Submission of Knowledge Ecology International
U.S. Copyright Office Docket No. 2015-6

This is the submission of Knowledge Ecology International (KEI) in response to the U.S. Copyright Office request for public comment on "software-enabled consumer products" (U.S. Copyright Office Docket No. 2015-6).

Introduction

Knowledge Ecology International is a non-governmental organization with offices in Washington, DC, and Geneva, Switzerland, that searches for better outcomes, including new solutions, to the management of knowledge resources.

This submission covers these topics:

1. Privacy and informed consent in end user agreements for the use of copyrighted software in consumer products.
2. The use of copyright protections and additional measures in the Trans-Pacific Partnership (TPP) to block access to imported software source code.
3. The impact of copyright law on the ability to audit artificial intelligence and other software in consumer products that may present national or global security risks.

The status of software as an expression protected by copyright law was not settled immediately. [1] Some experts have proposed a *sui generis* regime of protection may be more appropriate. It is not surprising that the legal framework for copyright has at times been an uncomfortable fit for software.

It is of course true that copyright law was not initially designed to address the advent of mass-market consumer products that are functional only when installed with proper software.

Consumers often do not know how the software functions, what information it collects, what rights they have to restrict access to that information, and they are often unaware or in fundamental disagreement about the nature of the rights. The legal regimes associated with software, including importantly the enforcement of non-negotiated mass market licenses associated with its use, and the DMCA protections for technical protection measures and digital rights management, create a number of risks to consumers, including those highlighted by the Copyright Office in the request for comment.

I. Privacy, Mass Data Collection, and Informed Consent in the Use of Software-Enabled Consumer Products

Users of copyrighted software in software-enabled consumer products have a legitimate interest in understanding, approving and influencing the terms under which data on use of a product will be collected, used and distributed.

[1] http://digital-law-online.info/lpdi1.0/treatise17.html

Even well-educated users have neither the time nor the legal expertise to give their informed consent to the hundreds of licenses and agreements that are imposed upon them when they begin to use software-enabled consumer products. The web of legal obligations imposed upon consumers and the lack of transparency around those obligations has contributed to the creation of a system that offers few oversights over copyright holders.

This section explores the interest of consumers in controlling their privacy rights and how the practices of copyright holders restrict that interest, and proposes the creation of a mechanism for third-party advocates to represent the interests of consumers in the negotiation of standard end user licensing contracts. We note that this section is in response to the fourth subject of inquiry in the Copyright Office's December 15, 2015 Notice of Inquiry, which asks "Whether, and to what extent, legitimate interests or business models for copyright owners and users could be undermined or improved by changes to the copyright law in this area," and the fifth recommendation on issues to explore that topic, which suggests addressing "The state of contract law *vis-à-vis* software embedded in everyday products, and how contracts such as end user license agreements impact investment in and the dissemination and use of everyday products, including whether any legislative action in this area is needed."[2]

A. Consumers have an interest in retaining control over private information in their use of products with copyrighted software.

The ability of consumers to influence the terms of privacy agreements in use licenses for products with copyrighted software would align with the public interest. According to a January 2014 survey conducted by the Pew Research Center, 91% of adults agreed or strongly agreed "that consumers have lost control over how personal information is collected and used by companies."[3] That poll also found that consumers were willing to make "trade-offs" for the sake of convenience in using online services. Over half, 55% of respondents, agreed or strongly agreed that they would be "willing to share some information about myself with companies in order to use online services for free."[4]

Software-enabled consumer products were the subject of a recent Pew survey on "Privacy and Information Sharing." Pew asked U.S. adults whether they found the following scenario acceptable:

> "A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room."[5]

[2] Software-Enabled Consumer Products Study: Notice and Request for Public Comment, 80 F.R. 77,668, 77,671-2 (December 15, 2015).
[3] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center, November 12, 2014, *available at* http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (accessed February 11, 2016).
[4] Ibid.
[5] Lee Rainie and Maeve Duggan, *Privacy and Information Sharing: 7: Scenario: Home activities, comfort and data capture*, Pew Research Center, January 14, 2016, *available at*

Only 27 percent of respondents found the scenario acceptable, while 55 percent found it not acceptable. An additional 17 percent of those surveyed responded that the acceptability of the scenario "depends" upon the "particulars of the arrangement."[6] One respondent noted that they would find the scenario acceptable depending upon the "details of the company's privacy statement:"

