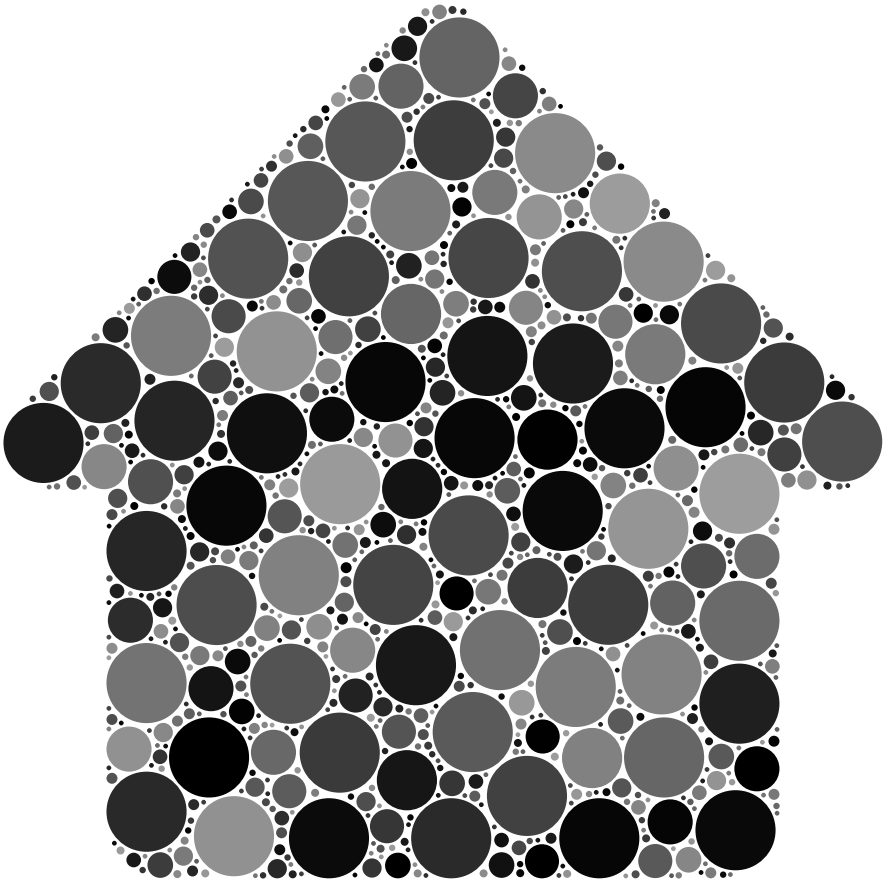

WHO CONTROLS YOUR PHONE:
CLIENT-SIDE SCANNING AND THE FUTURE OF OWNERSHIP

BY
JOHN BERGMAYER

John Bergmayer is Legal Director at Public Knowledge, specializing in telecommunications, Internet, and intellectual property issues. He advocates for the public interest before courts and policymakers, and works to make sure that all stakeholders, including ordinary citizens, artists, and technological innovators, have a say in shaping emerging digital policies.

Visit www.competitionpolicyinternational.com for access to these articles and more!

WHO CONTROLS YOUR PHONE: CLIENT-SIDE SCANNING AND THE FUTURE OF OWNERSHIP

By John Bergmayer

The swift rise of Generative AI has brought notable benefits to consumers. Despite this, rising concerns about potential harms and a surge of U.S. litigation, threaten AI's continued progress. This article examines ongoing legal challenges against OpenAI and Stability AI, underlining the unresolved legal issues AI providers face. A close look at these cases shows that fears surrounding Generative AI's alleged consumer harms do not present new legal dilemmas. Existing legal frameworks effectively filter out baseless claims unrelated to Generative AI's nature. Instead, this article argues that lawmakers should focus on promoting the advancement and deployment of Generative AI rather than altering current legal structures to facilitate its demise.

Everyone reading this probably has a smartphone nearby. In their pocket, on their desk, or in their hands. But who really owns them? Who gets to say what they do?

