

Foundations of Computer Security

Vulnerability Disclosure Programs

LEVI SCHOTT AND SONIA SAINI

November 2024



HELLO!



BU/MIT Student Innovations Law
Clinic

- 
- Free and confidential legal service for students at MIT and BU who seek legal assistance related to their research, advocacy, and creative projects.
 - Intellectual Property & Media;
 - Privacy, Security & Health; and
 - Venture & Finance

Please feel free to reach out to the clinic!

Intake Questionnaire: <https://sites.bu.edu/silc/intake-questionnaire/>



OVERVIEW

01

**HISTORY OF CYBERSECURITY
RESEARCH**

02

ALL ABOUT VDPS

03

CFAA

04

CASE STUDIES

05

CONTRACT LAW

06

ACTIVITY





ROBERT TAPPAN MORRIS

HISTORY OF THE PURSUIT AND EXPLOITATION OF VULNERABILITIES



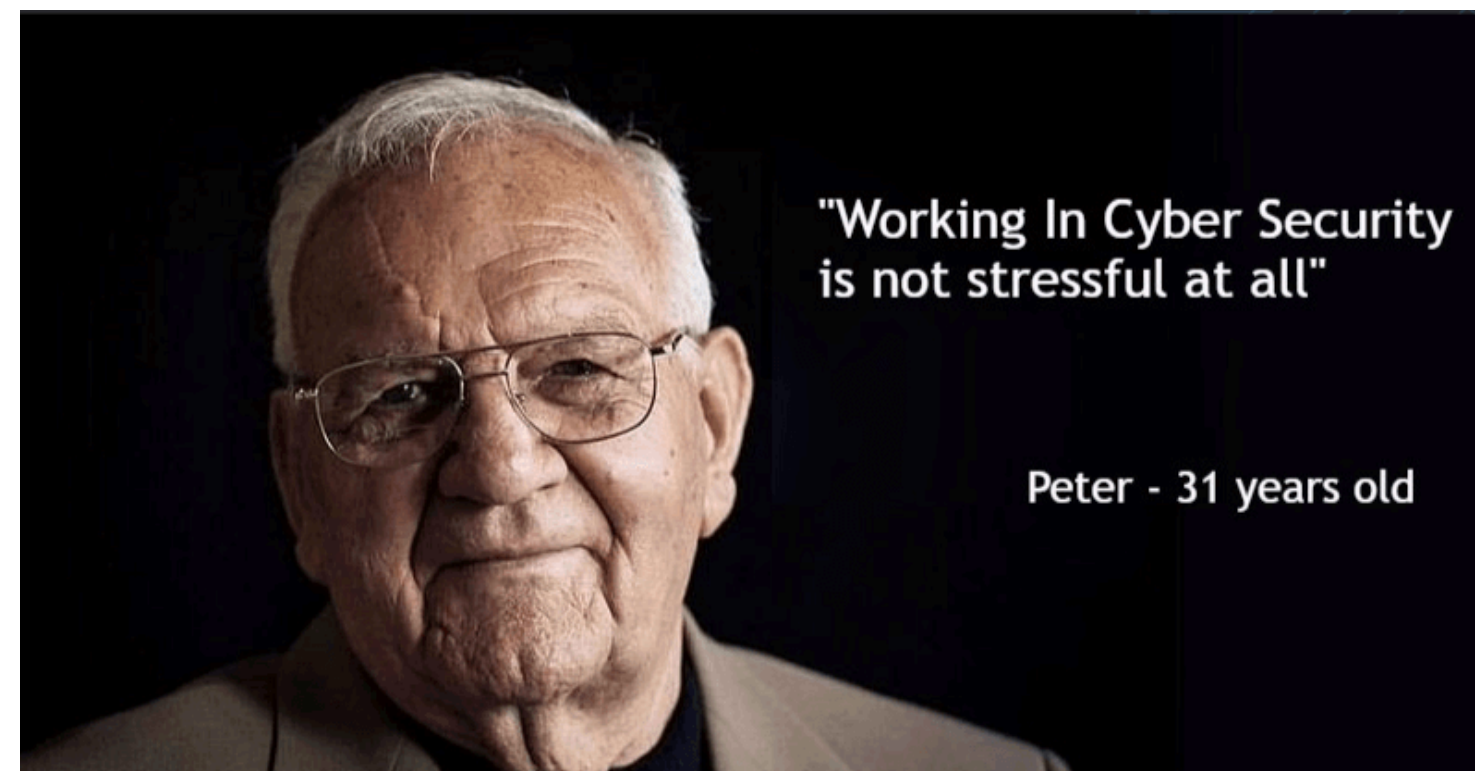
- November 1988 - Morris Worm disabled 10% of the internet
- Three lasting effects:
 - a. Computer Emergency Response Team (CERT) Coordination Center
 - b. First person convicted under the Computer Fraud and Abuse Act (CFAA)
 - c. Increase in research/testing of security practices

