RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: SBX1-R3

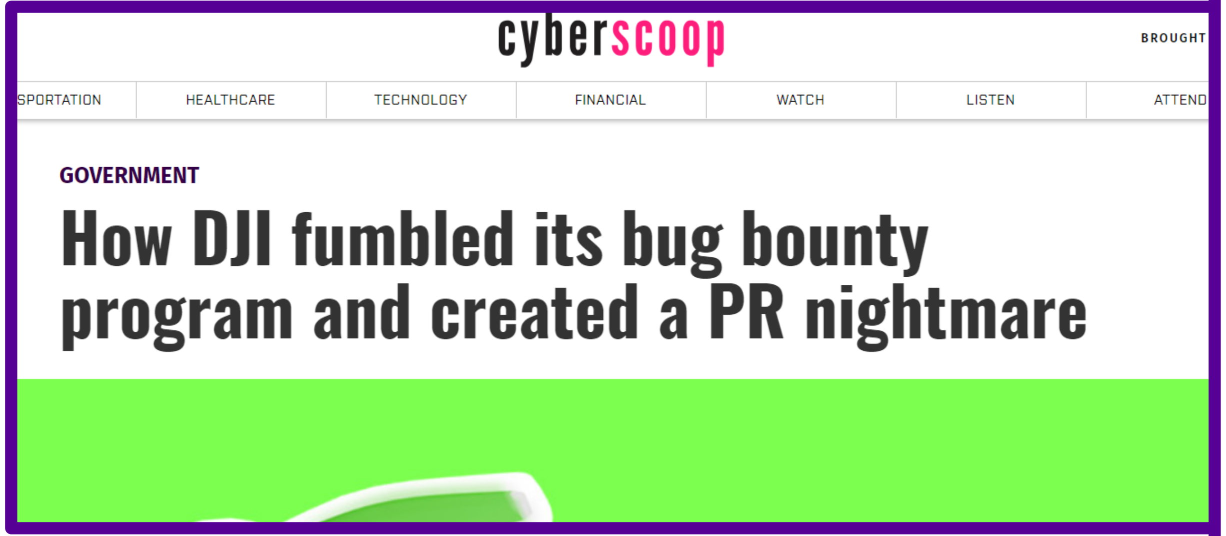
Internet of Laws: Navigating the IoT Legal Landscape

