This is a Word document that allows users to type into the spaces below. The comment may be single-spaced, but should be in at least 12-point type. The italicized instructions on this template may be deleted.

UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

[ ] Check here if multimedia evidence is being provided in connection with this comment

ITEM A. COMMENTER INFORMATION

The Petition submitter is Software Freedom Conservancy (Conservancy), a not-for-profit organization that helps to promote, improve, develop, and defend Free and Open Source Software (FOSS)—software developed by volunteer communities and licensed for the benefit of everyone. Conservancy is the nonprofit home for dozens of FOSS projects representing well over a thousand volunteer contributors. Our communities maintain some of the most fundamental utilities in computing today, and introduce innovations that will shape how software will be created in the future.

Conservancy fights for software freedom, which gives people control over the functionality of the software they use, including the freedom to add or remove features. One of the most important aspects of this control is allowing individuals to determine when and how private information is sent to other people or companies. Because of this, Conservancy naturally cares deeply about privacy for all software users. While our ultimate organizational goal is to preserve all software freedom for everyone, the ability to protect one's own privacy is one of the most essential rights in the entire group of rights that software freedom activists seek. Conservancy is at the forefront of non-profit organizations in making practical progress toward a future where people can correct and improve the software in devices they own, in large part to improve their privacy while using these devices.

Conservancy may be contacted as follows:

Karen Sandler, Executive Director
Software Freedom Conservancy, Inc.
137 Montague St., Ste.
380 Brooklyn, NY 11201-3548
dmca-exemption@sfconservancy.org
+1-212-461-3245

Privacy Act Advisory Statement: Required by the Privacy Act of 1974 (P.L. 93-579)
The authority for requesting this information is 17 U.S.C. §§ 1201(a)(1) and 705. Furnishing the requested information is voluntary. The principal use of the requested information is publication on the Copyright Office Web site and use by Copyright Office staff for purposes of the rulemaking proceeding conducted under 17 U.S.C. § 1201(a)(1). NOTE: No other advisory statement will be given in connection with this submission. Please keep this statement and refer to it if we communicate with you regarding this submission.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 13: Computer Programs—Security Research

To expand "good-faith security research" to include good-faith testing, investigation, and/or correction of privacy issues (including flaws or functionality that may expose personal information) and permits the owner of the device to remove software or disable functionality that may expose personal information.

ITEM C. BRIEF OVERVIEW OF PROPOSED EXEMPTION

In its Notice of Proposed Rulemaking for 2021 the Office says that it intends to recommend renewal the exemption permitting circumvention of technological protection measures ("TPMs") that control access to copyrighted works for purposes of "good-faith security research," codified at 37 C.F.R. § 201.40(b)(11). Conservancy supports the renewal of this exemption and seeks its expansion to encompass good-faith testing, investigation, and/or correction of privacy issues.

There is a significant degree of overlap between security and privacy research. Privacy researchers use many of the same techniques to access and assess the functionality of the programs they study. And often, privacy issues result from security flaws, such as when private information may be accessed due to the vulnerabilities in software. But privacy research extends beyond such issues, for example to investigating whether a company's data collection practices are consistent with their stated policies. The security research exemption, which applies only to research "testing, investigation, and/or correction of a security flaw or vulnerability," therefore does not protect the full gamut of socially valuable privacy research.[1]

Likewise, the permanent statutory exemption at 17 USC § 1201(i) permits end users to take measures to disable privacy-invasive functionality, but does not extend to publicly-minded research. Circumvention is permitted only if "carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected."[2] Privacy research is typically focused on documenting and explaining a product's functionality, and largely for the benefit of people other than the privacy researchers themselves.

Because the existing exemptions do not adequately protect privacy researchers, the security research exemption should be clarified to explicitly protect privacy research. As to Conservancy's request for an expansion of the good-faith security research exemption to permit consumers to "remove software or disable functionality that may expose personal information," we recognize that 17 USC § 1201(i) addresses such end-user mitigations and is the more appropriate focus of any proposed expansion to those protections. Conservancy discusses the limitations of § 1201(i) below and suggests that the Office recommend legislation to expand §

[1] *See* 37 C.F.R. § 201.40(b)(11).

