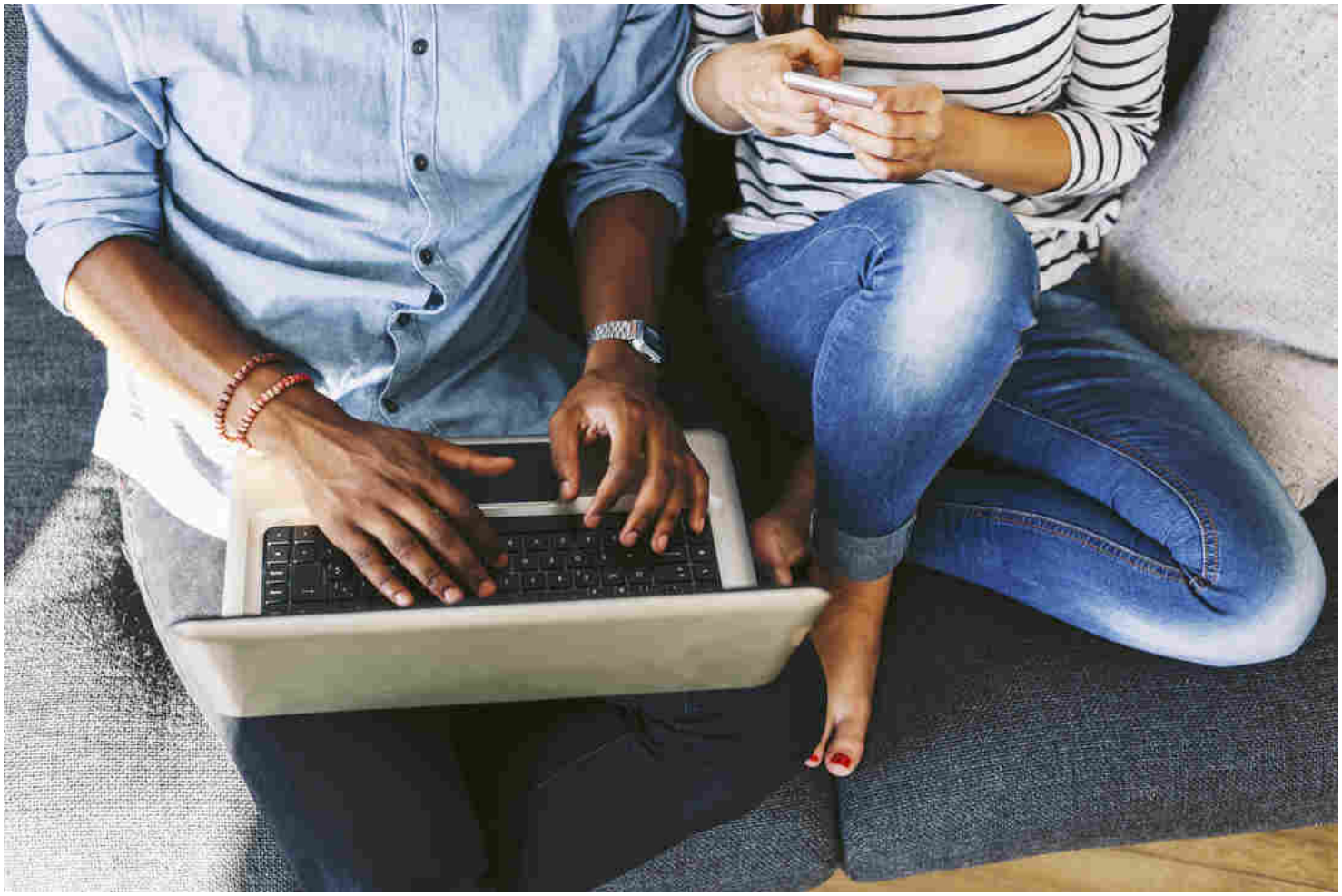
How A 'Nightmare' Law Could Make Sharing Passwords Illegal

www.npr.org/sections/alltechconsidered/2016/07/14/485735920/how-a-nightmare-law-could-make-sharing-passwords-illegal



A new law could make sharing passwords, even in seemingly innocuous circumstances, considered illegal.
Westend61/Getty Images hide caption

toggle caption
Westend61/Getty Images

A new law could make sharing passwords, even in seemingly innocuous circumstances, considered illegal.

Westend61/Getty Images

Updated at 11:32 a.m. ET to reflect a recent ruling in the *Facebook v. Power Ventures* case.

People share passwords all the time. A husband might give his wife his bank account login so she can pay a bill. A professor might ask a secretary to check emails. Comedian Samantha Bee's segment on Syrian refugees featured her teaching them essential phrases in U.S. culture, including "Can I have your HBO Go login?"

But a recent federal court ruling has advocates, researchers and the dissenting judge worried that sharing passwords, even in seemingly innocuous circumstances, could be considered illegal. That's because the anti-

hacking law used is so vague that Columbia law professor Tim Wu called it "a nightmare for a country that calls itself free."

