discover vulnerabilities. Incentives could include government support for smaller players setting up disclosure programs, requiring vendors who sell the government "smart" tech to create their own disclosure programs, and more.