These pocket-sized supercomputers can be tools for ubiquitous surveillance, or strong user privacy. The only difference is the code that runs on them. Every tap, every photo, every message, every app download tells a story about us. Without proper safeguards, this story can be told (and sold) to others without our knowledge or consent. It's a story that might be used to influence our decisions, shape our behaviors, determine our credit-worthiness, or whether we get a job. Or in some places, put us in jail.

Smartphones can also be tools for protecting privacy: they can instantaneously encrypt messages and data to keep them from being seen by anyone but the intended recipient. They can connect us to anonymous networks, ensuring our browsing habits remain private. They can alert us when applications or websites try to access our personal information without consent.

The difference between these two worlds is just software. Today, more than the law, it's software that determines ownership. That is because ownership isn't just about who physically possesses the device; it's about control. Even though you've paid for your smartphone, in a sense it is not really "yours" as long as the operating system, the preinstalled apps, and the data they collect are all controlled by corporate giants.

One way that technology can be used to enhance, rather than limit user privacy is through end-to-end encryption ("E2EE"). End-to-end encryption ensures that the contents of our communications – be they messages, voice calls, video calls, or even file transfers – are accessible only to the sender and the intended recipient. No one else, not even the service provider or platform hosting the communication, can decrypt and read the encrypted data. This serves as a critical safeguard against unauthorized access, whether it's by hackers, corporations, governments, and even rogue employees of service providers or law enforcement agencies. Popular messaging apps like WhatsApp, Signal, and iMessage each implement this form of strong encryption.

Unlike a lock on a house or a safe, the digital locks that encrypt E2EE messages are truly unbreakable (provided they are implemented flawlessly – no software is free of bugs). Even if served with a warrant, service providers like Apple or Meta cannot grant law enforcement access to E2EE-encrypted messages, not as a matter of policy, but as a matter of possibility. They don't have the keys to decrypt them, and without the key,[2] all computers in the world, calculating for all time, can't decrypt them.

Law enforcement, national security, and other interests have objected to this. Downplaying privacy concerns, these stakeholders admonish that E2EE allows criminals to shield their behavior, and have argued that encrypted communications systems must be designed to allow for "exceptional" access by law enforcement, subject to warrant requirements. Critics call these proposals "backdoors." However, most encryption experts maintain that designing a system to allow for anyone other than the intended recipient to read a message, no matter how carefully done, would inevitably weaken the encryption that everyone else relies on. They argue that the only way to achieve privacy online is through E2EE, not through less-private systems; systems that, in the end, depend on the internal processes of companies and governments to keep out eavesdroppers, snoops, and stalkers.

Recently, advocates of increased monitoring of communications have hit upon a new approach: client-side scanning. Under proposals like this, the device would scan its own contents – such as messages, photos, and documents – against a database of known illegal content or digital markers. If there's a match, the device would either block the content, notify the user, or in more extreme cases, alert law enforcement.

On the surface, client-side scanning seems like a reasonable compromise. Instead of weakening encryption, it could offer a way for tech companies to police content without having to decrypt messages. The idea is that client-side scanning would help in the prevention and reporting of illegal content, like child exploitation materials, without compromising the overall security of encrypted communications.

> ***"The difference between these two worlds is just software. Today, more than the law, it's software that determines ownership***

But on further inspection, client-side scanning undermines E2EE as much as any "backdoor" approach. Compromising the "endpoints" of an encrypted system, and scanning materials either before they are encrypted, or after they are decrypted on the recipient's device, effectively sidesteps the robust security provided by E2EE. This form of undermining E2EE could even be worse than simple backdoor proposals. Like adding a screen door to a fortress while the walls remain impenetrable, a single clear entry point can defeat the entire purpose of a secure system.

2 Or breakthroughs in quantum computing – but even so, encryption techniques that can resist hypothetical attacks from quantum computers already exist.

Client-side scanning creates a new realm of potential vulnerabilities, as devices become valuable targets for hackers seeking to manipulate the scanning process or database. This could, in turn, lead to wrongful flagging of content. Systems that are designed to scan for child exploitation materials can easily be repurposed to scan for other things – materials relating to political dissent, sexual behavior, or even copyright infringement. Moreover, the constant surveillance by one's own device would foster an environment of mistrust, potentially deterring users from storing personal or crucial information on their devices.