The 9th U.S. Circuit Court of Appeals in San Francisco ruled 2-1 on July 5 against David Nosal, who left a company with others to start a new one. He asked a current employee to give him her password to access client data, which she did, and the majority ruled Nosal acted "without authorization" under the Computer Fraud and Abuse Act.

The problem is: The employee gave Nosal her password, so whose authorization matters — hers, or the company's?

The majority judges wrote that "authorization" is a clear term, citing various dictionaries. Judge Stephen Reinhardt dissented, saying the majority didn't draw a clear line between the kind of password sharing that is a crime under the CFAA and the consensual kind where we give our loved one a Facebook password, even though that might violate Facebook's terms of service.

Reinhardt writes: "If we interpret 'without authorization' in a way that includes common practices like password sharing, millions of our citizens would become potential federal criminals overnight."

This doesn't mean Reinhardt says what Nosal did was right. Not even Dennis Riordan, Nosal's lead attorney, says that.

"It's clearly true that people who had left the company were getting information out of the company computer," Riordan says. "Most people would agree that that is not right ... you shouldn't be doing that. But that's a very different question as to whether it's a CFAA violation."

He says he will petition for a larger panel of judges to review the decision and said the case may end up before the U.S. Supreme Court.

Riordan says the language of the CFAA is "just inconsistent with the modern world and the cloud as it's evolved." He says it's unfair if something like consensual password sharing can be considered criminal.

An alliance of tech companies, including Apple, Adobe and Microsoft, agrees, and filed a brief warning the court against interpreting "without authorization" too broadly.

The Obama administration has proposed a CFAA amendment that, among other things, requires the government to "make clear that trivial conduct does not constitute an offense," the Justice Department said in a blog post last year.

Jamie Williams, a legal fellow and lawyer for the Electronic Frontier Foundation, says the CFAA needs to be amended to clarify what is and isn't a crime, so "prosecutors do not have broad discretion to just go after whatever violation they choose to at any particular point in time for any given reason."

She says the EFF has been arguing for CFAA reform ever since the Aaron Swartz case. Swartz was a computer prodigy and activist who faced charges of computer fraud and possibly years in federal prison because he downloaded millions of pages of academic articles. Swartz supporters, including Harvard Law professor Lawrence Lessig, say the Justice Department had taken this out of hand. Swartz hanged himself in 2013.

Williams says overly broad interpretations of the statute will become more and more relevant as more of our thermostats and other household devices are connected to the cloud. Those are also "protected" devices under the CFAA, and she says sharing those passwords could also be seen as violations of the terms of service and thus the CFAA. The tech companies agree, and so does the dissenting judge.

Williams and James Hendler, a professor of computer, Web, and cognitive sciences at Rensselaer Polytechnic Institute, say the vague language of the CFAA (enacted in 1986) could be used to cover quite a lot of legitimate cybersecurity and social media research. Hendler says this is a case of "a very fast-moving technology coming up

against a very, relatively slow-moving justice system."

"More and more technologies will be deployed that don't have policies behind them, and when policymakers play catchup, we often see laws like CFAA which end up being well-intentioned but poorly written," Hendler says.

In late June, a group of computer science professors, journalists, and the American Civil Liberties Union filed a lawsuit saying the CFAA violates the First Amendment, because research on online algorithms often involves collecting public data from websites using automation or creating multiple accounts. Website terms-of-service agreements often don't allow that.

"Written as an anti-hacking statute, (the CFAA) has become anti-research," two of the professors write in The Guardian.

Orin Kerr, a law professor at George Washington University and former trial attorney at the Justice Department, says the fears about the CFAA are valid, but they don't apply to this case.

He says the kind of routine password sharing that Reinhardt, Williams, Hendler and others are worried about is addressed in another 9th Circuit case, which was decided this Tuesday. In the Nosal case, the defendants used the employee's account for their own benefit rather than acting on her behalf. He says that draws the line between routine password sharing and criminal behavior.

In the second case, a company called Power Ventures let Facebook users set up an account and give the company permission to access and scrape data from their Facebook accounts. Facebook sued, saying that's not allowed.

"That's the fact pattern that Judge Reinhardt is really worried about, because that's the one where an outsider, Power, is acting as an agent of a legitimate account holder as a user of Facebook," Kerr says.

On Tuesday, the court decided in favor of Facebook, which Kerr writes in The Washington Post is "troubling" because the interpretation of the CFAA and legal reasoning "appears to be very broad." That's bad news for people worried about broad readings of the CFAA. Kerr writes that he thinks the decision is "wrong" and has big implications. Kerr reminds us this is a civil dispute, but the CFAA is a criminal statute.

In any case, Kerr expects the Supreme Court to review the CFAA over the next five years or so, because even though lower court judges have tended to interpret the CFAA narrowly in recent cases, they are still divided over what is and isn't a crime under this law.