■ Why was the Morris Worm so Impactful?

- Ethical Hacking
 - Same skills/tools/strategies as malicious hackers, BUT with the purpose of enhancing network security without harm
- Importance of analyzing systems from the outside
- Why don't we do this with banks? What is unique about computer security?

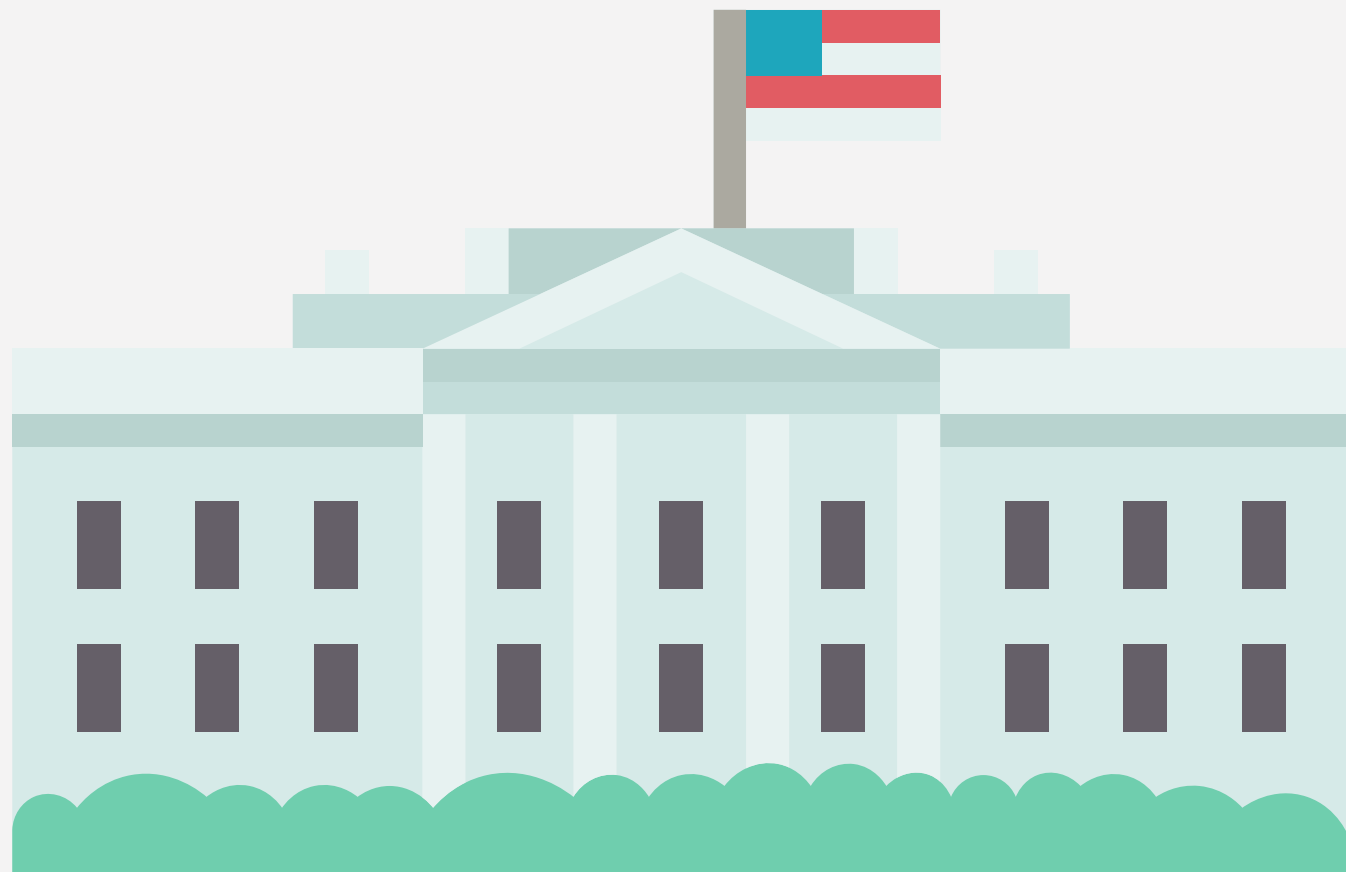


Vulnerability Disclosure Programs (VDPs)