> "It would depend more precisely on the details of the company's privacy statement. What can they use the collected information for? And do they share it with third parties? If they can use the information for anything but controlling my house's HVAC [heating, ventilation and air conditioning], I would be very hesitant to participate."[7]

One can imagine any number of reasons a consumer would be interested in controlling the data collected and transmitted by the software that controls their smart thermostat. Data could be used by malicious parties to determine the optimal time to break into a home, by a former lover (think restraining order type) to determine when someone has a guest, or by an employer to determine if someone calling in sick was actually at home.

B. The use of copyright licenses on software-enabled consumer products erodes consumer control over privacy rights.

With the advent of software-enabled consumer products has come a new business model: the collation and distribution of mass quantities of data, both in the aggregate and on individual users. Consumers have little control over what data is collected, who can collect that data, and how that data will be used. This is a problem for consumers who do not want their data to be collected and sold to private companies, but also for those who would like their data to go towards research efforts that may have social benefits.

End User License Agreements (EULA) and privacy policies are notoriously inscrutable; they are lengthy, convoluted, and filled with legal jargon. One 2008 study estimated that an individual would require almost 250 hours, around 30 workdays, to read every privacy policy for every website they visited on the internet in any given year. The study valued the nationwide time to read privacy policies at $781 billion annually.[8]

Privacy policies for software-enabled consumer products are particularly concerning because they are often presented to users in the course of downloading or installing an app; most consumers will not take the time to search through websites to find privacy policies, but will click "I agree" and move on from the terms presented to them upon installation of an app.

Software-enabled consumer products have complex privacy policies, EULAs, and terms of sale or service that contain important information about privacy, allowed uses of products, and resale

---

http://www.pewinternet.org/2016/01/14/scenario-home-activities-comfort-and-data-capture/ (acccessed February 11, 2016).

[6] Ibid.

[7] Ibid.

[8] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. and Pol'y for the Info. Soc'y 540 (2008).

rights. We analyzed relevant documents containing privacy provisions for five software-enabled consumer products or brands, summarized in table 1 below. Specifically, we determined the word count of the document, the estimated time to read the agreement,[9] and the Flesch-Kincaid Reading Ease score, which measures readability of written text (the lower the score, the more difficult the text is to read; scores below 50 indicate college level and above, and scores between 50 and 60 indicate a high school graduate reading level).[10]

Table 1: Analysis of Privacy Documents

Product or Brand	Word Count	Estimated Reading Time	Readability Score
Fitbit[11]	3,485	14 minutes	54.1
Nest[12]	3,518	14 minutes	46.6
Apple products[13]	3,068	12 minutes	37.9
Philips Hue[14]	2,900	12 minutes	53.1
August[15]	3,290	13 minutes	51.2

The privacy policies listed above allow businesses to set the terms of what information is collected about users, and how that information is distributed and used. There are legitimate concerns that consumer privacy may be abused by third parties that have access to data collected in the course of use of a software-enabled consumer product, or that such data may be compromised by other malicious parties.

Strong privacy policies may also be important to prevent copyright holders from collecting data that could then be subpoenaed, seized, or hacked into by government agencies. James Clapper, the U.S. Director of National Intelligence recently admitted that the federal government may use data collected by smart devices to surveil persons.[16] The Copyright Office should

[9] Adopting the methodology of McDonald and Cranor, we assume the average reader reads at a rate of 250 words per minute. Note that we do not adjust the reading time according to readability score, nor do we make assumptions about the ability for end users to understand legal jargon. Our estimated reading time should be considered a minimum.

[10] Note that the Flesch-Kincaid scale does not account for the complexity of words, but rather measures the relationship of various syntactic elements. Thus, documents containing particular legal terms may be less readable than indicated by the score noted above.

[11] Fitbit, Privacy Policy, December 9, 2014, *available at* https://www.fitbit.com/legal/privacy-policy (accessed February 12, 2016).

[12] Nest, Privacy Statement for Nest Products and Services, June 17, 2015, *available at* https://nest.com/legal/privacy-statement-for-nest-products-and-services/ (accessed February 12, 2016).

