Ex Parte Meeting Concerning Class 13 - Security Research Eighth Triennial Rulemaking Docket No. 2020-11

On Jul. 14, 2021, Harley Geiger (Rapid7), Prof. J. Alex Halderman (University of Michigan¹), and Blake Reid (Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law, counsel to Prof. Halderman) met with Kevin Amer and Brad Greenberg of the Copyright Office to discuss the exemption petition for Class 13 - Security Research. The meeting focused on 1) the "any applicable law" provision of the 2018 security research exemption, and 2) the Software Freedom Conservancy petition related to privacy. Below, we summarize the discussion at the meeting.

1) The "any applicable law" provision of the 2018 exemption.² We agreed with the US Department of Justice (DOJ) that the "any applicable law" provision should be converted to a reminder that other laws apply, rather than a requirement that all other laws are followed to be eligible for the security research exemption.³ Rapid7 referred to the specific language we proposed⁴ to accomplish this, for which the DOJ has also expressed⁵ support:

Inserting in the definition of "good faith security research" in 201.40(b)(11)(ii) - "Good faith security research that qualifies for the exemption under paragraph (a) may nevertheless incur liability under other applicable laws, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code."

And striking in 37 CFR 201.40(b)(11)(i) - "and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code"

¹ Affiliation listed for identification purposes only.

² 37 CFR 201.40(b)(11)(i).

³ "Although good faith computer security research should indeed comply with all applicable laws, we are now persuaded that replacing the existing requirement that research not violate "any applicable law" with alternative explanatory language would provide equally sufficient notice of the need to comply with applicable law. This change would also reduce the chance that potentially valuable research projects may be discouraged by fears that inadvertent or minor violations of an unrelated law could result in substantial liability under the DMCA." 2021 DOJ letter, pg. 3,

https://www.copyright.gov/1201/2021/comments/reply/Class%2013_Reply_Department%20of%20Justice.pdf ⁴ Rapid7 2020 comments, pg. 5,

 $https://www.copyright.gov/1201/2021/comments/Class\%2013_InitialComments_Rapid7.pdf$

⁵ 2021 DOJ letter, pg. 4,

a. **Scope of "other laws."** We addressed questions from the hearing regarding whether "obscure" and foreign laws are included in "any applicable law.⁶ The DOJ acknowledged in their 2021 letter that obscure domestic and foreign laws are implicated.⁷ There is nothing in Section 1201 that says obscure and extraterritorial laws do not apply under the "any applicable law" provision. We noted that the EU's GDPR and China's highly restrictive rules on security vulnerability disclosure⁸ (the final version of which the Chinese government published this week)⁹ are examples of relevant foreign laws that apply extraterritorially.

We emphasized that non-US laws are not the only cause of ambiguity for researchers, and that there continues to be substantial overlap and ambiguity in domestic law. Examples we provided included the Computer Fraud and Abuse Act after the Supreme Court's *Van Buren*¹⁰ ruling, as well as swiftly evolving privacy laws.¹¹ We reiterated that the "any applicable law" provision continues to cause adverse effects on good faith security research because of the broad, ambiguous, and constantly changing applicability of other laws.

b. **Consistent with Congressional intent.** We addressed the issue of Congressional intent regarding the "any applicable law" provision, which was raised during the security research and medical device hearings,¹² as well as the comments.¹³ Rapid7 pointed out that removal of the "any applicable law" provision would not be inconsistent with Congressional intent because the Copyright Office has already accommodated Congress' intent through other areas of the exemption.

Rapid7 explained that the legislative record on Congress' intent with regard to the "any applicable law" provision in 17 USC 1201(j) was limited to consent and lawful acquisition. Applicable 2 Rapid7 explained that the Copyright Office has already squarely addressed these issues by requiring lawful acquisition and authorization in the temporary

https://www.copyright.gov/1201/2021/comments/reply/Class%2013_Reply_Department%20of%20Justice.pdf

⁶ Apr. 8, 2021 transcript, pg. 491.

⁷ 2021 DOJ letter, pg. 4,

⁸ Rapid7 2020 comments, pg. 5,

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf

⁹ https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/

¹⁰ For example, while *Van Buren* holds that it is not a CFAA violation for authorized users to breach TOS, it does not settle the crucial question of whether TOS alone can provide authorization to access. See *Van Buren v. US* (2021) opinion, pg. 13, fn. 8, https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf

¹¹ The upcoming FTC privacy rulemaking, California Consumer Privacy Act rulemakings, and the GDPR *Schrems II* guidance are all examples of ongoing changes to privacy laws.

¹² Apr. 8, 2021 hearing transcript, pgs. 496, 509.