OVERVIEW

- Identifying a weakness before it is exploited
- Establishes a clear, private reporting channel when third-party discovers a vulnerability
 - external parties disclose bugs
- “See something, say something” culture
- Encouraged, and even mandated by legislation, regulations, and global compliance (U.K, NIST)

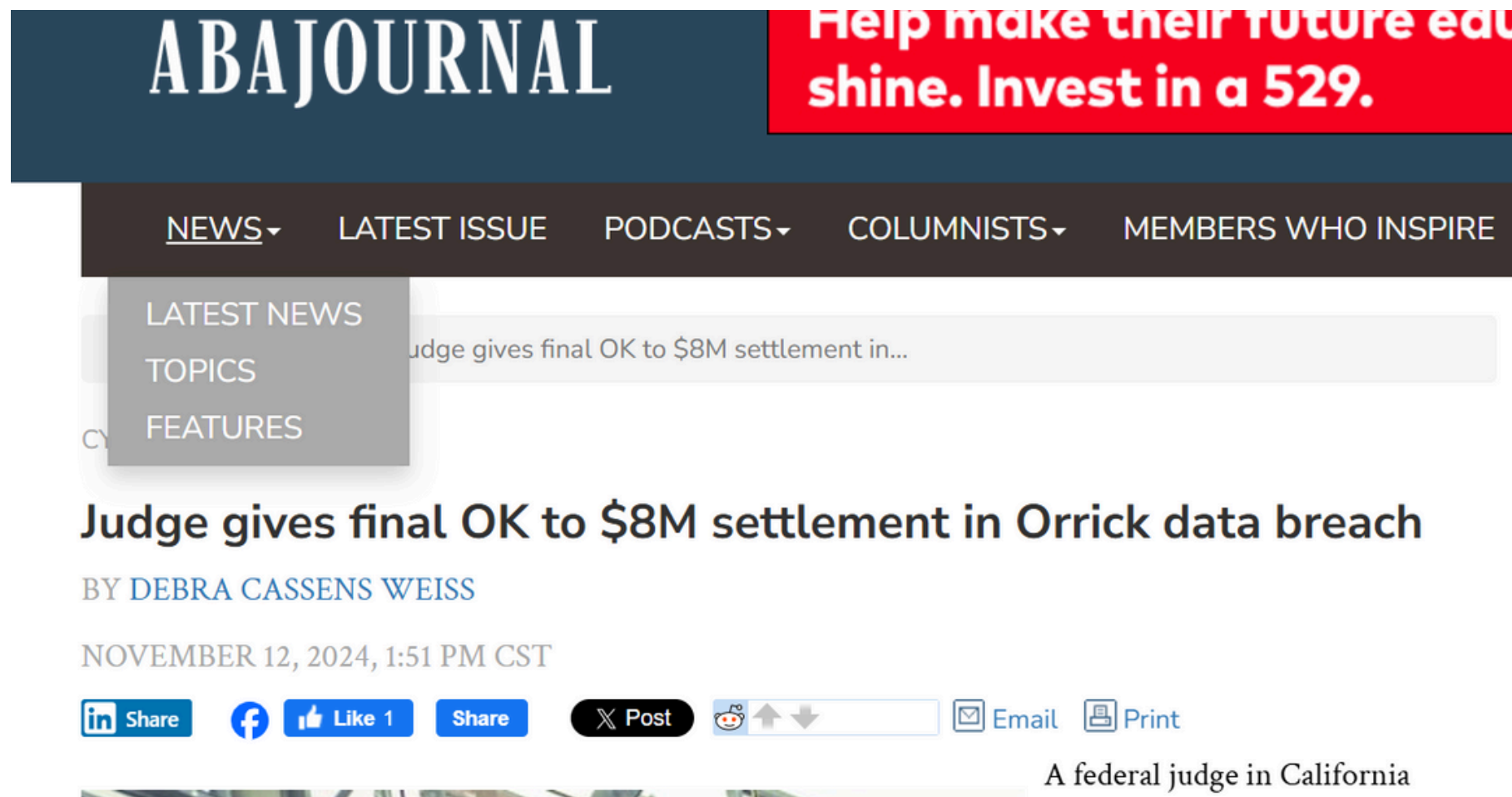


Government Endorsement/Adoption of VDPs

- DOJ Framework
 - Cybersecurity Infrastructure Security Agency (CISA)
- DOD: “Hack the Pentagon Event” (2016)
 - Cost: \$150,000 → >1,000 vulnerability reports
 - “Hack the Army,” “Hack the Airforce,” “Hack the Marine Corps,” etc.
 - Similar programs adopted by Department of State, Food and Drug Administration (FDA), General Services Administration (GSA)
- SECURE Technology Act (2018)
 - Required the DHS to establish a security vulnerability disclosure policy

VDPs in the Private Sector

- 2024 global average cost of data breaches: \$4.88 million (IBM [Cost of a Data Breach Report 2024](#))
- 2023 US average cost of data breach: \$9.48 million (Morgan Lewis [Blog](#))



