

Forum:[Hack Forums](#)

Thread: [A Court Ruling on Bug Bounties Just Made the Internet Less Safe - Horrible News](#)

MadScientist - July 26, 2025, 10:44 pm

At a time when cyber threats are growing in frequency, scale and sophistication, public-private cooperation is our great defense. Yet a recent decision by the Ninth Circuit Court of Appeals in *United States vs. Sullivan* threatens to unravel one of the most effective public-private tools we have – responsible vulnerability disclosure through bug bounty programs.

The ruling takes power away from private organizations to manage their own computer systems by interpreting the federal Computer Fraud and Abuse Act (CFAA) to prohibit them from retroactively authorizing access to their systems.

Under this interpretation, security researchers who act in good faith, identify vulnerabilities, and responsibly report them to enterprises may still face criminal prosecution if they accessed the system before receiving formal permission.

This decision is deeply out of step with modern cybersecurity practices and puts organizations, CISOs and national security at greater risk.

Bug bounty programs and coordinated vulnerability disclosure (CVD) frameworks are used extensively by leading private companies – including Microsoft, Meta, Apple – as well as by the US Department of Defense and many other government agencies. These programs incentivize ethical hackers to discover and report flaws before malicious actors exploit them.

According to the FBI, global losses from cyber-enabled crimes exceeded \$50bn over the past five years. In that same period, ethical researchers identified hundreds of thousands of exploitable vulnerabilities through programs that depend on post-access authorization.

When a federal court strips CISOs and legal teams of their flexibility to retroactively authorize access – even when it is demonstrably beneficial, risk-managed, and contractually bound – it chills the very disclosures that improve national cyber resilience.

The case in question relates to an unsuccessful appeal against the conviction of former Uber CISO Joe Sullivan on charges relating to covering up a data breach at the firm. The 2016 breach involved hackers accessing and downloading sensitive information from Uber's servers. Sullivan and his team tracked down the hackers and had them sign a non-disclosure agreement (NDA) in exchange for a payment, recharacterizing the hack as part of Uber's Bug Bounty Program.

<https://www.infosecurity-magazine.com/opinions/court-ruling-bug-bounties-internet/>

Punisher - July 27, 2025, 12:12 am

(Jul 26, 2025 10:44 PM)MadScientist Wrote: [\[CITE\]](#) Under this interpretation, security researchers who act in good faith, identify vulnerabilities, and responsibly report them to enterprises may still face criminal prosecution if they accessed the system before receiving formal permission.

The key part of this is:
before receiving formal permission.

(Jul 26, 2025 10:44 PM)MadScientist Wrote: [\[CITE\]](#) Bug bounty programs and coordinated

vulnerability disclosure (CVD) frameworks are used extensively by leading private companies – including Microsoft, Meta, Apple – as well as by the US Department of Defense and many other government agencies. These programs incentivize ethical hackers to discover and report flaws before malicious actors exploit them.

Isn't this where they "receive formal permission" via the BB programs?

(Jul 26, 2025 10:44 PM)MadScientist Wrote: [\[CITE\]](#) The case in question relates to an unsuccessful appeal against the conviction of former Uber CISO Joe Sullivan on charges relating to covering up a data breach at the firm. The 2016 breach involved hackers accessing and downloading sensitive information from Uber's servers. Sullivan and his team tracked down the hackers and had them sign a non-disclosure agreement (NDA) in exchange for a payment, recharacterizing the hack as part of Uber's Bug Bounty Program.

Sounds like it has more to do with Joe Sullivan trying to cover up a data breach by paying off malicious actors [who were not participating within a scope of an official bug bounty] and pretending it was part of an ongoing bug bounty that didn't exist.

This article seems like rage bait.

MadScientist - July 27, 2025, 1:47 am

(Jul 27, 2025 12:12 AM)Punisher Wrote: [\[CITE\]](#) The key part of this is: before receiving formal permission.

Isn't this where they "receive formal permission" via the BB programs?

Sounds like it has more to do with Joe Sullivan trying to cover up a data breach by paying off malicious actors [who were not participating within a scope of an official bug bounty] and pretending it was part of an ongoing bug bounty that didn't exist.

This article seems like rage bait.

It does, but the resulting court ruling will result in people being afraid and potentially jailed for 10 years if they in good faith reveal a bug they found. On top of that if people find bugs who'd normally inform the company they're likely to sell them on the black market now instead of attempting to expose the bug to the company in hopes for a bounty or a CVE.

Doesnt matter WHY the court ruling was made, it will affect everyone else moving forward now.

Punisher - July 27, 2025, 12:01 pm

(Jul 27, 2025 01:47 AM)MadScientist Wrote: [\[CITE\]](#)

It does, but the resulting court ruling will result in people being afraid and potentially jailed for 10 years if they in good faith reveal a bug they found. On top of that if people find bugs who'd normally inform the company they're likely to sell them on the black market now instead of attempting to expose the bug to the company in hopes for a bounty or a CVE.

Doesnt matter WHY the court ruling was made, it will affect everyone else moving forward now. Nothing has changed, this has always been how this works. Don't compromise a system you don't have permission to access, that has always been the law.

MadScientist - July 27, 2025, 10:35 pm

(Jul 27, 2025 12:01 PM)Punisher Wrote: [\[CITE\]](#) Nothing has changed, this has always been how this works. Don't compromise a system you don't have permission to access, that has always been the law.

Yeah but if you did the company had the right to not prosecute