Dr. Amit Elazari Bar On

Lecturer, UC Berkeley School of Information
(MICS)
@amitelazari

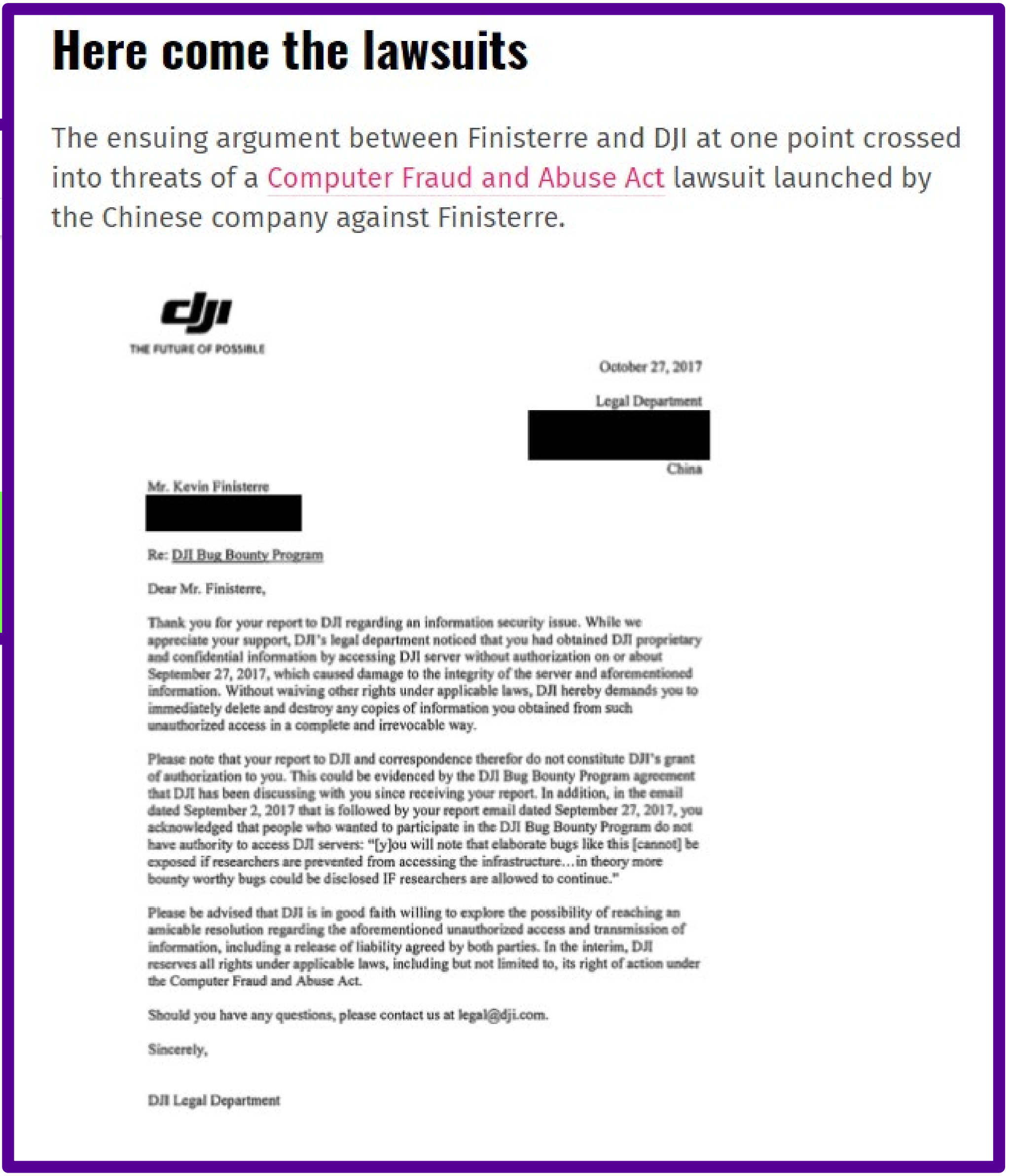
@d0tslash

Photo Credit DFSB DE



GOVERNMENT

How DJI fumbled its bug bounty program and created a PR nightmare



Here come the lawsuits

The ensuing argument between Finisterre and DJI at one point crossed into threats of a Computer Fraud and Abuse Act lawsuit launched by the Chinese company against Finisterre.

dji
THE FUTURE OF POSSIBLE

October 27, 2017

Legal Department
[redacted]
China

Mr. Kevin Finisterre
[redacted]

Re: DJI Bug Bounty Program

Dear Mr. Finisterre,

Thank you for your report to DJI regarding an information security issue. While we appreciate your support, DJI's legal department noticed that you had obtained DJI proprietary and confidential information by accessing DJI server without authorization on or about September 27, 2017, which caused damage to the integrity of the server and aforementioned information. Without waiving other rights under applicable laws, DJI hereby demands you to immediately delete and destroy any copies of information you obtained from such unauthorized access in a complete and irrevocable way.

Please note that your report to DJI and correspondence therefor do not constitute DJI's grant of authorization to you. This could be evidenced by the DJI Bug Bounty Program agreement that DJI has been discussing with you since receiving your report. In addition, in the email dated September 2, 2017 that is followed by your report email dated September 27, 2017, you acknowledged that people who wanted to participate in the DJI Bug Bounty Program do not have authority to access DJI servers: "[y]ou will note that elaborate bugs like this [cannot] be exposed if researchers are prevented from accessing the infrastructure…in theory more bounty worthy bugs could be disclosed IF researchers are allowed to continue."