[2] *See* 17 U.S.C. § 1201(i)(1)(D) (exemption only applicable where the "act of circumvention is carried out *solely* for the *purpose of preventing* the collection or dissemination of personally identifying information") (emphasis added); *See also id.* § (A) and (D) ("personally identifying information" must relate to the "person who seeks to gain access to the work protected").

1201(i) to address these concerns rather than expanding the good-faith security research exemption to do so.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

A. Privacy-Focused Research Requires Circumvention of TPMs

The techniques used by privacy researchers to study how software collects and uses private information are largely the same as those used by security researchers. These include installing legitimately obtained software on devices for the purpose of evaluating the device's functionality,[3] de-obfuscating and decompiling code in order to study it,[4] and accessing protected memory spaces to evaluate the software within.[5]

Often, these techniques reveal privacy concerns that do not relate to security vulnerabilities, for example:

- Researchers at Cardiff University published a paper in 2018 analyzing the security and privacy practices of various internet-connected home devices, to determine whether they were consistent with manufacturers' privacy policies.[6] To analyze whether a "smart plug" transmitted information other than that disclosed in its privacy policies, the researchers extracted and decompiled the device's firmware to reverse-engineer its data-encryption scheme and read its encrypted outbound traffic.[7]

- Researchers at Princeton University decompiled the mobile app associated with an internet-connected "hydration tracker" water bottle marketed to children and discovered by examining the code that the application "imported libraries for communication with third-party analytics and performance monitoring services…, [including] Yahoo's Flurry Analytics, Google Analytics, Crashlytics, and a Chinese analytics platform."[8]

---

[3] *See* Dr. Matthew D. Green, Comment on Sixth Triennial 1201 Rulemaking Proceeding at 5 (Feb. 6, 2015), *available at* https://cdn.loc.gov/copyright/1201/2015/comments-020615/InitialComments_shortform_MGreen_Class22.pdf (*hereinafter* "Green 2015 Comment").
[4] *See id* at 7.
[5] *See id* at 8.
[6] Alanoud Subahi and George Theodorakopoulos, *Ensuring compliance of IoT devices with their Privacy Policy Agreement*, available at http://orca.cf.ac.uk/123089/1/Ensuring%20compliance%20of%20IoT%20devices%20with%20their%20Privacy%20Policy%20Agreement.pdf.
[7] *Id.*
[8] Gordon Chu, Noah Apthorpe, and Nick Feamster, *Security and Privacy Analyses of Internet of Things Children's Toys*, available at https://arxiv.org/pdf/1805.02751.pdf.

- An independent researcher used a "debug port" on an internet-connected presence, temperature, and humidity monitor to extract the device's firmware and analyze its functionality.[9]

As the Office recognized in its 2015 recommendation to adopt the security research exemption, these techniques require researchers to first bypass various forms of TPM where they're used, "including challenge-response mechanisms, dongles, code obfuscation, runtime checks, encryption, and disabled access ports on the circuitry [of computing devices]."[10]

A recent example will illustrate where TPMs have prevented research into privacy issues unrelated to vulnerabilities. Developers of Android any iOS applications commonly use code obfuscation or encryption measures to prevent reverse engineering.[11] Earlier this year, a privacy researcher discovered, after decompiling the popular social media smartphone application TikTok, that the application was collecting information far in excess of what it disclosed to the public in its privacy policy.[12] To discover these data collection practices, the researcher was required to circumvent an "unusual added layer of encryption" that hindered reverse engineering of the application.[13] The application did not necessarily use private information insecurely, only contrary to the company's disclosures.

B. End Users Must Circumbent TPMs to Adopt Privacy Safeguards

Consumers who learn about privacy issues in the devices or software they own may wish to adopt safeguards to protect their privacy. Modifying hardware or software to alter or disable functionality, however, often requires circumventing TPMs.

---

[9] DZone, *Reverse Engineering of a Not-So-Secure IoT Device*, Erich Styger, available at https://dzone.com/articles/reverse-engineering-of-a-not-so-secure-iot-device.

