DOI:10.1145/3587825

Kendra Albert and James Grimmelmann

Law and Technology

Do the Right Thing

Exploring the intersection of legal compliance and ethical judgment.

ACTING ETHICALLY MEANS following the law, except when it does not. Laws are not automatically right, and they are never neutral. The legal system favors those who already have power.[1] And what is criminal often says more about society's biases and foibles than any underlying or consistent moral truth.[2]

This may seem like a radical claim. But computing professionals know firsthand that sometimes the law stands in the way of doing what is right. For decades they have struggled with anti-"hacking" laws that seemed to prohibit socially vital work. Instead of being celebrated for finding security vulnerabilities, for uncovering hidden discrimination, or for making consumers' devices work better, they have been threatened with lawsuits or criminal prosecution. Some of them were chilled into silence by these threats. But others fought back. They challenged overbroad laws, in court and out. Some engaged in civil disobedience; others simply ignored the law altogether.

We can learn from their example. Computer-misuse laws are not the only ones that society uses to protect the powerful and control the weak. Computing professionals can draw on their own experience with unjust laws to empathize with others who are subject to marginalization and mistreatment, to make common cause, and to fight for change. And sometimes they may need to break those other laws, too, because it is the right thing to do.

Research and Repression

The Computer Fraud and Abuse Act (or CFAA) is the U.S.'s primary anti-hacking law. It was enacted in 1984, and at first it covered only intrusions affecting particularly important systems (such as the federal government's own computers). But over time, Congress repeatedly amended it, expanding its coverage again and again. Now, it can be a federal crime to "access" without "authorization" any computer, smartphone, electronic doorbell, talking doll, or other device with an Internet connection, even if they only thing you do is "obtain information"—and the computer owner can sue you even if the only harm it has suffered is the cost of its own investigation.

Computing professionals can draw on their own experience with unjust laws to empathize with others who are subject to marginalization and mistreatment.

Computer security researchers have repeatedly found themselves in the crosshairs of the CFAA. Scanning for vulnerabilities is one of the most basic techniques of Internet security; it is how known holes are closed, and unknown ones discovered. But to a CFAA maximalist, sending data to a port on someone else's computer to see what comes back is a prohibited "access" to that computer without their "authorization." Some researchers have been sued, and many more have been threatened with legal action.

Making matters worse, for many years lawyers argued (and some courts agreed) that "authorization" under the CFAA could be defined by a website's terms of service or a company's employee handbook. Under this theory, you

IMAGE BY FANDIJKI

could find yourself on the wrong side of a Justice Department investigation or a $100,000 lawsuit if you checked the sports scores from a work-only computer or lied about your age on a dating site.

This interpretation put anyone whose work depended on analyzing scraped data at risk—because a company could trivially add a "no bots" rule to the fine print on its terms of service page. Security researchers looking for cross-site scripting vulnerabilities, privacy advocates checking for tracking pixels, anti-discrimination lawyers trying to gather eviction data, misinformation researchers tracking the spread of medical lies, and entrepreneurs trying to create better search and analytics services—all of them must routinely violate terms of service to gather the data they need.

Although some courts have rejected the most expansive theories of the CFAA, its usage was not an idle threat. CFAA claims have been asserted against college students who found a way to ride the subway for free, a high schooler who submitted a term paper to a plagiarism checker using a password intended for a college course, and a mother who lied about her age when signing up for a MySpace account. Craigslist sued a competitor for trying to provide a better search engine for Craigslist's famously retro classified ads; LinkedIn sued an HR analytics company for scraping resumes. As legal scholar Andy Sellars explains, these doctrines created an environment where the best guidance on offer was "a rough combination of 'try not to get caught' and 'talk to a lawyer.'"[3]

Resistance and Reform

Despite these legal risks and uncertainties, computing professionals did not give up, and their work did not disappear. The vast majority of computer scientists understood scraping and scanning as acceptable forms of data collection. They recognized that if the CFAA prohibited their work, then to quote Charles Dickens, "If the law supposes that, the law is an ass."

Some researchers received assistance from public-interest law firms and clinics to help them deal with legal threats, responding to cease-and-desist letters with their own carefully worded responses. Others were outspokenly defiant. They presented their findings publicly, hoping their ethically righteous conduct would deter companies worried about the PR impact of being seen as insecure bullies. Others tailored their work to evade detection, holding off on announcing open barn doors until the horses were safely far away. And others, many others, simply ignored the legal restrictions entirely.