So, when we ask of our smartphones "Who really owns them?," we are asking who controls them, and who do they work for? The lines of code that determine whether our phones serve as tools of privacy or nodes of surveillance are part of a power dynamic where technology companies try to maintain control over the products they sell, even after they've sold them. This context of decreasing user autonomy, where people spend hundreds of dollars (or more) on devices that are not truly their own, can be seen in many areas: software updates that are mandatory and might change the phone's functionalities; proprietary app stores that dictate which applications you can or cannot install; restrictions on resale; and warranties that are claimed void if you try to repair your device yourself or use non-official parts. The gradual whittling away of what it means to "own" a device is what makes client-side scanning proposals plausible in the first place.

01

UNCOMPROMISED END-TO-END ENCRYPTION IS NECESSARY TO PROTECT PRIVACY

Privacy is a human right. Article 12 of the UN's Universal Declaration of Human Rights states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence[.]" The United States Constitution, although not explicitly mentioning the word "privacy," has been interpreted by the courts to offer protection in matters of personal privacy. The Fourth Amendment, for instance, protects citizens from unreasonable searches and seizures; similarly, the First Amendment protects the freedom of association and the freedom of speech, with both freedoms directly implicating privacy. The Fourteenth Amendment's Due Process Clause further ensures that individual liberties, including certain privacy rights, are safeguarded against unwarranted government actions.

In their seminal 1890 article "The Right to Privacy," Samuel D. Warren and Louis D. Brandeis contended that privacy is a natural right, and its violation is an affront to individual dignity. Thinkers such as Martha Nussbaum, Alan Westin, Beatte Roessler, Daniel Solove, and many others, have argued that a private, personal sphere is essential for an individual to lead a fulfilling life. They show that privacy is fundamental to human flourishing, not a mere luxury, or something to be traded away. But a fundamental right like that to privacy is hollow absent practical ways to achieve it.

In some cases, fundamental rights can be achieved multiple ways. For example, Article 13 of the Universal Declaration of Human Rights states that "Everyone has the right to freedom of movement … within the borders of each state." This does not mean that people have a specific right to ride on a train, or drive a car, or ride in a helicopter or a blimp. But the right would be infringed if someone was denied access to any form of transportation at all: forbidding someone from realizing a right is the same as denying it. The right to health implies access to medical care, and the right to education means that people must be allowed access to schools, books, libraries, and even the internet. In many societies the means necessary to achieving fundamental human rights such as health care and education are considered public services.

Online, E2EE provides an indispensable way to preserve the fundamental right to privacy. Without E2EE, our digital lives can be an open book for anyone with enough technical know-how to read it. It's a stark contrast to traditional privacy violations. In the past, one might eavesdrop on a conversation or intercept a letter, but the scale of potential exposure was limited. Today, with the amount of data we entrust to our digital devices, the potential for mass surveillance and exploitation under a client-side-scanning regime is unparalleled.

Forms of encryption short of full E2EE do not adequately protect privacy. They generally depend, not on mathematics, but on internal company or government procedures to keep data private. The premise is that companies or governments will collect or have the ability to access private data, which they promise not to abuse. This falls short in a number of ways.

- First, relying solely on internal procedures means trusting that all employees or individuals involved are trustworthy and do not have any malicious intent. This opens the door for potential insider threats, where an employee or associate with access could abuse their privileges for personal gain, blackmail, or even corporate espionage.

- Second, internal processes are susceptible to human errors. Even if no one within an organization

intends to misuse the data, mistakes can still be made. For instance, misconfigurations can inadvertently expose sensitive data, or a well-intended employee might accidentally share data with unauthorized individuals.

- Third, even the most stringent internal protocols cannot guard against external threats like cyberattacks. In recent years, several high-profile data breaches have demonstrated that even corporations with vast resources can fall victim to cyber threats. When data protection relies on company processes rather than solid encryption, the risk of breach increases.

- Fourth, internal processes can be subject to changes. Company policies might change with new management or in response to financial pressures. What's promised as a strict privacy policy today can easily be altered tomorrow, leaving users exposed.