ABA JOURNAL Help make their future education shine. Invest in a 529.

NEWS ▾ LATEST ISSUE PODCASTS ▾ COLUMNISTS ▾ MEMBERS WHO INSPIRE

LATEST NEWS
TOPICS
FEATURES

Judge gives final OK to \$8M settlement in...

Judge gives final OK to \$8M settlement in Orrick data breach

BY DEBRA CASSENS WEISS

NOVEMBER 12, 2024, 1:51 PM CST

[Share](#) [Like 1](#) [Share](#) [Post](#) [Email](#) [Print](#)

A federal judge in California



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement ▾ Policy ▾ Advice and Guidance ▾ News and Events ▾ About FT

Home / Business Guidance / Business Blog

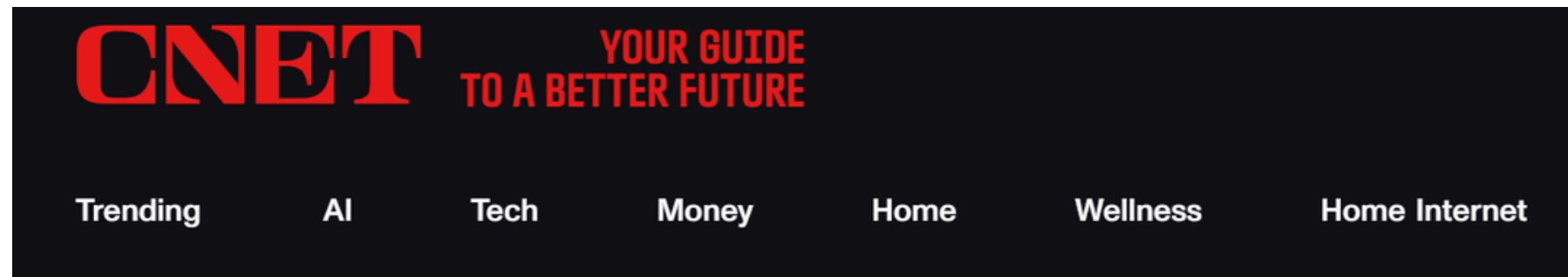
Business Blog

\$575 million Equifax settlement illustrates security basics for your business

By: Lesley Fair | July 22, 2019 | [f](#) [X](#) [in](#)

VDPs in the Private Sector

In 2020, Google paid \$6.7 million in bug bounties, with the highest single award being \$132,500 ([Bloomberg](#)).



Tech > Mobile

Google's Android bug bounty program will now pay out \$1.5 million

Hacking the Pixel's Titan M chip and finding exploits in the developer preview versions of Android will earn you the big bucks.