The work did not stop. Indeed, organizations like the ACM drafted ethics codes recognizing that some laws are made to be broken. The ACM's code explains that "compelling ethical justifications" can support breaking the law when it "has an inadequate moral basis or causes recognizable harm."[a]

Computing professionals also acted to change the law. A coalition of computer scientists and anti-discrimination researchers challenged the CFAA on the ground that it violated their First

[a] See https://perma.cc/RG6M-MMEH

Amendment rights to study the world and discuss their findings. While the court never ruled on their First Amendment claim, it did the next-best thing: hold that the CFAA does not prohibit violations of terms of service.[b]

The following year, the Supreme Court took a similar case involving a police officer who took a bribe to use his patrol-car computer to look up a license plate in a law-enforcement database.[c] Computer security researchers and technology companies filed briefs in the case explaining how turning his violation of departmental policy into a computer crime would stifle vulnerability disclosure, bias auditing, and automated scraping. The Supreme Court agreed. It explained that if the CFAA "criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals," and struck down the conviction.

Victory! But the lesson of the computer science community's interaction with the CFAA is not that a couple of court cases changed everything. Instead, the history of how computer scientists resisted the CFAA shows how they have never let the law be the primary guide of their actions. They looked to the norms of their profession and their own careful ethical judgment in recognizing the law was wrong, and acting accordingly. The benefits for society of scraping Web data usually far exceeded its costs, the CFAA be damned, and so the work continues.

Criminalization as Marginalization

It is time to let you in on a secret. *There is nothing particularly unique about the CFAA.* Many other laws are just as overbroad and just as harmful. What's shocking is not that the CFAA precludes normal behavior, but just how common this pattern is.

When common behaviors are criminalized, legal threats do not just ensure compliance: they also become a tool of subordination. The CFAA shields companies, governments, and other powerful computer owners from scrutiny, allowing them to weaponize the law as a tool to silence critics and competitors.

When common behaviors are criminalized, legal threats do not just ensure compliance: they also become a tool of subordination.

It does so by carving out a space where computer users fear to tread, at constant risk of liability. Try to disable the webcam watching you, and you become a "criminal." And if *your entire profession* must routinely violate the CFAA to do your jobs, you and your colleagues will be constantly on edge, since all it takes to upend your work is someone powerful being angry about it.

Criminalization is a process, and often a vector of marginalization. Fare evasion laws disproportionately harm the poor, but they also allow cops to hassle youth of color. Anti-pornography laws make it more difficult for sex workers to earn a living, and also reinforce stigma against them, making it more difficult for them to find other jobs if they want them. Immigration laws allow farm owners to tip off authorities if undocumented farm workers try to fight for better conditions.

These laws, like the CFAA, isolate the criminalized, depriving them of access to everyday tools that others can easily use. They prevent people from gathering in community, from helping each other, from sharing information. They affect entire communities, whether through disenfranchisement, financial discrimination, or just plain fear.

The story of the CFAA is the story of hundreds of other unjust laws. And so is the story of resistance. Computer scientists acted their conscience, regardless of what the statute or the general counsel said. They refused to substitute the box-checking of legal compliance for the hard work of making real moral and ethical judgments.

Following their example requires us to be equally nuanced in seeing how others also live under the threat of state violence. Think of protesters who are teargassed while blocking a highway to push for an end to police brutality. Or think of pregnant people and their doctors in states that prohibit abortion, where life-saving medical care is treated as a felony. Maybe they are just as justified in breaking the law as computer security researchers were.

Challenging the law is not giving up on ethics—quite the opposite. We still must always ask whether what we plan to do is ethical, appropriate, and respectful of human rights and dignity. What the law says is an important part of that process; law at its best is a legitimate democratic expression of a community's moral beliefs and helps people live together in society. But law is neither the beginning nor the end of ethical responsibility, and equating legal compliance with real ethical judgment is a lazy shorthand that falls apart on close scrutiny.

The areas of the greatest legal uncertainty and the greatest legal risk are often the ones where our work is most necessary. For some, that involves publicly blowing the whistle on substandard security. For others, it involves secretly transporting minors across state lines to obtain abortions. For a third group, it might involve building tools that keep the government from spying on protesters. Some will file lawsuits; others will flout the law and dare the authorities to arrest them.

None of this will be easy. But those of us who often end up on the right side of the ever-moving line between "law-abiding" and "criminal" owe our criminalized colleagues nothing less.

We just did the right thing. And if we could do it once, we can do it again. C

[b] See *Sandvig v. Barr*, 451 F. Supp. 3d 73 (D.D.C. 2020).

[c] See *Van Buren v. United States*, 141 S. Ct. 1648 (2021).

References

1. Galanter, M. Why the haves come out ahead: Speculations on the limits of legal change; https://doi.org/10.2307/3053023
2. Hollinger, R.C. and Lanza-Kaduce, L. The process of criminalization: The case of computer crime laws. *Criminology 101*, 26 (1988).
3. Sellars, A. Twenty years of Web scraping and the Computer Fraud and Abuse Act. *B.U. J. Sci. and Tech. L. 372* (2018).

Kendra Albert (kalbert@law.harvard.edu) is a clinical instructor at the Cyberlaw Clinic at Harvard Law School, Cambridge, MA, USA.

James Grimmelmann (james.grimmelmann@cornell.edu) is the Tessler Family Professor of Digital and Information Law at Cornell Tech and in the Law School at Cornell University, New York, NY, USA.