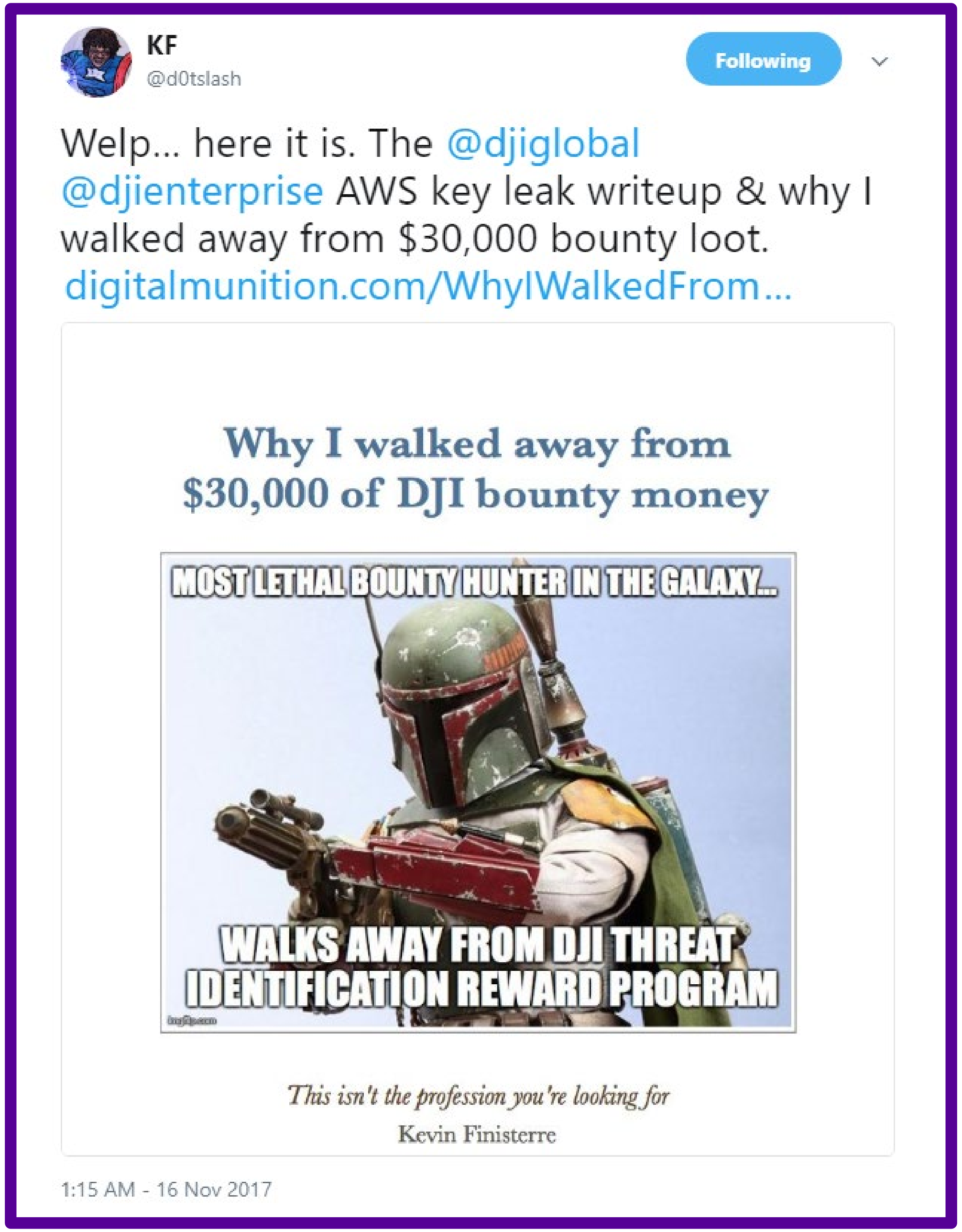
Please be advised that DJI is in good faith willing to explore the possibility of reaching an amicable resolution regarding the aforementioned unauthorized access and transmission of information, including a release of liability agreed by both parties. In the interim, DJI reserves all rights under applicable laws, including but not limited to, its right of action under the Computer Fraud and Abuse Act.

Should you have any questions, please contact us at legal@dji.com.

Sincerely,

DJI Legal Department

Sources: https://www.cyberscoop.com/dji-bug-bounty-drone-technology-sean-melia-kevin-finisterre/ *but see* https://www.dji.com/newsroom/news/statement-about-dji-cyber-security-and-privacy-practices



KF
@d0tslash

Following

Welp... here it is. The @djiglobal @djienterprise AWS key leak writeup & why I walked away from $30,000 bounty loot. digitalmunition.com/WhyIWalkedFrom...

Why I walked away from $30,000 of DJI bounty money

MOST LETHAL BOUNTY HUNTER IN THE GALAXY...
WALKS AWAY FROM DJI THREAT IDENTIFICATION REWARD PROGRAM

This isn't the profession you're looking for

Kevin Finisterre

1:15 AM - 16 Nov 2017

- “Nearly ***half of the researchers*** interviewed mentioned the DMCA specifically as a source of legal risk … In some cases, researchers avoided working with devices and systems protected by access controls to eliminate the legal risks stemming from the DMCA” (CDT, 2018).
- “***Half of the interview subjects reported the CFAA as a primary source of risk***. Of those, more than half reported avoiding some or all types of research that might implicate the CFAA” (CDT, 2018).
- A survey of more than **100** security researchers finding **22%** of them mentioned they were threatened with legal action (Gamero-Garrido et al. 2017).
- “The threat of legal action was cited by **60%** of **414** researchers surveyed as a reason they might not work with a vendor to disclose” (NIST, 2015).