Corinne Reichert 

Nov. 21, 2019 2:01 p.m. PT 



Guidance

Hackerone

Guidance

Uber

- Security page
- Program guidelines**
- Scope
- Hacktivity
- Thanks
- Updates
- Collaborators

Program highlights

- Platform Standards Fully compliant with Platform Standards. [View](#)
- Top Response Efficiency This program's response efficiency is above 90%. [View](#)

Managed by HackerOne Collaboration Enabled Includes Retesting

- 11 hours**
Average time to first response
- 2 days, 15 hours**
Average time to triage
- 2 days, 10 hours**
Average time to bounty
- 5 days, 1 hour**
Average time from submission to bounty

Rewards summary

Last updated on March 25, 2022. [View changes](#)

Each severity lists the 90-day average bounty and the percentage of total resolved reports, if applicable.

Low	Medium	High	Critical
Avg. bounty \$484 27.87% submissions	Avg. bounty \$1,890 45.50% submissions	Avg. bounty \$5,250 22.26% submissions	Avg. bounty \$15,000 4.38% submissions
\$250–\$750	\$1,000–\$3,000	\$5,000–\$10,000	\$10,000–\$15,000

Scope exclusions



<https://www.uber.com>

Bug Bounty Program launched in Mar 2016

Response efficiency: 98%

[Submit report](#)

Rewards

Severity	Rewards
low Avg. bounty \$484 27.87% submissions	\$250–\$750
medium Avg. bounty \$1,890 45.50% submissions	\$1,000–\$3,000
high Avg. bounty \$5,250 22.26% submissions	\$5,000–\$10,000
critical Avg. bounty \$15,000	\$10,000–\$15,000

WHY SHOULD YOU PARTICIPATE IN A VIDEO

LEGAL



- Reputation
- Money

RISK



WHAT IS A LEGAL RISK?

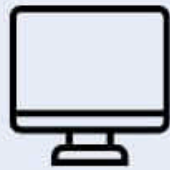
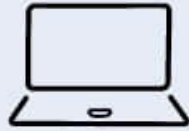
- Civil Liability
 - Private party seeking compensation or an injunction
- Criminal Liability
 - Government seeking to punish an offender via fine or incarceration
- Cease and Desist Letter
 - Sent to an *alleged* wrongdoer, demanding they stop the activity believed to be unlawful
 - Notice that legal action may/will be taken if conduct continues



COMPUTER FRAUD AND ABUSE ACT

Civil or Criminal

Computers (CFAA)



The term "computer" includes many types of high-speed data processing devices

"[W]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer* . . . shall be punished" by fine or imprisonment. 18 U.S.C. § 1030(a)(2)(C).

Risk = accessing devices that you do NOT own, without the owner's permission

Solution = Get permission to access ALL resources for your research AND make sure you are receiving permission from the right people

Van Buren v. United States (2021)

Exceeding authority vs.
Exceeding access (CFAA)

With authorization in order to
obtain information for an
improper purpose?

-> \$5,000 to search police
computer database for as
specific individual



hiQ Labs v. LinkedIn (2022)

- hiQ was using LinkedIn public profile data for its "Keeper" and "Skill Mapper" analytics services.
 - Contracts with eBay, Capital One, and GoDaddy
- Cease-and-desist within a month of the announcement of Talent Insights
- The CFAA
 - "protected computer" clause
 - "exceeds authorization" clause

hiQ Labs v. LinkedIn (2022)

LinkedIn sent a cease-and-desist letter and selectively blocked hiQ's access to public member profiles → hiQ sought an injunction



hiQ Labs v. LinkedIn (2022)

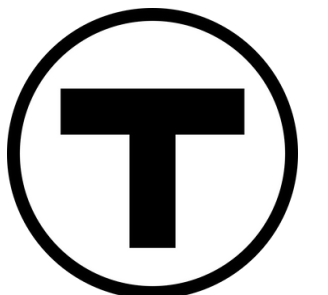
- Exceeds authorization? → ???
 - The CFAA was implemented to prevent hacking, was this hacking?

hiQ Labs v. LinkedIn (2022)

“Entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels claims may still be available. And other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy, may also lie.”