¹³ Rapid7 2020 comments, pg. 3,

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf

¹⁴ "What that person may not do, however, is test the lock once it has been installed on someone else's door, without the consent of the person whose property is protected by the lock." H.R. Rep. No. 105-706, at 67 (1998) (Conf. Rep.), https://www.congress.gov/105/crpt/hrpt796/CRPT-105hrpt796.pdf

exemption.¹⁵ Rapid7 pointed out that the Copyright Office's addition of these requirements to the exemption addresses Congress' motivation for passing the "any applicable law" provision.¹⁶

We noted that nothing in the Sec. 1201 legislative history expresses an intent by Congress for the "any applicable law" provision to encompass every law on the planet. On the other hand, we noted, there is a clear intent by Congress that the triennial rulemaking process provide flexibility in enforcement to rebalance Sec. 1201 in light of a changing technological and legal landscape.

Prof. Halderman remains opposed to the inclusion of the lawful acquisition and authorization requirements, and urged the Office to remove them for the reasons noted in the record.¹⁷ However, Prof. Halderman agrees that the conversion of the "any applicable laws" limitation to a non-binding reminder would mitigate a meaningful and significant subset of the adverse effects imposed by conditioning the exemption on non-copyright legal regimes.

- c. **Examples of affected research.** At the Apr. 8, 2021 hearing, the Office asked proponents for examples of adverse effects due to the "any applicable laws" provision.¹⁸ The proponents' comments also made several references to adverse effects on research.¹⁹ During the ex parte meeting, we addressed these questions and further clarified the statements with the following examples:
 - i. Halderman: A security research project by one of Professor Halderman's colleagues was halted by senior colleagues who sent him to the University Office of General Counsel to clear the project's intersection with many areas of law because of the DMCA implications.²⁰ Prof. Halderman also discussed how the uncertainty regarding the status of DMCA protection, due to other laws implicated by the unknown sourcing of voting equipment, adversely affected his potential participation in election security research at the upcoming DEF CON Voting Village.
 - ii. **Zemoudeh:** Researchers do not want to undertake research on medical devices because of the risk of not complying with security-related laws.²¹

¹⁵ See 37 CFR 201.40(b)(11)(i). "[...] undertaken on a lawfully acquired device or machine [...] with the authorization of the owner or operator of such computer.

¹⁶ These requirements go beyond those already included in Section 1201(j).

¹⁷ See Comment of J. Alex Halderman, et al. at 23-29 (Dec. 14, 2020),

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_J.%20Alex%20Halderman,%20Center%20for%20Democracy%20&%20Technology,%20and%20U.S.%20Technology%20Policy%20Committee%20of%20the%20Association%20for%20Computing%20Machinery.pdf

¹⁸ Apr. 8, 2021 hearing transcript, pg. 489. Adverse effects are not limited to avoiding litigation, but also include the burden of demonstrating that researchers' conduct is affirmatively in compliance with all applicable laws.

¹⁹ See, for example, Rapid7 2020 comments, pgs. 3-4,

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf

²⁰ Apr. 8, 2021 hearing transcript, pg. 441.

²¹ Apr. 8, 2021 hearing transcript, pg. 572.

iii. **Beardsley:** See additional details below. A security researcher wants to engage in research on unprotected hospital pager messages, but is held back by concerns that he would not be eligible for the security research exemption due to potential violation of wiretap laws.

However, we urged the Copyright Office to avoid an entrapping standard that requires proponents seeking to reform the "any applicable law" provision to assert that security researchers would violate other laws if not for Sec. 1201.²² We noted that, in 2018, opponents baselessly speculated that a security research exemption would lead to unfettered lawlessness,²³ requiring proponents to explain that researchers do not seek to break other laws or cause harm.²⁴ Removing the "any applicable law" condition simply would ensure that the risk of an abstract violation of literally any local, state, federal, or international law would not subject a security researcher to being hailed into federal court by any person claiming to be injured by the researcher's work under penalty of statutory damages.²⁵

d. **Not a reversal by DOJ.** During the Apr. 8 hearing, the parties were asked if the DOJ reversed its position from 2018.²⁶ During the ex parte meeting, we further addressed this question: the DOJ's 2021 and 2018 letters are consistent.

We pointed out that the 2018 DOJ letter does not express support for making exemption eligibility contingent on compliance with all other laws. Instead, the DOJ's 2018 letter stated that DOJ "would not object to the removal of [the Other Laws Limitation] from the exemption, were it standing alone," but supported retaining an express *reference* to CFAA "to avoid confusion that could place security researchers in legal jeopardy."²⁷

We explained that, consistent with DOJ's goal of avoiding confusion, the 2021 DOJ letter clarified its support for specific language that would replace the current "any applicable law" provision with a reminder that other laws (including CFAA) still apply.²⁸ We also noted that the 2021 DOJ letter clarified its position that the "any applicable law"

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf

²² See Rapid7 2020 comments, pgs. 3-4,

²³ See Rapid7 2020 comments, pg. 4, fn. 12.

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf

²⁴ See Reply comments of Felten, Halderman, and Center for Democracy & Technology at 19-27 (Mar. 14, 2018), https://cdn.loc.gov/copyright/1201/2018/comments-031418/class10/Class_10_Reply_Felten_Halderman_CDT.pdf ²⁵ See 17 USC 1203(a), (c)(3).

