TECHFREEDOM
LAW FOR A DYNAMIC FUTURE

771.200.4997
Washington, DC
techfreedom.org

August 31, 2023

The Honorable Buffy Wicks
1021 O Street, Suite 4240
Sacramento, CA 95814

The Honorable Heath Flora
1021 O Street, Suite 4730
Sacramento, CA 95814

The Honorable Rebecca Bauer-Kahan
1021 O Street, Suite 6320
Sacramento, CA 95814

The Honorable Jesse Gabriel
1021 O Street, Suite 5220
Sacramento, CA 95814

The Honorable Josh Lowenthal
1021 O Street, Suite 5130
Sacramento, CA 95814

Dear Assembly Members Wicks, Flora, Bauer-Kahan, Gabriel, and Lowenthal:

As scholars of online free expression and privacy, we commend you for revising AB-1394[1] to avoid imposing liability on online platforms merely for offering end-to-end encryption (E2EE) or for refusing to scan all user communications. An earlier version would have effectively coerced such infringements upon the rights of law-abiding citizens to communicate privately. We urge you not to revert to that version.

Your bill revises Section 3345.1(g)(1) of California's civil code to impose civil liability on online platforms that "facilitate, aid, or abet commercial sexual exploitation" (CSE). The original bill included a constructive knowledge standard ("recklessly, or negligently") while the current version requires actual knowledge ("knowingly"). This distinction is vital. If courts can find a platform was "reckless" or "negligent" in transmitting CSAM or facilitating CSE because its use of strong encryption left it unable to detect and stop such messages, the net effect would be nearly the same as explicitly imposing liability for offering encryption. Few, if any, platforms would risk offering E2EE if they faced liability not for CSE they knew about, but for content plaintiffs allege they *should* have known about.

A platform might still offer what it called E2EE—after all, users increasingly expect "strong encryption" as the industry standard[2]—yet try to mitigate its liability by short-circuiting that encryption on the client-side (i.e., on the device). While communications might be encrypted

---

[1] A.B. 1394, 2023–2024 Reg. Sess. (CA 2023), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1394.

[2] *See, e.g.*, Jack Nicas et al., *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, N.Y. TIMES (Jan. 13, 2021), https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html.

in transit, they could be scanned prior to being encrypted and sent or after being received and decrypted. This would largely defeat the purpose of E2EE. It would also put user privacy at risk: client-side scanning could be used to create an architecture of surveillance by which the devices of all users could spy on them, reporting to centralized servers when the device sends or receives certain kinds of communications.[3]

Either way, the privacy and security of all law-abiding users would suffer. Even worse, a constructive knowledge standard would also jeopardize prosecutions of the very criminals the bill aims to thwart: courts would likely conclude that forcing providers to retain the ability to decrypt communications, or to scan user communications on devices, is tantamount to coercing them to conduct warrantless searches.[4] This would trigger the Fourth Amendment's requirement that platforms obtain a warrant from a judge upon a finding of probable cause before they search user communications.[5] While platforms would, *pro tanto*, be considered state actors, private companies have no practical mechanism for obtaining judicial warrants. Absent a warrant, anyone convicted based on evidence collected by platforms would have a strong constitutional grounds for appeal.[6] Precisely to avoid such an outcome, the federal statute governing CSE and child sexual abuse material (CSAM) explicitly disclaims imposing any duty to "monitor any user . . . or the content of any communication" or "affirmatively search, screen, or scan" for CSE or CSAM.[7] This provision has been crucial to courts in finding that federal law does not transform tech services into state actors subject to the Fourth Amendment.[8]

---

[3] Fact Sheet: Client-Side Scanning, INTERNET SOCIETY (Mar. 24, 2020), https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/ ("By making the contents of messages no longer private between the sender and receiver, client-side scanning breaks the E2E trust model."); Erica Portnoy, *Why Adding Client-Side Scanning Breaks End-to-End Encryption*, ELECTRONIC FRONTIER FOUNDATION (Nov. 1, 2019), https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption ("[E]ven a well-intentioned effort to build such a system will break key promises of the messenger's encryption itself and open the door to broader abuses.").

[4] United States v. Stevenson, 727 F.3d 826, 829 (8th Cir. 2013) (quoting Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614-15 (1989)) ("[I]f a statute or regulation so strongly encourages a private party to conduct a search that the search is not 'primarily the result of private initiative,' then the Fourth Amendment applies.").

[5] United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016).

[6] *See, e.g.*, Letter re: Committee markup of S. 3538, The EARN IT Act, TechFreedom, at 2 (Feb. 8, 2022), https://techfreedom.org/wp-content/uploads/2022/02/TechFreedom-Letter-re-EARN-IT-Amendments-for-Markup-2.8.22.pdf.

[7] 18 U.S.C. § 2258A(f).