Massachusetts Bay Transportation Authority v. Anderson (2009)

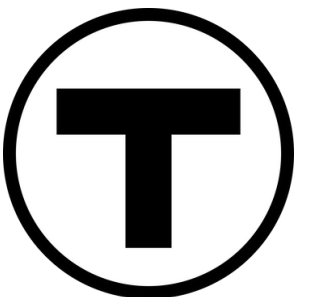
- MIT Undergrads claimed to have discovered a vulnerability in the "CharlieCard" and intended to share their research at DEFCON
- "Want free subway rides for life?"
- MBTA filed a complaint and motion for a temporary restraining order
 - CFAA: "[W]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . [or] knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished" by fine or imprisonment. 18 U.S.C. §§ 1030(a)(2)(C); 1030(a)(5)(A).
 - Conversion and trespass to chattels
 - Negligent Supervision (MIT)



Massachusetts Bay Transportation Authority Terms of Use

“By using our Platform, you agree to comply with these Terms and to otherwise comply with the following Code of Conduct, under which you shall not:

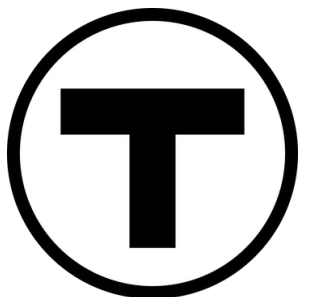
...Use the Platform or any Platform Content to test or reverse engineer the Platform or any Platform Content in order to find limitations, vulnerabilities, or to evade filtering capabilities.”



Massachusetts Bay Transportation Authority v. Anderson (2009)

What could have been done differently?

- Perhaps not include in the presentation description the phrase “free subway rides for life”
 - Sounds like you’re disseminating source code with functional components
- Notify MBTA in advance of the presentation:
 - provide the MBTA and its vendors with information sufficient to replicate, test, and repair the purported security flaws prior to the presentation
 - The complaint was filed on August 8, 2008, just 2 days before DEFCON



Contracts:

- EULA: end-user license agreements
- TOS/TOU: terms of service or terms of use.
- NDA: non-disclosure agreement
 - restricts the ways you can report or publish about security flaws

-> Click-through consent = assent to contract terms

“No reverse engineering” clauses

Some contracts explicitly prohibit reverse engineering



Uber Terms and Services

Restrictions.

You may not: (i) remove any copyright, trademark or other proprietary notices from any portion of the Services; (ii) **reproduce, modify, prepare derivative works based upon, distribute, license, lease, sell, resell, transfer, publicly display, publicly perform, transmit, stream, broadcast or otherwise exploit the Services except as expressly permitted by Uber;** (iii) **decompile, reverse engineer or disassemble the Services except as may be permitted by applicable law;** (iv) link to, mirror or frame any portion of the Services; (v) cause or launch any programs or scripts for the purpose of scraping, indexing, surveying, or otherwise data mining any portion of the Services or unduly burdening or hindering the operation and/or functionality of any aspect of the Services; or (vi) **attempt to gain unauthorized access to or impair any aspect of the Services or its related systems or networks.**

VDP Contracts:

- Scope
 - What assets and vulnerabilities should external parties focus on? What shouldn't they focus on?

Focus Areas:

- Unauthorized access to GS customer/user account
- Application compromise via physical access
- GS app attack via user installed legitimate/malicious application
- Application Login/Authentication Bypass
- Application Logic Bypass
- Authorization Bypass

On top of the above, the following items also are out-of-scope for mobile applications:

- Vulnerabilities that can *only* be exploited on a rooted, jailbroken, or device with intentionally reduced security controls are considered out of scope. Submissions will be rewarded only if the vulnerability exists and can be exploited on a non-jailbroken, non-rooted or non-modified device.
- Lack of / Incomplete certificate pinning
- Bugs that simply cause an app to crash without any security impact
- Exposure of non-sensitive data on the device
- Exposure of data via usage of overlays or accessibility services.

VDPs Contracts:

- Outdated and overly-broad anti-hacking laws create uncertainty
- Safe Harbor Provision
 - Company will protect those who disclose vulnerabilities from legal action in certain situations/under certain conditions
 - Recommended by the DOJ framework
- Gold Standard Safe Harbor (default)

VDPs Contracts:

We consider Good Faith Security Research to be **authorized activity that is protected from adversarial legal action by us. We waive any relevant restriction in our Terms of Service (“TOS”) and/or Acceptable Use Policies (“AUP”) that conflicts with the standard for Good Faith Security Research outlined here.**

This means that, for activity conducted while this program is active, we:

- **Will not** bring legal action against you or report you for Good Faith Security Research, including for bypassing technological measures we use to protect the applications in scope; and,
- **Will** take steps to make known that you conducted Good Faith Security Research if someone else brings legal action against you.