- Fifth, governmental influence or legal requirements can compromise these internal procedures. Governments, particularly those with authoritarian tendencies, can pressure companies to hand over user data. Without E2EE, complying with these demands becomes far easier, undermining the trust users have in a platform.

The fundamental difference between end-to-end encryption and other forms of securing data and communications is crucial. One is a promise, dependent on trust, processes, and good intentions. These are not enough. The other is a mathematical certainty.

Granting law enforcement exceptional access to encrypted communications would be the start of a slippery slope. Today, the argument might be about combating severe crimes like terrorism or child exploitation. But what stops the scope from expanding tomorrow? If access is granted for one type of crime, it can set a precedent. Over time, the reasons for access could expand to lesser crimes, civil offenses, or even political dissent. Further, the internet is global. If one country mandates exceptional access, it affects users worldwide. Additionally, it could lead other countries to demand similar access, potentially enabling oppressive regimes to spy on dissidents, journalists, and political opponents. The cascading effects of one country's policy could have profound impacts on global privacy norms.

With the power to access encrypted communications, there's always the risk of overreach or abuse. Law enforcement and national security concerns have often been used as a pretext for civil liberties violations. Further, this isn't just about the potential misuse by law enforcement officers, but also the risk of this access falling into the wrong hands. Rogue employees, hackers, or external adversaries could exploit this access for various malicious intents, ranging from personal blackmail to espionage.

Technically speaking, creating a "backdoor" for law enforcement inherently creates a vulnerability in an E2EE system just as much as a software bug does. While the intent might be to use this backdoor responsibly and only when necessary, its mere existence makes the system more vulnerable to cyber-attacks. Hackers, whether state-sponsored, part of organized crime, or independent, are continuously on the lookout for vulnerabilities. A backdoor would be a tempting target. Further, encryption relies on mathematical principles. If there's a way to bypass or weaken this encryption in one place, it can be done everywhere. You can't create a vulnerability that only "good guys" can exploit.

E2EE is not just one way that people can protect their privacy online. It's an indispensable tool. Weakening or banning E2EE therefore amounts to an abridgment of the fundamental right to privacy, and proposals to do so should be rejected. There are ways to enforce the law, protect national security, and protect vulnerable people that do not abridge ordinary people's fundamental rights.

02

CLIENT-SIDE SCANNING IS NOT THE SOLUTION

Broadly speaking, client-side scanning ("CSS") means having a device inspect its own contents. Instead of scanning data on centralized servers (like those of a service provider), the scanning happens right where the data resides: on the user's device.

In 2021 Apple put forward a proposal for client-side scanning that was aimed at curbing the spread of Child Sexual Abuse Material ("CSAM") on its platforms.[3] The plan was to scan photos that users stored in iCloud or sent in iMessage for CSAM and make reports about such uploads available to law enforcement. The technology designed for this purpose was called NeuralHash, and it would compare cryptographic hashes of photos in individual devices' iCloud photo libraries with a database of hashes of known CSAM material.

However, Apple faced substantial backlash from technologists, security researchers, and digital rights groups, who argued that this approach posed significant security and privacy risks. Fourteen of the world's most prominent computer

3 CSAM Detection, Technical Summary (August 2021), https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf.

security and cryptography experts issued a paper opposing the use of CSS due to these concerns.[4] In response to this backlash and the concerns raised, Apple decided to postpone and eventually cancel its client-side scanning plans.

But governments are going forward. Since 2022 the European Commission has been advocating for a new law that critics call "Chat Control," that would require messaging providers to scan all private messages. Patrick Beyer, a member of the European Parliament, described this as the "proposed indiscriminate mass scanning of private communications of millions of citizens not even remotely connected with crime."[5] Despite an aggressive lobbying push backed in part by surveillance technology vendors,[6] this measure recently failed to advance.[7]