[10] *See* United States Copyright Office, Section 1201 rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, October 2015, *available at* https://cdn.loc.gov/copyright/1201/2015/registers-recommendation.pdf (hereinafter "Register's 2015 Recommendation") at Pg. 254.

[11] Simform, *How to avoid reverse engineering of your android app?*, available at https://www.simform.com/how-to-avoid-reverse-engineering-of-your-android-app/; App Sealing, *Securing Mobile Apps Against Reverse Engineering*, Govindraj Basatwar, available at, https://www.appsealing.com/securing-mobile-apps-against-reverse-engineering/; IBM Mobile Foundation, *Obfuscating Android code using Proguard in MobileFirst Foundation 8.0*, available at https://mobilefirstplatform.ibmcloud.com/blog/2016/09/19/mfp-80-obfuscating-android-code-with-proguard/. *See also* Register's 2015 Recommendation at Pg. 254 (recognizing code obfuscation and encryption as technological protection measures).

[12] Digital Information World, *This researcher claimed to reverse-engineered TikTok app, and unveiled alarming privacy aspect*, Arooj Ahmed, available at https://www.digitalinformationworld.com/2020/06/tiktok-app-alarming-privacy-aspect.html.

[13] The Wall Street Journal, *TikTok Tracked User Data Using Tactic Banned by Google*, Kevin Poulsen and Robert McMillan, available at https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738;

For example, modifying the code running on an electronic device requires the consumer to replace the device's firmware. Firmware is often cryptographically signed or encrypted to prevent the device from running code not explicitly authorized by the manufacturer.[14] Firmware encryption is used on wireless cameras[15] and smart TVs.[16] Amazon's Echo smart speaker likewise uses cryptographic signatures to prevent the installation of unauthorized firmware updates.[17] A consumer wishing to modify the device's functionality would need to circumvent these measures to do so.[18]

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

A. The prohibition on circumvention chills privacy research and harms consumers

Privacy researchers are adversely affected by § 1201's prohibition on circumvention because it is often necessary to circumvent TPMs on copyrighted computer programs for the purpose of testing, investigating, and correcting privacy issues. By putting essential research techniques in legal jeopardy, the prohibition chills beneficial privacy research.

This also harms consumers, because consumer privacy in the United States is largely driven by the "notice and choice" approach, making it incumbent on individuals to decide, on the basis of available information, which products align with their privacy interests.[19] Without the work of independent privacy researchers, consumers seeking to assess the privacy practices of companies they entrust with their personal information must rely solely on the companies' own privacy disclosures. Adequate protections for privacy research are necessary to support informed consumer choice.

1. *The class of works affected*

The proposed exemption would permit privacy researchers to circumvent the TPMs on computer programs, including desktop and mobile applications, as well as software embedded in computing devices—the same class of works encompassed by the security research exemption.[20] All of these are computer programs protected by copyright.

---

[14] Sternum, *Is Encryption Enough for Security? - Part 1*, available at https://www.sternumiot.com/blog/2019/4/8/is-encryption-enough-for-security-part-1.
[15] *See* IPVM, *Cyber Security - Firmware Encryption*, https://ipvm.com/forums/video-surveillance/topics/cyber-security-firmware-encryption.
[16] *See* Marco Ramilli, *Firmware Hacking: The Samsung smart TV turn*, available at https://marcoramilli.com/2013/05/13/firmware-hacking-the-samsung-smart-tv-turn/.
[17] *See* XDA, *Sideloading an Echo Show?*, https://forum.xda-developers.com/t/sideloading-an-echo-show.3871093/.
[18] *See* Register's 2015 Recommendation at 254 (discussing the role of firmware encryption as a TPM).
[19] Berkeley Law, *Alan Westin's Privacy Homo Economicus*, Chris Jay Hoofnagle and Jennifer M. Urban, *available at* https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/berkeley-consumer-privacy-survey/.
[20] *See* Register's 2015 Recommendation at 254 (discussing the class of works affected by security research).