[13] Apple, Privacy Policy, September 17, 2014, *available at* http://www.apple.com/legal/privacy/en-ww/ (accessed February 12, 2016).

[14] Philips, Privacy Notice for Hue, January 4, 2015, *available at* http://www2.meethue.com/en-us/privacy-policy/ (accessed February 12, 2016).

[15] August, Privacy Policy, August 31, 2015, *available at* http://august.com/legal/privacy-policy/ (accessed February 12, 2016).

[16] Spencer Ackerman and Sam Thielman, US intelligence chief: we might use the internet of things to spy on you, February 9, 2016, available at

consider the reform of policies related to the privacy implications of copyrighted software in the context of civil liberties concerns.

C. Proposal for the creation of a mechanism for third-party consumer advocates to represent the privacy interests of end users of software-enabled consumer products.

No matter have much effort goes into improving informed consent processes, the problems of too much complexity and too little time will remain.

In some cases, it may be feasible and appropriate to provide consumers of software-enabled consumer products to choose representation by entities/agents with appropriate legal and policy experience prior to their accepting the terms or conditions of any software in such products.

End users have neither the legal expertise nor the time to evaluate complex privacy and licensing agreements that govern their interactions with objects containing proprietary and copyright-protected software. Inevitably, those consumers waive important privacy rights merely by using an object in the course of their everyday lives. Many users would also be willing to authorize third-party use of the data collected from their interactions with software-enabled consumer products, but do not have the opportunity to shape the software license that governs their use of the copyrighted product. Both groups of consumers — those deeply concerned about incursions into their lives and those who would be willing to share potentially useful information about their use of products — would benefit from a system of advocates that could not only navigate the terms of such agreements, but in some cases negotiate with copyright holders on their behalf.

Our concerns about this issue are partly related to our interest in health related information produced through the use of products with software components. Rather than master the details of all issues in detailed consent forms, a consumer should have the option to electing an agent to act on its behalf, one that is considered trustworthy and competent to make decisions in the consumer's best interests.

The Copyright Office need not initially explore legislation to implement this system. One avenue would be to explore including requirements in government procurement contracts that would enable government employees who use software-enabled consumer products that were purchased with federal funds to engage in a system similar to the one described above.

The scope of this proposal is modest, and is similar to actions that have already been taken by the government and industry. For example, consumers now have the option of choosing the default search engine on their browser because of antitrust litigation against Microsoft. When consumers download new apps to certain mobile operating systems, they have a level of control over what information the app can access and share online.

In the future, the Copyright Office could explore legislation to expand this right to bring a third party privacy advocate to the broader consumer market.

---

http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper (accessed February 12, 2016).

II. The Trans-Pacific Partnership Provisions and Source Code Transparency

The Trans-Pacific Partnership contains a consequential provision for products that rely upon the operation of software in its Electronic Commerce Chapter.

Article 14.17 of the TPP concerns the transparency of software source code. This provision had not been debated, and was not widely vetted. The text reads:

> **Article 14.17: Source Code**
>
> 1. No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.
>
> 2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.
>
> 3. Nothing in this Article shall preclude:
>
> (a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or
>
> (b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.
>
> 4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.[17]

Under article 14.17, member parties to the TPP, including the United States, would not be allowed to compel the manufacturers of software-enabled consumer products (or, more broadly, software products) to disclose or transfer their source code for inspection prior to allowing the software or product onto the market. The provision would prevent regulatory authorities from examining mass market consumer products for security flaws, malicious code, or code designed to circumvent federal regulations.

It would not apply, however, to government procurement or "critical infrastructure," and does not interfere with contracts between private parties.

[17] Trans-Pacific Partnership Agreement, Art. 14.17, https://www.mfat.govt.nz/assets/_securedfiles/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf (accessed February 16, 2016).

Note that paragraph 1 of the article limits the scope of the provision to software source code that is "owned by a person of another party," implying a special form of protection for foreign-owned copyrighted software.

Application of article 14.17 could damage national security, consumer privacy, and harm competition and innovation.

In defending the provision, USTR indicated that companies were concerned about requests for source code from China. But since China is not a member of the TPP, the impact is to prevent the United States and other TPP member countries from insisting on open source code. The provision is somewhat narrow, it does not apply to government procurement, "critical infrastructure" (whatever that means), it is limited to mass market software, and it does not interfere with contracts between private parties, fact noted by the Software Freedom Law Center in its conclusion that the provision provides "no harm, no foul."[18]

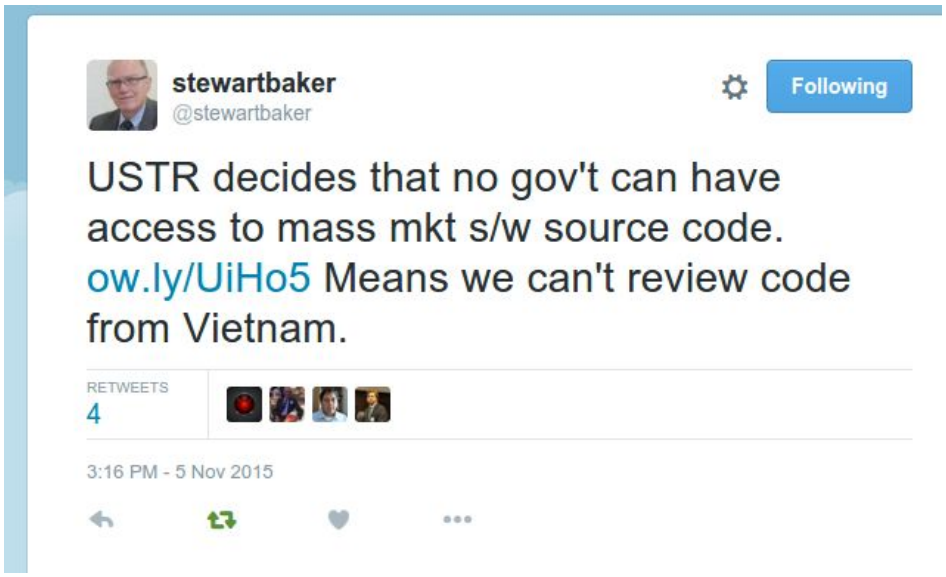
However, in the areas where the provision does apply, it provides an astonishingly broad attack on government authority to regulate software applications, including areas where security, privacy, fraud, interoperability or other issues are at play. Klint Finley of Wired was quick to question whether or not the provision would prevent governments from requiring manufacturers of automobiles or other things to open the code for certain software:[19]

> Volkswagen's infamous emissions-test-subverting software lurked in cars for years before it was discovered by regulators. The company got away with it for so long, in part, because it's hard to actually tell what's going on within the embedded computers of an automobile.
>
> One way to deal with the issue would be to require that certain types of companies, like automakers, release the software code that powers their products to the public, so that researchers could evaluate deceitful practices as well as security flaws. A less extreme solution, suggested by Zeynep Tufekci in the New York Times this year, would be to simply require automakers to release code to auditors, the same way the manufacturers of casino slot machines must open their code to gambling regulators.
>
> . . .
>
> The proposal includes an exception for critical infrastructure, but it's not clear whether software involved in life or death situations, such as cars, airplanes, or medical devices would be included.

[18] TPP Article 14.17 & Free Software: No Harm, No Foul, November 11, 2015. IP-Watch. http://www.ip-watch.org/2015/11/24/tpp-article-14-17-free-software-no-harm-no-foul/
[19] Klint Finley, Trade Pact Could Bar Governments From Auditing Source Code, November 5, 2015. Wired. http://www.wired.com/2015/11/trade-pact-could-bar-governments-from-auditing-source-code/

> Forcing companies to publish their source code won't necessarily solve the problem of cheating or buggy software. Huge security problems have been known to linger for years in open source projects that had too few security audits. And there are ways to encourage companies to release their source code that don't involve passing import laws. But the TPP, as written, would remove one powerful option in the fight to open the Internet of Things.

Others, including Stewart Baker, a former NSA General Counsel, commented that "USTR decides that no gov't can have access to mass mkt s/w source code. Means we can't review code from Vietnam."[20]



Stewart Baker was concerned about countries or criminals using the TPP provision to hide spyware aimed at people living the United States.