In the United States, for the past few years Senators Blumenthal and Graham have been trying to win support for the "EARN IT Act," a bill that would increase platform liability for content. In response to one version of the bill, I wrote that "The convoluted process it sets up appears designed to discourage platforms from allowing users to secure their communications."[8] Since its first introduction, Joe Mullin from the Electronic Frontier Foundation writes, "Under pressure, the bill sponsors did add language that purports to protect encryption. But once you take a closer look, it's a shell game. The bill clearly leaves room to impose forms of 'client-side scanning,' which is a method of violating user privacy by sending data to law enforcement straight from user devices, before a message is encrypted."[9]

Recently, the UK enacted its Online Safety Act[10] designed to tackle the dissemination of CSAM through mandating that all messages be scanned "whether communicated publicly or privately." After substantial pushback from technologists and privacy experts, including statements from Meta and Signal that they would prefer to exit the UK market than undermine the privacy of their service, the government decided not to enforce the law.[11] Apple was key in lobbying against a proposal that was consistent with its own earlier client-side scanning plans.[12]

The potential upsides of client-side scanning explain its appeal to some policymakers. If implemented with care, CSS could, in theory, ensure that only content matching specific criteria is flagged, without exposing non-matching content. Since the scanning happens on the device, data doesn't need to be sent to external servers for analysis. This could reduce data transmission and server-side processing requirements, as well as carrying a privacy benefit in itself. In some cases, something like client-side scanning can be beneficial. This is how devices scan for malware, for instance. But that is an instance of the technique being used to benefit users, not monitor and potentially report on them.

"In the United States, for the past few years Senators Blumenthal and Graham have been trying to win support for the "EARN IT Act," a bill that would increase platform liability for content

4 Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso, Bugs in our Pockets: The Risks of Client-Side Scanning (October 2021).

5 Patrick Breyer, Chat Control 2.0: EU governments set to approve the end of private messaging and secure encryption (October 2023), https://www.patrick-breyer.de/en/chat-control-2-0-eu-governments-set-to-approve-the-end-of-private-messaging-and-secure-encryption/.

6 Giacomo Zandonini, Apostolis Fotiadis, & Luděk Stavinoha, 'Who Benefits?' Inside the EU's Fight over Scanning for Child Sex Content, Balkan Insight (September 2023), https://balkaninsight.com/2023/09/25/who-benefits-inside-the-eus-fight-over-scanning-for-child-sex-content/.

7 David Meyer, Privacy-busting 'chat control' plans rejected by European Parliament as CSAM law heads into final stretch, Fortune (October 2023), https://fortune.com/europe/2023/10/26/eu-chat-control-csam-encryption-privacy-european-commission-parliament-johansson-breyer-zarzalejos-ernst.

8 Public Knowledge Urges Congress to Support User Privacy and Security by Rejecting EARN IT Act (February 2022), https://publicknowledge.org/public-knowledge-urges-congress-to-support-user-privacy-and-security-by-rejecting-earn-it-act/.

9 Joe Mullin, The EARN IT Bill Is Back, Seeking To Scan Our Messages and Photos, EFF (April 2023), https://www.eff.org/deeplinks/2023/04/earn-it-bill-back-again-seeking-scan-our-messages-and-photos.

10 Jon Porter, The UK's controversial Online Safety Bill finally becomes law, The Verge (October 2023), https://www.theverge.com/2023/10/26/23922397/uk-online-safety-bill-law-passed-royal-assent-moderation-regulation.

11 UK will not immediately enforce disputed Online Safety Act provision (September 2023), https://iapp.org/news/a/uk-will-not-immediately-enforce-disputed-online-safety-act-provision/.

12 Jon Porter, Apple says proposed UK law 'poses a serious threat' to end-to-end encryption, The Verge (June 2023), https://www.theverge.com/2023/6/27/23775356/apple-online-safety-bill-statement-encrypted-messaging-apps-e2ee-end-to-end.

The risks of CSS outweigh its potential benefits, and Apple, the UK, and the EU were right to put their plans to the side. People's devices should not be turned into surveillance tools, even if the target of surveillance is, at first, people engaging in heinous crimes.