2. *The proposed uses are non-infringing*

Privacy researchers examine computer programs to determine whether their functionality is consistent with the manufacturers' disclosures, with the law, and with best practices. These uses are non-infringing because they make use only of the non-protected elements of the works, and because they are fair use.

a. Privacy researchers make use of non-protected elements of computer programs

When privacy researchers access a protected work, such as a mobile application or the firmware of an internet-connected camera, they are not concerned with the work's expressive elements, but with their functional elements—what the work is doing and how. The works produced by these researchers, typically in the form of research reports and academic papers, typically do not incorporate any expressive portion of the works studied. Because copyright does not protect functional elements of a work,[21] or any "process, system, [or] method of operation," 17 U.S.C. § 102, the work of privacy researchers is fundamentally non-infringing.[22]

b. The proposed uses are fair use

Privacy research, like security research, sometimes requires reproduction, and adaptation of a protected work in service of the research.[23] For example, when a researcher decompiles a binary application, the resulting decompiled source code may be an adaptation of the work. But as the Office has recognized in the context of approving the security exemption, such intermediate or ancillary uses in service of good-faith research are fair uses.[24]

All four fair use factors support this conclusion. First, the "purpose and character" of the access and reproduction of the protected work would be for "academic inquiry" or would "result in criticism or comment about the work and the devices in which [the protected work] is incorporated."[25] Second, the "nature of the copyrighted work"—computer programs—is "likely to fall on the functional rather than creative end of the spectrum," affording them thinner copyright protection and favoring privacy researchers' claim to fair use of the work.[26] Third, privacy researchers will only copy the portion of the software necessary to evaluate the "functional elements" of the computer program, which are not protected by Copyright law, and any copying of the non-functional aspects of the inspected code will be incidental, with such

[21] *See Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602 (9th Cir. 2000) (citing 17 U.S.C. § 102(b)).
[22] *See* Register's 2015 Recommendation at 301 (computer programs "are likely to fall on the functional rather than creative end of the spectrum").
[23] Dr. Matthew D. Green, Comment on Sixth Triennial 1201 Rulemaking Proceeding at 15 (Feb. 6, 2015), *available at* https://cdn.loc.gov/copyright/1201/2015/comments-020615/InitialComments_shortform_MGreen_Class22.pdf.
[24] *See* Register's 2015 Recommendation at Pg. 300 (discussing the application of the Fair Use factors to good-faith security research); *citing* 17 U.S.C. § 107 (listing Fair Use factors).
[25] *See* Register's 2015 Recommendation Pg. 300-01 citing § 107 (1).
[26] *See id*. at 301 (citing § 107 (2).

incidental copying traditionally being considered fair use.[27] Lastly, any market harm resulting from privacy research "would be due to potential criticism... which is not considered a cognizable harm under" the fair use factors.[28]

In sum, privacy research will concern the same class of protected works covered by the existing good-faith security research exemption, and, for the same reasons the Office found good-faith security research to be non-infringing fair use, privacy research will similarly "be socially productive and fair" under § 107.

3. *Existing exemptions are insufficient to protect privacy researchers.*

While privacy research and security research often overlap, valuable privacy research may not always meet the criteria for the exemption at 37 C.F.R. § 201.40(b)(11), because investigating how a product or service collects and disseminates consumer information may not relate to any "security flaw or vulnerability." Rather, privacy researchers often aim to investigate and raise awareness about the intended (although obscured or undocumented) functioning of a particular product or service.

The investigation of the TikTok mobile app described above illustrates this distinction.[29] Although TikTok's data collection practices were a violation of its users' privacy, the violation was not the result of any security flaw. Rather, TikTok was reportedly intentionally collecting the data for advertising targeting purposes.[30] Similarly the research cited above concerning whether various internet connected devices are in compliance with privacy regulations and privacy disclosures was concerned with exposing deceptive marketing or ethically questionable practices, rather than vulnerabilities or other security issues.[31]

The permanent statutory exemption permitting circumvention for purposes of protecting "personally identifying information," codified at 17 USC 1201(i), also fails to adequately protect privacy focused research. The exemption is only applicable where the "act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information."[32] Privacy research focused on documenting and explaining a product's information practices—rather than seeking to prevent or disable any particular data collection practice—would therefore fall outside this exemption.