The United States has on more than one occasion required software publishers to open parts of their software code, in order to address competition concerns. In various cases involving Microsoft, the United States and the European Union has insisted on third party access to software APIs and protocols. Access to the source code of MySQL was a major issue in the EU competition review of the Oracle acquisition of Sun Microsystems.[21]

There is considerable interest today in requiring Google to be more transparent about its searching algorithms, or in ensuring that certain platforms, such as the Android operating system, are sufficiently open. And, as Klint Finley noted earlier, the explosive growth of the Internet of Things[22] will make interoperability, security, privacy, and other software related

[20] Baker inadvertently cited the wrong TPP chapter.
[21] Case No COMP/M.5529 – ORACLE/ SUN MICROSYSTEMS, January 21, 2010. http://ec.europa.eu/competition/mergers/cases/decisions/m5529_20100121_20682_en.pdf
[22] https://en.wikipedia.org/wiki/Internet_of_Things

issues increasingly more important, not to mention the more speculative but plausible dangers and risks that non-auditable source code will present in the future.

The non-transparency of software source code is of course a product of a non-transparent negotiation, and ironic evidence that secrecy presents risks — in this case, the risk that a few government officials will create a permanent rule that no one had a chance to debate on its own merits, a rule that will have unintended consequences and negative consequences for competition, privacy and security, and make it harder to detect and overcome fraud.

Software code imported from other countries would not be subject to the same scrutiny by regulators of code produced by businesses in the United States.

III. Copyright as a Barrier to Auditing Artificial Intelligence and Other Software Products that Potentially Pose Security Risks

Currently, most software-enabled consumer products have limited capabilities. While some products have the capacity to understand and react to human input, and to store basic information about users, such products do not have an advanced grasp of human interactions, and they have limited capacity to learn. As processors become faster and computer science researchers continue to increase the learning capacity of these machines, artificial intelligence could pose threats to national security and create new existential risks.

A particular concern is superintelligent artificial intelligence. Nick Bostrom, an academic philosopher who leads the Future of Humanity Institute and Strategic AI Research Center at the University of Oxford, has noted that "many leading researchers in AI place a 90 percent probability on the development of human-level machine intelligence by between 2075 and 2090."[23] Bostrom and other AI experts anticipate the eventual development of superintelligent artificial intelligence.[24]

As has been imagined in science fiction from Isaac Asimov to Philip K. Dick, human-level and superintelligent AI may not feel bound to the same ethical or legal constraints that humans are bound to. Like the aliens in the *Twilight Zone* episode "To Serve Man," superintelligent computers may have a different idea about the meaning of the word "serve" than humanity, or may develop the capacity to consider humans as inferior beings that should serve the interests of machines, themes that have been central to many science fiction novels and movies, but also highlighted by highly regarded experts in computer science.

In his seminal 2003 article "Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards," Bostrom warned that the development of a flawed artificial intelligence could significantly disrupt the course of human evolution and limit the future possibilities for humanity.

---

[23] Caspar Henderson, "Superintelligence by Nick Bostrom and A Rough Ride to the Future by James Lovelock," July 17, 2014, *available at*: http://www.theguardian.com/books/2014/jul/17/superintelligence-nick-brostrom-rough-ride-future-james-lovelock-review (accessed February 15, 2016).
[24] Ibid.

[25], views echoed by many others, including such prominent science and technology voices as Elon Musk and Stephen Hawkings.

Writing in the *Bulletin of the Atomic Scientist,* Edward Moore Geist said, "if artificial intelligence might not be tantamount to "summoning the demon" (as Elon Musk colorfully described it), AI-enhanced technologies might still be extremely dangerous due to their potential for amplifying human stupidity."[26]

The relationship between AI and software may be important. When machines write and modify software, is that expression protected by copyright? And, will governments or consumers have the right and/or ability to have access to, audit or modify the software code?

The Copyright Office should ensure that when HAL 9000 is invented, we have access to its source code to ensure its integrity.

Please direct all inquiries for this submission to Zack Struver at 202-332-2670 or zack.struver@keionline.org.

[25] Nick Bostrom, *Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards*, 9 J. Evolution & Tech. (2002), *available at*: http://www.nickbostrom.com/existential/risks.pdf (accessed February 16, 2016).
[26] Edward Moore Geist, Is artificial intelligence really an existential threat to humanity? Bulletin of the Atomic Scientist, August 9, 2015.