Vulnerability Disclosure Attitudes and Actions

A Research Report from the NTIA Awareness and Adoption Group

TAKING THE PULSE OF HACKING:

A RISK BASIS FOR SECURITY RESEARCH

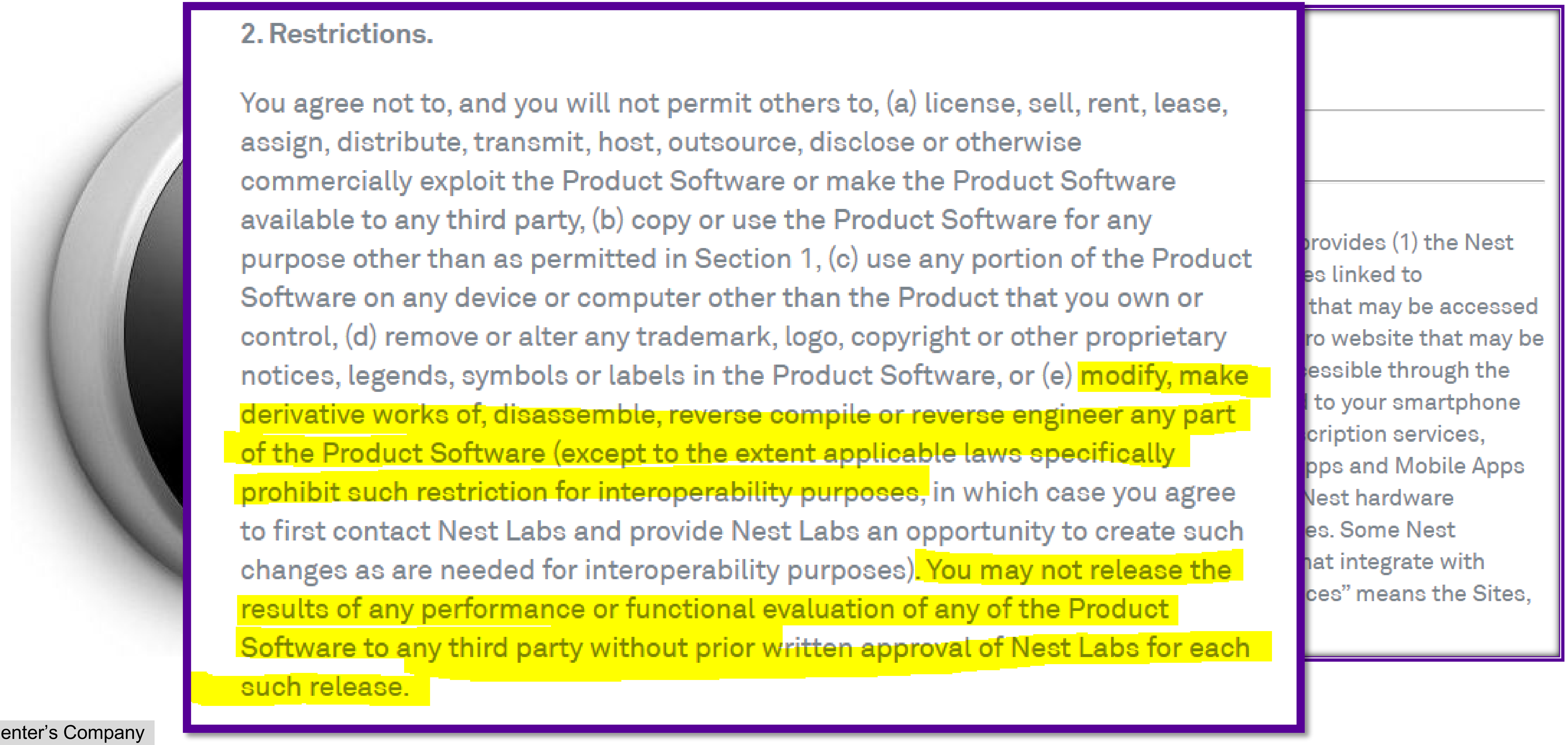
MARCH 2018

Sources: Alexander Gamero-Garrido, Stefan Savage, Kirill Levchenko, & Alex C. Snoeren, Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research, 2017 PROCEEDINGS OF THE 2017 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 1501, https://cdt.org/files/2018/04/2018-04-09-security-research-expert-statement-final.pdf, https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

Disclaimer

photo credit: Brian Hancock

EULAs - Imagine I'm hacking a ….