Moreover, the exemption is available only to the person whose "personally identifying information" is collected or disseminated by the product.[33] But privacy researchers primarily investigate products not to prevent collection and dissemination of their own personally

[27] *See id.* at 301 (citing § 107 (3)).
[28] *See id.* at 302 (citing § 107 (4)).
[29] *See supra*, § Item D (A).
[30] Tech Crunch, *TikTok found to have tracked Android users' MAC addresses until late last year*, Natasha Lomas, *available at* https://techcrunch.com/2020/08/12/tiktok-found-to-have-tracked-android-users-mac-addresses-until-late-last-year/.
[31] *See supra*, § Item D(A).
[32] *See* 17 U.S.C. § 1201(i)(1)(D) (emphasis added).
[33] *See* 17 U.S.C. § 1201(i)(1)(A).

identifying information, but "to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines."[34]

In sum, the relevant exemptions fail to protect privacy research (a) focused on documenting and explaining a product's information practices, rather than seeking to prevent any particular data collection practice, and (b) research focused on products that collect information from individuals other than the researcher. Accordingly, the universe of privacy research protected by the relevant exemptions is unduly narrow, excluding a wide variety of good faith, and socially beneficial, privacy investigations.

4. *The prohibition adversely affects non-infringing uses*

The lack of a clear exemption for privacy-focused research has similar adverse effects as those underlying the security research exemption.[35] Specifically, the current prohibition limits privacy researcher's ability to investigate TPM-protected software, which as this Office noted, represents "a significant number" of consumer products.[36] As a result, privacy researchers are discouraged from producing good-faith privacy research—including criticism, comment, news reporting, scholarship, and research related to privacy issues—with respect to a wide swath of consumer products.[37]

Although some privacy research can be conducted with the consent of copyright holders, for all the same reasons discussed by the Office with respect to information security research, many copyright holders may withhold their consent in the event that privacy researchers plan to release critical or negative analysis of a copyright holder's product.[38] This outcome will similarly deprive the public of important information about products that handle increasingly sensitive personal information.

5. *The statutory factors favor the exemption*

a. Availability for use of copyrighted works

Expanding the security research exemption to include good-faith privacy research will increase the availability of copyrighted works. First, consumers are more likely to purchase products—and trust them with their personal data—if the products have been vetted by independent privacy researchers. Second, privacy research may spur the development of more privacy-protecting products than is presently offered in the market. Third, the exemption will promote the publication of privacy research in the form of "scholarly articles and presentations, as well as new computer programs aimed at rectifying" the various privacy issues discovered by researchers.[39]

---

[34] *See* 37 C.F.R. § 201.40(11)(ii).
[35] *See* Register's 2015 Recommendation at 305.
[36] *Id*.
[37] *Id*.
[38] *Id.* at 306.
[39] *Id*. at 310.

b. The impact that the prohibition on circumvention of technological measures applied to copyrighted works has on scholarship and research

Expanding the good-faith security research exemption to include good-faith privacy research will "enhance criticism, comment, news reporting, teaching, scholarship and research."[40] Should the exemption be expanded, research focused on privacy issues that don't necessarily relate to security flaws or vulnerabilities will encourage the production of scholarship and research related to such issues. Additionally, increased privacy research may "enhance media attention to, and reporting on, [privacy] issues."[41]

c. The proposed exemption's effect on the market for or value of copyrighted works will be positive

Expanding the good-faith security research exemption to include good-faith privacy research will not have any adverse effect on the value of the copyrighted work at issue. As noted by the Office with respect to the information security exemption, harm to the copyright holder due to the exposure of security issues is not relevant to the Office's inquiry, and the same is true for privacy issues. Moreover, as the Office acknowledged with respect to security research, "knowledge of and ability to correct [software] flaws will in fact enhance the value of the software and products at issue."[42] Accordingly, privacy research will not adversely affect the market for or value of copyrighted works for the same reasons noted by the Office with respect to security research.[43]

B. The prohibition on circumvention prevents end users from protecting their privacy

In addition to expanded protections for privacy researchers, Conservancy suggests an expansion of the permanent exemption at 17 USC § 1201(i). The current exemption permits end users to circumvent TPMs to "identify[] and disable[]" the collection and dissemination of "personally identifying information reflecting [their own] online activities."[44] The exemption is available only where the work collects or disseminates such information "without providing conspicuous notice of such collection or dissemination to such person, *and* without providing such person with the capability to prevent or restrict such collection or dissemination."[45] This exemption's limitations have not kept pace with the expanding scope of privacy issues raised by new technology.