One inherent flaw with CSS is the potential for false positives. No algorithm is perfect. With billions of devices and an even greater number of files, even a minuscule error rate can result in thousands of wrongful accusations, leading to unjust investigations or punishments. An innocent family photo or a benign document could be flagged, causing unnecessary distress to the individual involved. This already happens with content that is scanned in the cloud, as the New York Times has reported.[13] CSS would greatly increase the likelihood of such mistakes. Beyond mistakes, client-side scanning systems can be targeted, hacked, and abused. Researchers have demonstrated "it is also possible to taint the database of images of known child sexual abuse material (CSAM), allowing an adversary to trick the client-side scanning system to also trigger an alarm for other, non CSAM, material."[14] Moreover, just like any other software, CSS tools can have vulnerabilities. These could be exploited by malicious actors to gain unauthorized access to personal data or even to plant incriminating evidence on an individual's device.

Even more concerning is what CSS can turn into. While the initial intent might be to target explicit forms of illegal content, it's a small leap from there to scanning for other types of information. Governments with authoritarian tendencies might use this technology to target minority populations, or political dissidents, and perhaps to even identify individuals participating in protests or opposition movements. Today's database of illegal images could easily morph into tomorrow's database of banned books, prohibited religious texts, or anti-government speech. Rightsholder groups are already demanding that the technique be used to limit the unauthorized streaming of sports matches, asking Google to scan for and disable apps installed on people's phones.[15]

Leading experts have concluded that:

> CSS neither guarantees efficacious crime prevention nor prevents surveillance. Indeed, the effect is the opposite. CSS by its nature creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic. There are multiple ways in which client-side scanning can fail, can be evaded, and can be abused.[16]

The framework for CSS once in place can be extended, enhanced, and exploited. It sets a dangerous precedent, enabling not only governments but also corporations, hackers, and other entities to potentially misuse this power. It should not be implemented.

03

CLIENT-SIDE SCANNING IN THE CONTEXT OF DECREASING OWNERSHIP NORMS

Client-side scanning is emblematic of a broader trend wherein the tangible and intangible items we "buy" don't truly belong to us.[17] Just as client-side scanning can transform our personal devices into surveillance devices without our consent, other practices by manufacturers and software developers can erode traditional concepts of ownership.

Consider the right-to-repair movement — and the fact that such a movement is even necessary. Historically, when you purchased a product, it was yours to tinker with, repair, or modify. But now, many companies argue that opening up a

13 Kashmir Hill, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, NY Times (August 2021), https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html.

14 Tainting the CSAM client-side scanning database (October 2023), https://blog.xot.nl/2023/10/11/tainting-the-csam-client-side-scanning-database/index.html.

15 Andy Maxwell, LaLiga "Talks to Google" About Deleting Piracy Apps From a Million Phones (September 2023), https://torrentfreak.com/laliga-talks-to-google-about-piracy-apps-from-a-million-phones-230924/.

16 Bugs in our Pockets 1.

17 See Aaron Perzanowski & Jason Schultz, The End of Ownership: Personal Property in the Digital Economy (2016), for an excellent overview of this topic.

device or making unofficial repairs can void warranties,[18] violate user agreements, or even violate copyright law.[19] Companies erect barriers, through proprietary screws or software locks, effectively keeping users out of their own devices — forcing them to either just buy new ones when they break, or go through manufacturer-approved, costly repair channels. Devices are sometimes paired to specific parts making replacements difficult or impossible.[20] Legal barriers mean that the public has to petition the Copyright Office just to repair video game consoles. Jurisdictions such as California are beginning to enact laws to make it easier for consumers to repair their own devices, and to open up the repair market.[21]

But right-to-repair laws don't address all the barriers to reselling and repairing devices, such as activation locks, another tool in the arsenal of manufacturers aiming to restrict secondary markets and control the use of devices post-sale. These locks, justified as anti-theft measures, require the original user's credentials to unlock a device after it's been reset. While this feature can deter theft, it also renders devices inoperable if the original user's credentials are lost or if they didn't remove their account before selling or donating the device.[22]

Another example is the ownership of copies of copyrighted works. Traditionally, when someone purchased a book or a CD, they had the right to lend it, sell it, or give it to someone else. This is known as the "first sale doctrine." It means that once a copyrighted work is sold or given away, the copyright holder's control over that specific copy ends. However, in the digital age, this concept has become muddled. Today, people often do not buy physical copies of media — they might purchase downloads of music, games, movies, and ebooks. These typically come with legal and technical restrictions on what users can do with them which do not apply to traditional media. For instance, you can't resell a digital book or song in the same way you can a physical one — and "technical protection measures" (TPMs), which are unlawful to circumvent,[23] might even prevent you from making lawful fair uses of content, such as excerpting portions of it for criticism or commentary.