[8] "The only [statutory provision] that bears on scanning makes clear that an electronic communication service provider is not required to monitor any user or communication, and need not affirmatively seek facts or circumstances demonstrating a violation that would trigger the reporting obligation of § 2258A(a)." *United States v. Stevenson*, 727 F.3d at 830.

Under a constructive knowledge standard, platforms offering E2EE would face a quandary. E2EE means that the platform cannot view the contents of that user's communications. Thus, if someone alleges that a particular user is engaging in CSE over an encrypted service, the platform would have no way to assess the merits of specific complaints. Yet failing to act on a complaint would invite claims that the platform had been "negligent" or "reckless." Thus, such a platform would have no choice but to down material merely upon complaint—or to cease offering E2EE altogether. Research consistently shows that platforms exposed to such liability receive numerous false accusations and often follow the path of least resistance by simply removing lawful speech.[9] Such requests could easily be weaponized by a small group of ideologues to force the takedown of content or users they dislike. Yet because platforms could not distinguish valid from abusive complaints, they also could not identify serial abusers of the complaint process.

There is no need to open the door to such perverse consequences. An actual knowledge standard would not be toothless, but it should effectively distinguish between protecting the privacy of all users and truly nefarious conduct. In *Global-Tech Appliances, Inc. v. Seb S. A.* (2011), the Supreme Court recognized that willful blindness can supply the actual knowledge required by federal criminal laws and at least some federal civil laws.[10] "[A] willfully blind defendant," wrote the Court, "is one who takes deliberate actions to avoid confirming a high probability of wrongdoing and who can almost be said to have actually known the critical facts."[11] The Court concluded that "these requirements give willful blindness an appropriately limited scope that surpasses recklessness," where the defendant "merely knows of a substantial and unjustified risk of such wrongdoing," as well as negligence, where the defendant "should have known of a similar risk but, in fact, did not."[12] Willfully blind "ostriches," held one appeals court, "do not just fail to follow through on their suspicions of bad things. They are not merely careless birds. They bury their heads in the sand so that they will not see or hear bad things. They deliberately avoid acquiring unpleasant knowledge."[13] This includes a drug trafficker who "sought 'to insulate himself from the actual drug transaction so that he could deny knowledge of it,' which he did

---

[9] *See* Daphne Keller, Empirical Evidence of Over-Removal by Internet Companies Under Intermediary Liability Laws: An Updated List, THE CENTER FOR INTERNET AND SOCIETY BLOG (Feb. 8, 2021, 5:11 AM), https://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.

[10] Global-Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060, 2068-69 (2011).

[11] *Id.* at 2071.

[12] *Id.* at 2069-70.

[13] United States v. Giovannetti, 919 F.2d 1223, 1228 (7th Cir. 1990) (quoting United States v. Diaz,864 F.2d 544, 550 (7th Cir. 1988)).

sometimes by absenting himself from the [scene] of the actual delivery and sometimes by pretending to be fussing under the hood of his car.'"[14]

There *are* websites that do something equivalent in facilitating CSE. Imposing new civil liability against them might well be appropriate, and an actual knowledge standard would properly allow such claims. But when large platforms enjoyed by millions of users offer E2EE or decline to build client-side scanning into their apps, they are not "burying their heads" so that they can "deny knowledge of" criminal activity. Rather, they are offering valuable privacy and security features to all their users for overwhelmingly lawful purposes, as recommended by an overwhelming majority of security experts.[15] Just as "the Ninth Circuit does not set the willfulness bar so low that it requires active monitoring for infringement in the online platform context,"[16] nor would it require platforms to compromise their security offerings by abandoning E2EE or adopting client-side scanning.

In short, an actual knowledge standard would target AB-1394 properly against truly bad actors without causing legitimate platform operators to undermine the security features of the products enjoyed by millions of law-abiding users. For all these reasons, we applaud your retention of the actual knowledge standard.

We are still digesting other provisions of the bill, especially the notice-and-takedown system contemplated for CSAM by Section 3273.61(d). We note that your bill is preempted by existing federal law, 47 U.S.C. § 230, insofar as it imposes civil liability on platforms for content created by users. We urge you to allow time for experts to study all of the bill's provisions and testify about them before your committee before it advances. We would be happy to assist your committee in better understanding the implications of this legislation.

Sincerely,

Berin Szóka
President
TechFreedom

Ari Cohn
Free Speech Counsel
TechFreedom

---

[14] *Id.*

[15] Removing end-to-end encryption would do more harm than good, says poll of IT professionals, THE CHARTERED INSTITUTE FOR IT (Mar. 29, 2022), https://www.bcs.org/articles-opinion-and-research/removing-end-to-end-encryption-would-do-more-harm-than-good-says-poll-of-it-professionals/ ("78% of [security] industry professionals said they did not believe restricting the use of [end-to-end] encryption in messaging would protect users.").

[16] Greg Young Publishing, Inc. v. Zazzle, Inc., 2017 WL 5004719 (N.D. Cal. Oct. 27, 2017).