First, § 1201(i) only permits the consumer to modify a device that "contains the capability of collecting or disseminating personally identifying information reflecting the *online* activities of a natural person."[46] Many internet connected devices, however, such as smart cameras, voice-enabled smart TVs and smart speakers, and health and fitness trackers, passively

[40] *Id*.
[41] *Id*. at 311 (finding this statutory factor to "weighs strongly in favor of the exemption" with respect to security research).
[42] *Id*.
[43] *Id*.
[44] *See* 17 U.S.C. § 1201(i).
[45] *See id* (emphasis added).
[46] *See* 17 U.S.C. § 1201(i)(1)(A) (emphasis added).

collect information about their owners' offline activities as well.[47] Accordingly, the current permanent exemption fails to encompass consumer modifications to a wide range of devices that collect sensitive offline information about consumers, including highly intimate details about one's health and travel habits.[48]

Second, a consumer may wish to modify a device in a manner that protects the "personally identifying information" of those other than the person making the modification to the device.[49] For example, a consumer may want to make modifications to a smart camera that captures the activities of those outside of one's home, or make modifications to networking equipment to monitor and protect the internet activities of one's children. Accordingly, the current permanent exemption fails to encompass consumer modifications directed at protecting the privacy of those other than the consumer.

Finally, consumers commonly become aware of privacy issues with their devices after purchasing them, despite "conspicuous notice" from the manufacturer of its privacy practices.[50] Many consumers are not necessarily aware of the implications of such notices until being exposed to more detailed reporting on them in the media. In some cases, it's increasingly difficult to find products that don't transmit data to third parties.[51] A consumer should have the legal right to correct privacy issues on their own devices regardless of their privacy savvy at the point of sale, and even where the market offers no privacy-respecting alternatives.

To address these limitations, 17 USC § 1201(i) could be expanded to additionally permit users to circumvent TPMs where:

---

[47] *See* James K. Wilcox, *How to Turn Off Smart TV Snooping Features*, Consumer Reports, Jan. 27, 2020, *available at* https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/; Dorian Lynskey, *'Alexa, are you invading my privacy?' – the dark side of our voice assistants*, The Guardian, Oct. 9, 2019, *available at* https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants; Natasha Lomas, *Google gobbling Fitbit is a major privacy risk, warns EU data protection advisor*, Feb. 20, 2020, *available at* https://techcrunch.com/2020/02/20/google-gobbling-fitbit-is-a-major-privacy-risk-warns-eu-data-protection-advisor/.

[48] Notably, the Supreme Court of The United States has acknowledged that the digital aggregation of even *public* offline activity can be highly revealing and can contain the "privacies of life" including one's "familial, political, professional, religious, and sexual associations." *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

[49] *See* 17 U.S.C. § 1201(i)(1)(A) and (D) (limiting protection to "natural person who seeks to gain access to the work protected").

[50] *See, e.g.*, Karl Paul, *'Tossed my Fitbit in the trash': users fear for privacy after Google buys company*, The Guardian, Nov. 6, 2019, *available at* https://www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data.

[51] *See* Whitson Gordon, *Can I Save Money by Buying a 'Dumb' TV?*, Wired, Nov. 26, 2020, https://www.wired.com/story/save-money-buying-dumb-smart-tv/ (noting that, "'Dumb' TVs aren't completely extinct, but they're pretty close—the few that exist tend to come in small sizes with low resolutions.").

- the work protected is capable of collecting or disseminating identifying information reflecting the offline activities of a person or persons;
- the work protected is capable of collecting or disseminating identifying information about any person, so long as the person performing the circumvention lawfully obtained the work; and
- the work does not provide the capability to prevent or restrict collection or dissemination of personally identifying information, regardless of whether it provided conspicuous notice of those capabilities.

DOCUMENTARY EVIDENCE

N/A