Physical media such as Blu-Ray discs come laden with TPMs, as well — as do consumer products that have nothing to do with protecting copyrighted content at all. TPMs are used to restrict repair, to force coffee machine owners to use particular brands of coffee pod,[24] or to purchase printer ink on a subscription plan.[25] Even when subscriptions are not forced via TPMs, subscription-based business models are eroding ownership norms. Video and music subscriptions are more popular today than a la carte purchases, where users buy access to a catalog of music or video online. While this gives people access to more creative works than ever before, it also means that access to them can be lost at any moment. Further, major software packages like Microsoft Office and the Adobe Creative Suite are sold primarily as subscriptions, rather than one-time purchases. Many people resent having to pay a monthly fee to keep using the tools they need for their work, rather than just buying a one-time purchase. In any event, modern software and devices often rely on cloud access, and periodic software updates just to keep working. Even if devices or software can be resold or transferred, they might stop working at any moment.

> ***Client-side scanning is emblematic of a broader trend wherein the tangible and intangible items we "buy" don't truly belong to us***

18 FTC Staff Warns Companies that It Is Illegal to Condition Warranty Coverage on the Use of Specified Parts or Services (April 2018), https://www.ftc.gov/news-events/news/press-releases/2018/04/ftc-staff-warns-companies-it-illegal-condition-warranty-coverage-use-specified-parts-or-services.

19 Public Knowledge Joins Fight to Overturn Obscure Copyright Law Limiting Right to Repair (January 2022), https://publicknowledge.org/public-knowledge-joins-fight-to-overturn-obscure-copyright-law-limiting-right-to-repair/.

20 Wilfred Chan, California's new right to repair law fails to stop the 'parts pairing' loophole, Fast Company (October 2023), https://www.fastcompany.com/90967234/californias-new-right-to-repair-law-fails-to-stop-the-parts-pairing-loophole.

21 Elizabeth Lopatto, Right-to-repair is now the law in California (October 2023), https://www.theverge.com/23910066/right-to-repair-law-newsom-california-sb-244.

22 Matthew Gault, Perfectly Good MacBooks from 2020 Are Being Sold for Scrap Because of Activation Lock, Motherboard (January 2023), https://www.vice.com/en/article/xgybq7/apple-macbook-activation-lock-right-to-repair.

23 In the copyright context "technical protection measures," as defined by 17 U.S.C. § 1201, are often referred to as Digital Rights Management ("DRM"). This law makes it unlawful to "traffic" in tools for circumventing TPMs, and unlawful to circumvent TPMs unless an exception has been granted by the Librarian of Congress.

24 Chris Davies, Keurig 2.0 Pod DRM Will Lock Out Unofficial Coffee Pods, SlashGear (Mar. 3, 2014), https://www.slashgear.com/keurig-2-0-pod-drm-will-lock-out-unofficial-coffee-pods-03319137/.

25 Matthew Lynch, HP's Ink Subscription Has DRM That Disables Your Printer Cartridges, The Tech Edvocate (Sept. 27, 2022), https://www.thetechedvocate.org/hps-ink-subscription-has-drm-that-disables-your-printer-cartridges/.

The erosion of ownership, and its implications, might be most apparent with software, and devices with embedded software. When purchasing a game console, smartphone or tablet, you might own the hardware, but the software, encompassing the operating system and apps, is said to be merely "licensed" to you. For example, the Nintendo Switch user agreement says "The Software is licensed, not transferred to you," and Apple states that iPhone system software, "including Boot ROM code, embedded software and third party software[]...whether in read only memory, on any other media or in any other form (the Original Apple Software and Apple Software Changes are collectively referred to as the "Apple Software") are licensed, not sold, to you by Apple Inc."[26] Even with tangible software purchases, like game cartridges or discs, users are often regarded as "licensees" rather than owners. This distinction has a few implications. The Copyright Act[27] states that software copy owners have the right to make certain additional copies without permission of the copyright owner, or having to justify these copies as fair use. This includes backup/archival copies, and "essential step" copies that are needed to use the software. This was initially seen as allowing for software installation — for example, installing software from a CD onto a hard drive involves making a new copy. Because some courts have concluded that merely using software creates new "RAM copies"[28] of the software in the computer's memory, this means that simply using devices with embedded software can implicate copyright. This category includes household appliances and cars as well as smartphones and computers.