2. Restrictions.

You agree not to, and you will not permit others to, (a) license, sell, rent, lease, assign, distribute, transmit, host, outsource, disclose or otherwise commercially exploit the Product Software or make the Product Software available to any third party, (b) copy or use the Product Software for any purpose other than as permitted in Section 1, (c) use any portion of the Product Software on any device or computer other than the Product that you own or control, (d) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in the Product Software, or (e) modify, make derivative works of, disassemble, reverse compile or reverse engineer any part of the Product Software (except to the extent applicable laws specifically prohibit such restriction for interoperability purposes, in which case you agree to first contact Nest Labs and provide Nest Labs an opportunity to create such changes as are needed for interoperability purposes). You may not release the results of any performance or functional evaluation of any of the Product Software to any third party without prior written approval of Nest Labs for each such release.

provides (1) the Nest
es linked to
that may be accessed
ro website that may be
essible through the
to your smartphone
cription services,
pps and Mobile Apps
Nest hardware
es. Some Nest
hat integrate with
ces" means the Sites,

Source: Nest, https://nest.com/legal/eula/

Computer Fraud and Abuse Act

[w]hoever . . . intentionally accesses a computer **without authorization or exceeds authorized access**, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(2)(C)

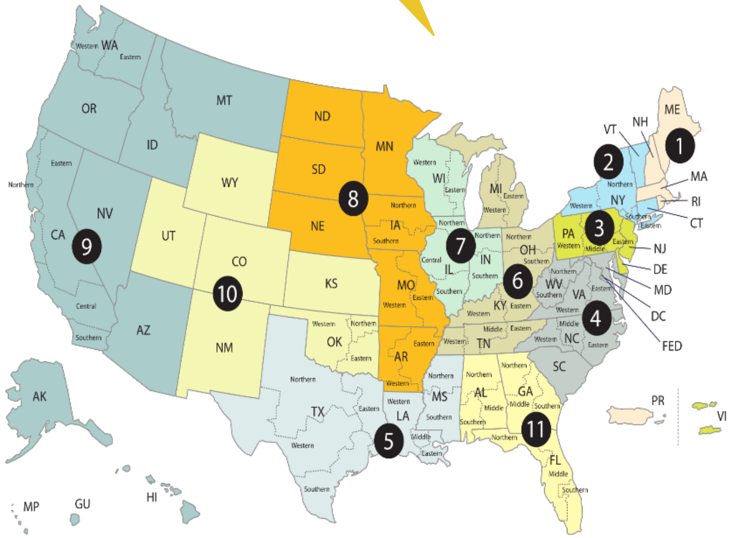
"Authorization" Circuit Split

Contract-Based Interpretation

7th Cir (*Citron*)

11th Cir (*Rodriguez*)

3rd Cir (*Tolliver/*USG)



9th Cir (*Nosal II, Power Ventures*)

TPM/Code-Based Interpretation

9th Cir (*Nosal I, hiQ**)

4th Cir (*WEC*)

2nd Cir (*Valle*)

D.C. Cir. (*Sandvig*)

The DMCA

Section 1201(a)(1) of the Copyright Act (codified under the DMCA) prohibits circumvention of technological measures that effectively control the access to software code (as copyrighted protect work).

- Copyright infringement needed?
- Security Exemption (recently expanded and extended)

The DMCA: Statuary Exemptions

“Security Testing”

- With Authorization
- With no violation of other laws
- solely to promote the security of the owner or operator of such computer system

Encryption

- Information disseminated?
- advance the state of knowledge or development of encryption technology/infringement (e.g. privacy/breach of security)
- The person is appropriately trained or experienced
- The copyright owner gets timely notice + documentation

The DMCA: Temporary Good-Faith Security

- ~~"Device Limitation." (individual consumers+ voting machines); motorized land vehicle; medical device).~~
- "lawfully acquired device or machine'' limitation;
- "solely for the purpose of good-faith security research''
- "not violate any applicable law, including CFAA"
- "carried out in ~~a controlled~~ environment designed to avoid any harm to individuals or the public''
- "information derived from the activity . . . is not used or maintained in a manner that facilitates copyright infringement.''

THE COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: SEVENTH TRIENNIAL PROCEEDING RECOMMENDATION OF THE ACTING REGISTER OF COPYRIGHTS (October 2018), https://www.copyright.gov/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf

NHTSA

FDA

FEDERAL TRADE COMMISSION ★ UNITED STATES OF AMERICA ★ MCMXV

AUTO-ISAC
Automotive Information Sharing and Analysis Center

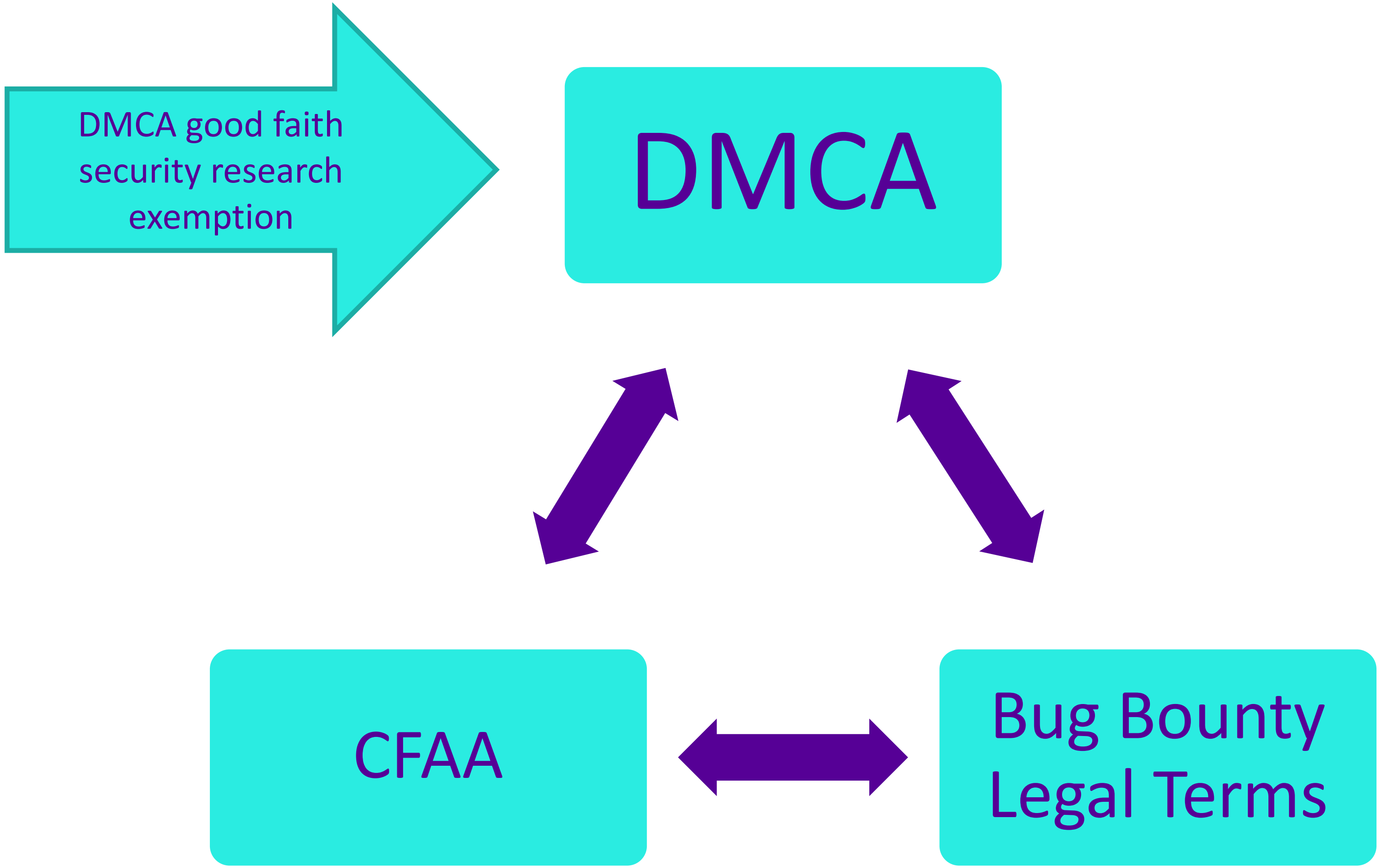
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

“Indeed, in many cases, the FTC has alleged, among other things, that the failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and academics is an unreasonable practice, *in violation of Section 5 of the FTC Act*”

https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf

Bug Bounty/Vulnerability Disclosure Terms



DMCA good faith security research exemption

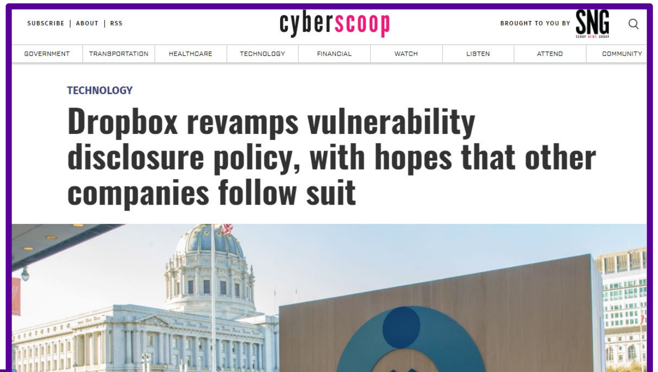
DMCA

CFAA

Bug Bounty Legal Terms

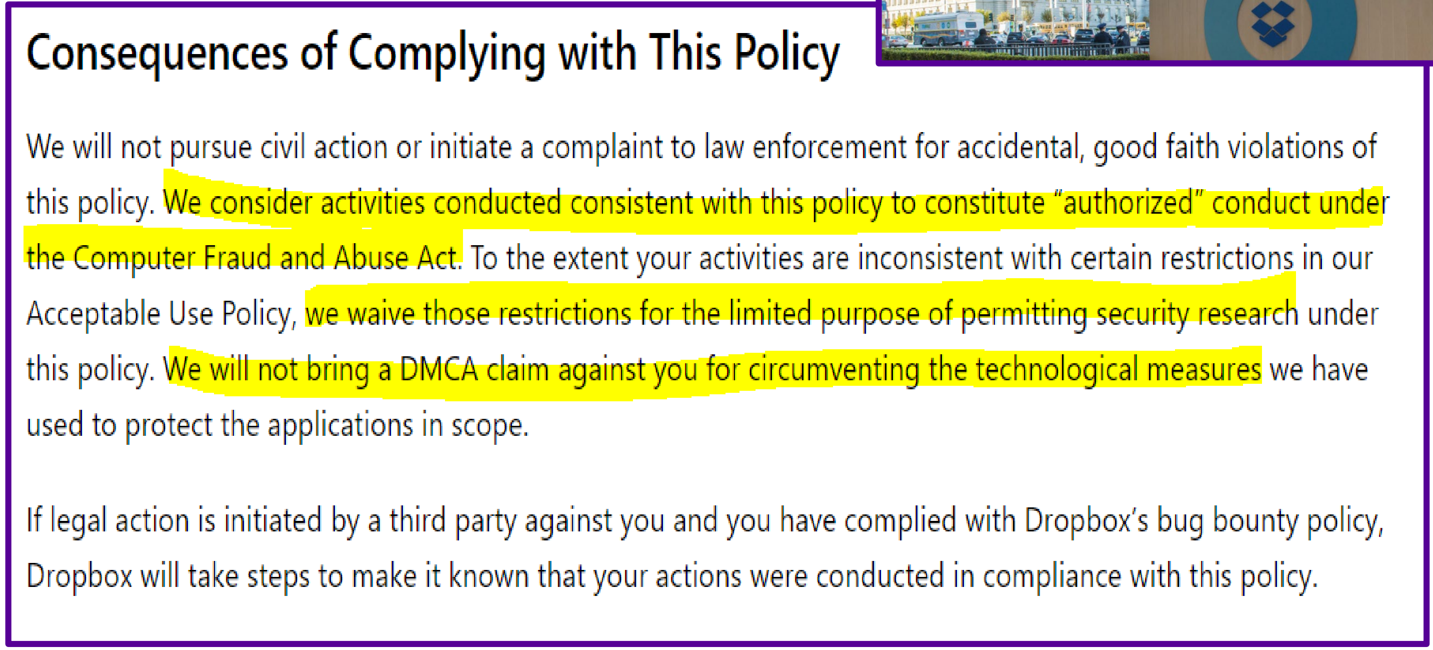
Bug bounty safe harbor

- Authorization under CFAA/DMCA
- DOJ Framework for VDP



TECHNOLOGY

Dropbox revamps vulnerability disclosure policy, with hopes that other companies follow suit