²⁶ Apr. 8, 2021 hearing transcript, pgs. 490-491.

 $^{^{27}\ 2018\} DOJ\ letter, pg.\ 6, https://cdn.loc.gov/copyright/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf$

²⁸ 2021 DOJ letter, pgs. 3-4,

- 2. **SFC and privacy.** We pointed out that the Software Freedom Conservancy (SFC) petition describes activities that are already encompassed by the security research exemption a position shared by the DOJ.³⁰ Security is widely accepted as fundamental to privacy, and exposure of personal or sensitive information is a common security risk.³¹ We urged the Copyright Office not to make any modification to the security testing exemption based on the SFC petition, though we agree with SFC that it is critical to ensure Sec. 1201 does not stand in the way of protecting user privacy.
 - a. **Narrowing barred by process.** We pointed out that any implicit or explicit narrowing of the existing security research exemption would require notice and a separate process, given the terms of the NPRM.³² However the Office resolves the SFC petition, it must make clear that it is in no way narrowing the existing security research exemption, which would be procedurally inappropriate at this stage of the triennial review.
 - b. Authorized vs. accidental exposure of personal information should make no difference. The joint post-hearing statement of several parties, including Prof. Halderman, noted "agree[ment that] the existing exemption covers testing, investigating, and correcting security flaws or vulnerabilities comprising or related to the unauthorized disclosure or collection of personal information."³³ Prof. Halderman and Mr. Reid noted their understanding that the letter was merely intended to convey that the activities described by SFC's petition are generally covered by the existing exemption, and did not imply any endorsement from Prof. Halderman that the statement was intended to exhaustively account for all conceivably "privacy-related" research allowed under the exemption.

We explained, for example, that intentional design features that deliberately expose personal information are legitimate targets of security research.³⁴ We also noted that security research often includes testing whether a device protects and discloses personal information in accordance with a vendor's privacy policy. Neither Sec. 1201 nor the 2018 security research exemption distinguish between authorized and unauthorized exposure of information as a factor, and we urged the Copyright Office against creating

²⁹ 2021 DOJ letter, pg. 4,

https://www.copyright.gov/1201/2021/comments/reply/Class%2013_Reply_Department%20of%20Justice.pdf ³⁰ 2021 DOJ letter, pgs. 5-6,

https://www.copyright.gov/1201/2021/comments/reply/Class%2013_Reply_Department%20of%20Justice.pdf ³¹ See Rapid7 2020 comments, pgs. 7-8,

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf

³² 85 Fed. Reg. 65,295, 65,300-01 (2020).

³³ Letter from Aaron Williamson to Regan Smith (May 14, 2021),

https://www.copyright.gov/1201/2021/post-hearing/letters/Class-13-Joint-Post-Hearing-Response.pdf ³⁴ See Rapid7 2020 comments, pg. 7,

https://www.copyright.gov/1201/2021/comments/Class%2013_InitialComments_Rapid7.pdf

this distinction in the 2021 exemption. We noted that adopting such a distinction not only would be procedurally improper at this juncture, but would risk arbitrarily and capriciously promulgating harmful and ill-advised policy with no support in the record.

Thank you for your consideration. Please let us know if you have any questions.

Harley Geiger Senior Director for Public Policy Rapid7 harley_geiger@rapid7.com

Intercepting Hospital Pager Data

I am Tod Beardsley and I am a security researcher. Hospitals in America still rely on the legacy, cleartext, unencrypted communications used by pager networks. This fact is well documented in researcher and hacker communities, and recent examples cited in the media discuss examples of this Tasmania, Canada, and Missouri. One crucial component of the scientific method is the notion of reproducibility of experimental results, but this appears to be cut off for researchers like myself who are worried about losing DMCA protections for research.

The issue here is that while it should be pretty straightforward to reproduce these effects for any given hospital area, doing so almost certainly would constitute a violation of state and federal wiretapping laws — namely, intercepting communications not intended for the general public. In addition, any experimentation here would require circumventing the protocol-based controls that restrict the reception of messages to only those addressed to a given pager number.

I would not conduct this activity for malicious purposes, but for the purpose of raising awareness about a security vulnerability so that it could be strengthened. Publishing any research in this area, be they new findings or reproducing already published findings, because it likely violates wiretap laws, would therefore lose any DMCA safe harbor protection for security research. Thus, it is extremely difficult for me to even consider software defined radio (SDR) a legitimate platform for advancing research.

If the general public were more aware of these pager system weaknesses, hospitals around the country would likely adopt more modern encrypted communications. Yet, as things stand, making this case in technical circles or the general public is nigh impossible without risking civil and criminal prosecution. Although I feel less likely to face federal prosecution for violating wiretap laws with this research, I would be concerned about civil lawsuits from the hospital or the pager network provider (to whom I would disclose the research in advance per best practices). In that scenario, the loss of the DMCA safe harbor would open another potential liability and complicate my ability to defend against a suit.

* * *