epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

February 5, 2018

Senator John Thune, Chairman
Senator Bill Nelson, Ranking Member
U.S. Senate Committee on Commerce, Science, & Transportation
Russell Senate Office Building, Room 253
Washington, DC 20002

Dear Chairman Thune and Ranking Member Nelson:

We write to you regarding the upcoming hearing on "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers."[1] The Electronic Privacy Information Center ("EPIC") supports initiatives, including payments to outside computer security experts, that prompt companies to fix vulnerabilities as this makes user data more secure. But Uber disguised a blackmail payment as a bug bounty payment and waited over a year to disclose the breach of personal data to authorities and to consumers. Bug bounty programs do not excuse non-compliance with data breach notification laws.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues in the information age. EPIC is a leading consumer privacy advocate and has played a key role in developing the authority of the Federal Trade Commission ("FTC") to safeguard the privacy rights of consumers.[2] EPIC's complaint[3] concerning Google Buzz provided the basis for the FTC investigation and subsequent settlement, and the Commission's settlement with Facebook also followed from a complaint filed by EPIC and a coalition of consumer privacy organizations.[4]

Uber's privacy and security practices have been of particular concern to EPIC. EPIC filed a complaint[5] with the FTC in 2015 regarding Uber's egregious misuse of personal data. That complaint led to an FTC settlement[6] with Uber in August 2017. In 2015, EPIC also proposed a privacy law for Uber and other ride-sharing companies.[7]

---

[1] *Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers*, 115th Cong. (Feb. 6, 2018), S. Comm. on Commerce, Science, & Transportation, https://www.commerce.senate.gov/public/index.cfm/hearings?ID=73871FA8-29AD-4ED5-ABB8-C86B4BE4E0A3.

[2] *See, e.g.,* Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html.

[3] *In re Google Buzz* (2011), https://epic.org/privacy/ftc/googlebuzz/.

[4] *In re Facebook, Inc*. (2011), https://epic.org/privacy/inrefacebook/.

[5] EPIC Complaint to the FTC, *In the Matter of Uber Technologies, Inc.* (June 22, 2015), https://epic.org/privacy/internet/ftc/uber/Complaint.pdf.

[6] Agreement Containing Consent Order FILE NO. 1523054, *In the Matter of Uber Technologies, Inc.*, https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_agreement.pdf.

[7] Marc Rotenberg and Julia Horwitz, *Privacy Rules for Uber*, HuffPost (Feb. 11, 2015), https://www.huffingtonpost.com/julia-horwitz/privacy-rules-for-uber_b_6304824.html.

It is important for this Committee not to lump in Uber's actions with legitimate payments to computer security experts. Bug bounty programs are used in both the public and private sectors to identify vulnerabilities. Blurring the line between bug bounties and breaches hurts white hat hackers who want to disclose vulnerabilities in an ethical way. Joe Sullivan, Uber's chief security officer (who has since been fired), denied that the 2016 incident was a breach and said the company had treated it as an authorized vulnerability disclosure.[8] But emails between Uber and the hacker reveal more complicated circumstances. After Uber told the hacker that the max payout of their bug bounty program was $10,000, he responded that he expected at least $100,000 and then threatened the company.[9]

Bug bounties need to be non-negotiable and clearly defined in company policy, otherwise companies are letting user data be held as ransom. $100,000 could have been an appropriate bounty for Uber to pay. Last month Google paid a security researcher $112,500 for an Android bug[10] and Apple offers up to $200,000 for iOS and iCloud bugs.[11]But the communications between Uber and the hacker make the $100,000 payment look more like extortion than a payment for services.

More critically, bug bounty programs do not exempt companies from data breach notification laws. Even though Uber obtained assurances that the downloaded data had been destroyed,[12] it was still required under state laws to notify users and authorities of the data breach. Once Uber was aware that user data had been compromised, it had a legal obligation to notify those affected by the breach. Waiting over a year to disclose is a clear violation of state data breach notification laws, most of which require a company to notify affected users within 30 or 45 days.[13]

The legal avenues for security researchers and white hat hackers to disclose vulnerabilities need to be more clearly defined. Most companies—94% of the Forbes Global 2000 to be exact—do not have a published vulnerability disclosure policy and because of this nearly one in four hackers have not reported a vulnerability that they found.[14] This hurts users, whose information may be stolen through a vulnerability that went unpatched because it was never reported.

---

[8] Nicole Perlroth and Mike Isaac, *Inside Uber's $100,000 Payment to a Hacker, and the Fallout*, N.Y. Times (Jan. 12, 2018), https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html?_r=0.

[9] *Id.* (One email read: "Yes we expect at least 100,000$ I am sure you understand what this could've turned out to be if it was to get in the wrong hands, I mean you guys had private keys, private data stored, backups of everything, config files etc... This would've heart [sic] the company a lot more than you think.")

[10] Charlie Osborne, *Google awards researcher over $110,000 for Android exploit chain*, ZDNet (Jan. 18, 2018), http://www.zdnet.com/article/google-awards-researcher-over-110000-for-android-exploit-chain/

[11] Andrew Cunningham, *Starting this fall, Apple will pay up to $200,000 for iOS and iCloud bugs*, ArsTechnica (Aug. 4, 2016), https://arstechnica.com/gadgets/2016/08/starting-this-fall-apple-will-pay-up-to-200000-for-ios-and-icloud-bugs/.

[12] Dara Khosrowshahi, *2016 Data Security Incident* (Nov. 21, 2017), https://www.uber.com/newsroom/2016-data-incident/.

[13] National Conference of State Legislatures, *Security Breach Notification Laws* (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[14] HackerOne, *The 2018 Hacker Report* (Jan. 17, 2018), https://www.hackerone.com/blog/2018-Hacker-Report.

The 2016 Uber breach also highlights the need for reform of the Computer Fraud and Abuse Act ("CFAA").[15] Due to the CFAA, companies are able to give white hat hackers little assurance that they will not seek civil or criminal penalties if they assist the company. The law blurs the line between ethical and unethical hacking, leaving companies and hackers in legal limbo. Former Secretary of the Army, Eric Fanning, said "what Hack the Pentagon validated is that there are large numbers of technologists and innovators who want to make a contribution to our nation's security, but lack a legal avenue to do so."[16] Last year, the Department of Justice created *A Framework for a Vulnerability Disclosure Program for Online Systems*, but following this framework only "substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law under the Computer Fraud and Abuse Act."[17] If we want white hat hackers to help companies and government identify vulnerabilities, we need to be able to give them more legal protection than they have now.

We ask that this letter be entered into the hearing record. We look forward to working with the Committee to help strengthen security practices that protect users.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

[15] *See* Testimony of Marc Rotenberg, *Computer Virus Legislation Before the Subcomm. on Criminal Justice of the House Comm. on the Judiciary,* 101st Cong., 1st Sess. 25 (November 8, 1989) *reprinted in* Marc Rotenberg, "Computer Virus Legislation," *Computers & Society,* vol. 20, no. 1 (March 1990).
[16] HackerOne, *Hack the Pentagon*, https://www.hackerone.com/resources/hack-the-pentagon.
[17] DOJ Cybersecurity Unit, *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), https://www.justice.gov/criminal-ccips/page/file/983996/download.