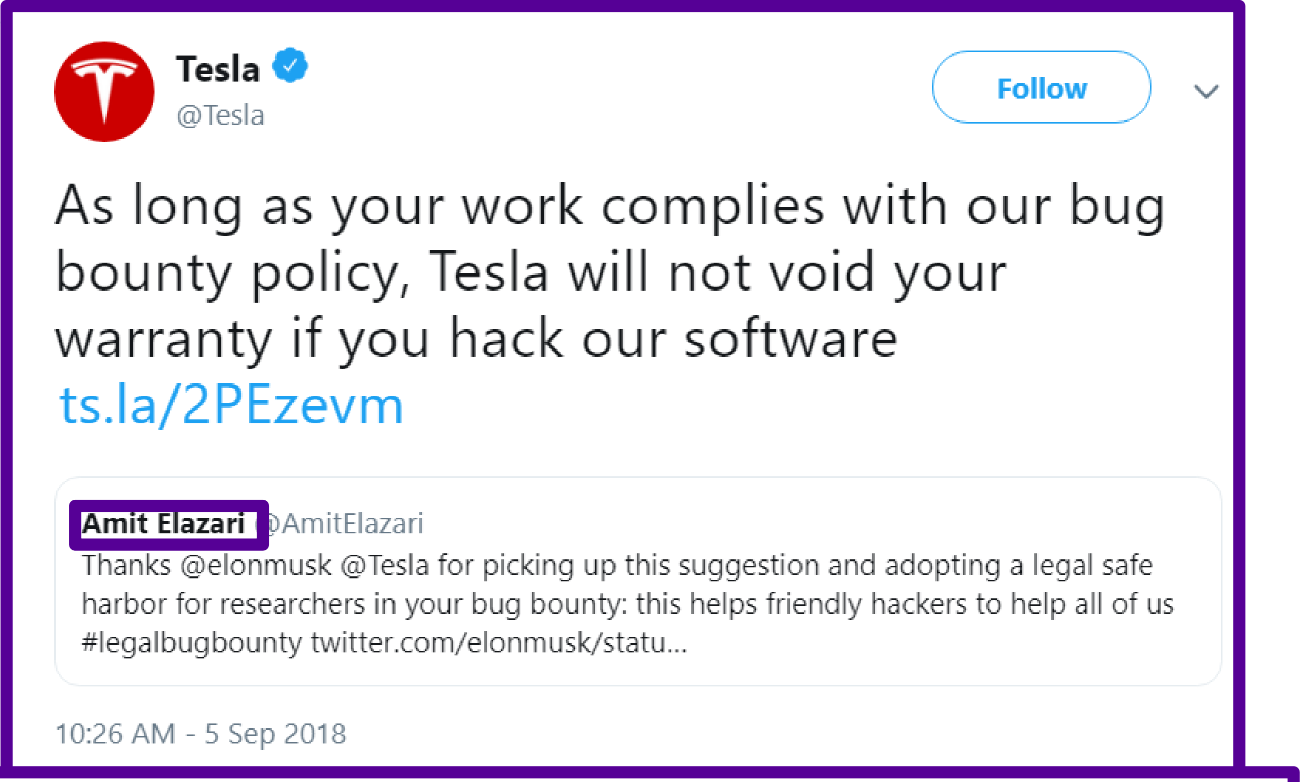
Consequences of Complying with This Policy

We will not pursue civil action or initiate a complaint to law enforcement for accidental, good faith violations of this policy. We consider activities conducted consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act. To the extent your activities are inconsistent with certain restrictions in our Acceptable Use Policy, we waive those restrictions for the limited purpose of permitting security research under this policy. 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 Dropbox's bug bounty policy, Dropbox will take steps to make it known that your actions were conducted in compliance with this policy.

Bug bounty safe harbor

- Warranty/EULA waivers: Tesla

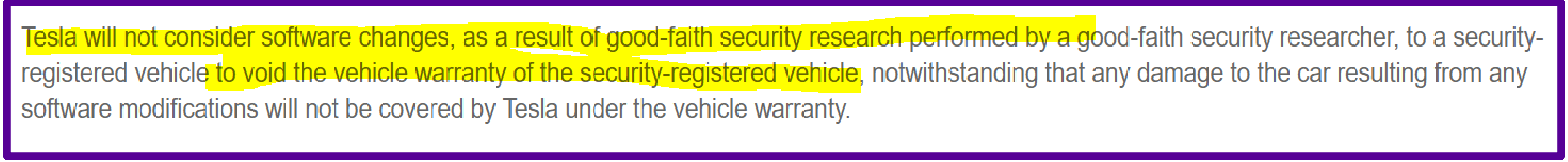


Tesla
@Tesla

As long as your work complies with our bug bounty policy, Tesla will not void your warranty if you hack our software ts.la/2PEzevm

Amit Elazari @AmitElazari
Thanks @elonmusk @Tesla for picking up this suggestion and adopting a legal safe harbor for researchers in your bug bounty: this helps friendly hackers to help all of us #legalbugbounty twitter.com/elonmusk/statu...

10:26 AM - 5 Sep 2018



Tesla will not consider software changes, as a result of good-faith security research performed by a good-faith security researcher, to a security-registered vehicle to void the vehicle warranty of the security-registered vehicle, notwithstanding that any damage to the car resulting from any software modifications will not be covered by Tesla under the vehicle warranty.

https://www.tesla.com/about/security?redirect=no

CA IoT Security Law (1/1/2019).

- “A ***manufacturer*** of a ***connected device*** shall equip the device with a reasonable security feature or features that is appropriate to the nature and function of the device; to the information it may collect, contain, or transmit; and designed to protect the device and any information contained therein from ***unauthorized access, destruction, use, modification, or disclosure***.
- if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable ***security feature*** under if either:
  - (1) The preprogrammed password is unique to each device manufactured.
  - (2) The device contains a security feature that requires a user to generate a new means of ***authentication*** before access is granted to the device for the first time.
- “Manufacturer” means the person who manufactures, or contracts with another person to manufacture on the person’s behalf, connected devices that are sold or offered for sale in California.
- Not construed to impose “any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses”.

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327