Keep in mind that we are **not able to authorize security research on third-party infrastructure, and a third party is not bound by this safe harbor statement.**



ACTIVITY!

- Safe harbor
- Partial safe harbor
- No safe harbor

Any other noteworthy language?

Prepare to discuss!



REVEAL

- **Safe harbor = General Motors (3)**
- **Partial safe harbor = Apple (2)**
- **No safe harbor = Axis Bank (1)**

Apple (partial safe harbor) #2

3. The Apple Security Bounty program extends to security research covering all Apple products and public-facing services, except research involving any of the following:

1. Apple Pay
2. Any non-public-facing Apple system
3. Phishing, social engineering, or similar techniques

5. You must not **disrupt, compromise, inappropriately access, store, or damage:**

Data or property (including a device) that you do not own, unless the data or property owner has given you express, written consent to disrupt, compromise, or damage the data or property; or

Apple services in a manner that can adversely affect other users. Adverse effects solely impacting you are allowed.

6. “you must not disclose it to anyone other than Apple until after Apple has released a software update and published a security advisory for the reported security vulnerability.”

7. A participant in the Apple Security Bounty program will not be deemed to be in breach of applicable Apple license provisions which provide that a user of Apple software may not copy, decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, or create derivative works of such Apple software, for in-scope actions performed by that participant where all of the following are met:

1. The actions were performed **strictly** during participation in the Apple Security Bounty program;
2. The actions were performed during **good-faith security research**, which was – or was intended to be – responsibly reported to Apple; and
3. Neither the actions nor the participant **have otherwise violated or exceeded the scope of these terms and conditions.**

8. You must comply with **all applicable laws** (including directives, regulations, and ordinances), **including those of the country** or region in which you reside or in which you download or use Apple software or services.

Axis Bank (no safe harbor) #1

- **Take responsibility and act with extreme care and caution.**
- **When investigating the matter, only use methods or techniques that are compliant with law and necessary in order to find or demonstrate the weaknesses. Without limiting the generality of the foregoing.**
- **If your actions are intrusive or an attack on our system, we may take action against the same including reporting them to law enforcement agencies.**
- **Axis Bank reserves its right to initiate legal action against any person and/or report to relevant authorities of such person who conduct any Tests or investigations which are prohibitive or not in compliance with law or not as per this Policy.**

Do not publicly announce the vulnerability, but get in touch with us and give us the time to examine the issue. The safety of our customers' information and assets is our top priority. Therefore, we encourage anyone, who have discovered a vulnerability in our systems to act instantly and help us improve and strengthen the safety of our sites and systems.

GM (safe harbor) #3

Safe Harbor

GM agrees **not to pursue civil action against researchers who comply** with General Motors' and HackerOne's policies regarding the VDP. We consider activities conducted consistent with the GM Policy Terms to constitute **“authorized” conduct under the Computer Fraud and Abuse Act**. Also, if you comply with the GM Policy Terms, **we will not bring a DMCA claim against you** for circumventing the technological measures we have used to protect the applications in scope.

If legal action is initiated by a third party against you and you have complied with the GM Policy Terms, we will, if asked, state that your actions were conducted in compliance with this policy.

By clicking [Submit Report](#), you consent to your Information being transferred to and stored in the United States and acknowledge that you have read and accepted the Terms, Privacy Policy and Disclosure Guidelines presented to you when you created your account.

.

RESOURCES

A Researcher's Guide to Some Legal Risks of Security Research

Sunoo Park Kendra Albert
New York University Harvard Law School

August 2024 (Version 2)*

Contents

1	About this guide	3
2	What do we mean by legal risk?	4
2.1	Types of legal liability	5
2.2	Publishing code that may be misused	6
2.3	Risks around open records requests	7
3	What areas of law raise legal risk for researchers?	8
3.1	CFAA (Computer Fraud and Abuse Act)	10
3.2	Copyright law	13
3.3	DMCA §1201 (Digital Millennium Copyright Act on circumvention)	16
3.4	Contract law	22
3.5	Defamation	25
3.6	Trade secret law	26
3.7	The Wiretap Act	27
3.8	Export controls	28
4	FAQ on getting and working with an attorney	32
4.1	Cease and desist letters	34
5	Conclusion	36
6	About the authors	37
A	Reference table	38

- Bug Crowd
- Hacker One

THANK YOU