But the Copyright Act's grant of rights to owners of copies does not apply if software or device vendors can assert—and if the legal system accepts—that buyers never really "owned" what they thought they purchased to begin with.[29] This is how software companies can assert that simply using software or devices in ways they don't like constitutes copyright infringement.[30] By conditioning permission to make "essential step" RAM copies (using a device or software) on the user accepting various terms and conditions, they can claim that any violation of those terms is not just a contract dispute, but copyright infringement, which carries steep statutory damages and is even potentially criminal.[31] Additionally, only the lawful owners of copies of copyrighted works can benefit from the first sale doctrine. Someone who steals books or CDs from a warehouse and fences them is guilty not just of theft, but is unlawfully "distributing" copies in violation of the Copyright Act. If software copies or devices are not "owned," then this is true of innocent potential resellers as well.[32] What seems like a technical point about legal terminology in the context of software can have profound effects on secondary markets, e-waste, and people's ability to continue to use and repurpose their electronic devices.

Like client-side scanning, these barriers serve to undermine the ownership of a device, turning people into mere users of the products they've ostensibly purchased. While not every issue stemming from eroding norms of ownership is as grave as someone being arrested because his phone falsely flagged content, the viability of client-side scanning proposals, the reduction or elimination of secondhand markets, and the necessity of the right-to-repair movement, are part of a trend where distant companies are the true "owners" of many of the things around us.

"But the Copyright Act's grant of rights to owners of copies does not apply if software or device vendors can assert—and if the legal system accepts—that buyers never really "owned" what they thought they purchased to begin with

26 iOS 16 Terms of Service, https://www.apple.com/legal/sla/docs/iOS16_iPadOS16.pdf.

27 17 U.S.C. § 117.

28 *Mai Systems v. Peak Computer*, 991 F. 2d 511 (9th Cir. 1993); see also Aaron Perzanowski, Fixing RAM Copies (2010), https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1045&context=faculty_publications.

29 The Copyright Act is clear that "copies" are material objects, 17 U.S.C. § 101, and typically physical objects cannot be "licensed" — they can be owned, lent, leased, or borrowed, for instance. A "license" is legal permission to do something that would otherwise be unlawful. A movie theater needs a license to publicly display a movie even if it lawfully owns the film reels, since "public performance," like making new copies, is one of a copyright owner's exclusive rights. But you do not need a license to read a book or watch a movie at home, and if you own a copy of software, you don't need to accept a license to lawfully use it. However due to judicial interpretations of copyright law, someone who has lawfully acquired a copy of software does not necessarily have the right to even use it, much less resell it, because they are not an owner of a copy. See *Vernor v. Autodesk*, 621 F.3d 1102 (9th Cir. 2010).

30 Sherwin Siy, MDY v. Blizzard: Cheating at WoW may be bad, but it's not copyright infringement (May 2008), https://publicknowledge.org/mdy-v-blizzard-cheating-at-wow-may-be-bad-but-its-not-copyright-infringement/.

31 17 U.S.C. § 506.

32 See *Vernor v. Autodesk*, 621 F.3d 1102 (9th Cir. 2010).

04
CONCLUSION

Client-side scanning is a bad idea that would eliminate user privacy and would not help fight crime. Debates over consumer use of strong encryption have been ongoing since the 1990s, but this new front in the debate — proposals to turn users' own devices into tools that monitor them for potential lawbreaking — is likely only possible in the context of decreased user control over and ownership of everyday devices. ■

> ***Client-side scanning is a bad idea that would eliminate user privacy and would not help fight crime***

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL