Comments Supporting Proposed Class 13 Exemption Under 17 U.S.C. § 1201
Computer Programs -- Security Research

March 9, 2021

Consumer Reports[1] submits this statement in support of clarifying the current exemption for enabling lawful, good-faith security research to find and correct security flaws or vulnerabilities in software-enabled products, to permit the disabling of functionalities that enable a product to obtain access to a personal information against the consumer's wishes.

As we have stated in previous submissions to the Copyright Office, and in our Digital Testing Standard launched in March 2017,[2] when a consumer purchases a product, the consumer should obtain genuine ownership of the product and its parts, including the ability to make effective use of the product, and the ability to effectively resell it.[3] We believe consumers should have the ability to use the products they have purchased in all these respects, as they see fit. We have successfully made this case with respect to mobile devices, both in Congress and before the Copyright Office. And we believe it also applies here.

In our view, the prohibition in section 1201 of the Digital Millennium Copyright Act against circumvention of technological protection measures has proven, in experience, to be an overbroad response to a concern that the digital age would usher in a massive deluge of copyright infringement, for which drastic new countermeasures were needed. Instead, its proliferating use to protect access to software that enables and governs – and restricts – the functioning of everyday consumer products in which it is embedded, and their interoperability with other products, causes far-reaching harm to fundamental consumer rights.

We recognize the value of copyright law in nurturing and protecting incentives for innovation, both generally and in particular with respect to computer software. At the same time, it

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers. CR has long been engaged in promoting consumer interests in the DMCA triennial reviews, particularly with respect to the exemption for unlocking mobile devices, both before the Copyright Office and in Congress.

[2] The Digital Testing Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use every day.

[3] *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.

is important that the monopoly rights conferred on creators by the copyright laws be kept appropriately contained, so they do not spill over into broader, unjustified and counterproductive restraints on competition and consumer choice, and do not undermine long-established, fundamental rights and expectations of consumers regarding their ownership and dominion over the products they have lawfully acquired. Beyond these immediate effects on consumer rights and expectations, broader innovation is impeded if a product's manufacturer is given inordinately sweeping power to control how it is used once it has been released into the marketplace.

We also recognize that some methods of accessing software could potentially have serious implications for safety and for privacy. Ensuring product safety has been a bedrock objective of Consumers Reports' mission since its founding over 80 years ago. Safety must of course be at the forefront of concerns carefully monitored and vigorously addressed as we move to increasingly complex and interactive technologies. Likewise, pro-consumer data privacy and data security practices must be a top priority, for manufacturers and for policymakers; companies should compete and be held accountable on the basis of the data privacy and security protections they incorporate into the design of their products and services, and consumers should receive sufficient information to exercise informed choices.

But these considerations generally do not implicate copyright law, and generally fall outside the Copyright Office's expertise. And it is important that they not be permitted to be used by companies as a pretext for blocking competition and consumer choice and undermining rights of ownership. So in our view, they should generally not be part of the Copyright Office's own deliberations in considering exemptions under section 1201. They are appropriately dealt with here by requiring that the research be conducted in a controlled "environment designed to avoid any harm to individuals or the public," and not be in violation of other applicable laws, enforced by other authorities whose missions and expertise are directed at those issues.

Moreover, in this instance, the proposed exemption is designed to address a significant security vulnerability that the product designer or seller may not have an interest in addressing.

This exemption has proven very beneficial to consumers in removing this obstacle to lawful, good-faith research into improving the security of electronic devices they use and depend on. One of the most significant security vulnerabilities is the capability of a software-enabled product to access personal information without the consumer's permission. We therefore support this clarification.

Respectfully,

George P. Slover, Senior Policy Counsel
Maureen Mahoney, Senior Policy Analyst
Consumer Reports
1101 17th St., NW, Suite 500
Washington, DC 20036
(202) 462-6262