TECHFREEDOM
LAW FOR A DYNAMIC FUTURE

202.803.2867
Washington, DC
techfreedom.org

February 16, 2023

The Office of Gov. Spencer J. Cox
350 N. State Street, Suite 200
P.O. Box 142220
Salt Lake City, UT 84114-2220

Re: Utah Social Media Bills (S.B. 152 & H.B. 311)

Dear Governor Cox:

We write to express concern about the threat to the First Amendment rights of Utahns—indeed, of all Americans—posed by two pending bills. S.B. 152 and H.B. 311 aim to protect minors from online harms. The wellbeing of minors is a crucially important issue; it deserves more thoughtful consideration than is reflected in these bills, which have been rushed through the legislative process with a reckless urgency that gives short shrift to both minors and our fundamental liberties. The grave constitutional questions posed by these bills have been ignored.

In this rushed process, the text of these bills has changed, with some provisions being removed from one bill and inserted into the other. Significantly, at all times, one or both of bills have contained the same operative provision: social media platforms must verify the age of every user and require the consent of a parent or guardian for accountholders under the age of 18. All adults would have to upload a driver's license or other official identity document, effectively abolishing online anonymity. This age-verification mandate is even more sweeping than those enacted by Congress in 1996 and 1998—both of which were struck down by the courts.[1] These bills will violate the First Amendment rights of both minors and adults, to the detriment of the citizens of Utah. Indeed, because there is no way for a platform to know that a user is *not* a Utah resident prior to verification, sites will be required to age-verify *all* users regardless of their location—extending the unconstitutional effects of these bills far beyond Utah's borders.

---

[1] Communications Decency Act of 1996, Pub. L. No. 104-104, Tit. V, 110 Stat. 133 (1996), struck down in Reno v. American Civil Liberties Union, 521 U.S. 844 (1997); Child Online Protection Act (COPA), Pub. L. No. 105-277, div. C, Tit. XIV, 112 Stat. 2681-736 (1998), enjoined in ACLU v. Ashcroft (*Ashcroft I*), 322 F.3d 240, 243, 247 (3d Cir. 2003), aff'd, 542 U.S. 656 (2004). The Third Circuit reviewed and affirmed *Ashcroft I* in American Civil Liberties Union v. Ashcroft, 534 F.3d 181, 196 (3d Cir. 2008), cert denied, 555 U.S. 1137 (2009).

Requiring parental consent for using social media violates minors' First Amendment rights. The Supreme Court has recognized that government regulation of access to social media implicates the First Amendment: "to foreclose access to social media is to prevent the user from engaging in the legitimate exercise of First Amendment rights."[2] Yet that is precisely what these bills do: any Utahn under the age of 18 would be precluded by default from participating on a social media platform.

Minors possess significant First Amendment rights, "and only in relatively narrow and well-defined circumstances may the government bar public dissemination of protected materials to them."[3] These narrow circumstances concern primarily specific material deemed obscene as to minors.[4] No court has ever ratified the notion that minors may be excluded from an entire forum for expression regardless of its content. Indeed, there is nothing "narrow" at all about prohibiting minors from using social media wholesale.

Accordingly, broad regulations restricting youth expression have been struck down on First Amendment grounds. Holding unconstitutional a California law prohibiting the sale of violent video games to minors, Justice Antonin Scalia, writing for a 7-2 majority of the Supreme Court, declared that, "whatever the challenges of applying the Constitution to ever-advancing technology, the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary when a new and different medium for communication appears."[5]

Further, the Court expressly stated that the very type of regulation presented by S.B. 152 and H.B. 311 is unconstitutional. In dissent, Justice Clarence Thomas argued that parents traditionally control what their children hear and say. Justice Scalia responded in the majority opinion:

> But it does not follow that the state has the power to prevent children from hearing or saying anything *without their parents' prior consent*. The latter would mean, for example, that it could be made criminal to admit persons under 18 to a political rally without their parents' prior written consent—

---

[2] Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).

[3] Brown v Entertainment Merchants Ass'n, 564 U.S. 786, 794 (2011) (quoting Erznoznik v. Jacksonville, 422 U.S. 205, 212–13 (1975)).

[4] In *Brown*, California argued that its statute banning the sale of violent video games to minors was constitutional because it mimicked a New York statute regulating obscene-as-to-minors material. The Court rejected this argument, noting that obscenity is limited to sexual materials and that the power to protect children from harm "does not include a free-floating power to restrict the ideas to which children may be exposed." 564 U.S. at 793–95.

[5] Brown, 564 U.S. at 790 (internal quotation marks omitted) (citing Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 593 (1952)).

> even a political rally in support of laws against corporal punishment of children, or laws in favor of greater rights for minors. . . . Such laws do not enforce *parental* authority over children's speech and religion; they impose *governmental* authority, subject only to a parental veto. In the absence of any precedent for state control, uninvited by the parents, over a child's speech and religion . . . those laws must be unconstitutional.[6]

Allowing government to punish third parties for "conveying protected speech to children *just in case* their parents disapprove" is, Scalia insisted, incompatible with minors' First Amendment rights.[7] Utah lawmakers are right to be concerned about the wellbeing of young Utahns, but they cannot run roughshod over youths' civil liberties in the name of protecting them.

Mandating age verification is unconstitutional. Requiring social media platforms to verify the age of each user also violates the First Amendment rights of adults to access lawful, constitutionally protected content anonymously. Consider the Child Online Protection Act (COPA) of 1998. When defending the law's constitutionality, the government argued that websites could avoid liability for providing information deemed "harmful to minors" by requiring users to input credit card information, thus verifying that they were not minors. The Third Circuit held COPA likely unconstitutional because, notably, age verification requirements would "likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial."[8] In 2008, striking down COPA again and for the final time, the Third Circuit reiterated that age verification "would deter users from visiting implicated Web sites" and therefore "would chill protected speech."[9]

---

[6] Brown, 564 U.S. at 795 n.3(emphases in original).

[7] *Id.* at 802.

[8] American Civil Liberties Union v. Ashcroft, 322 F.3d 240, 259 (3d Cir. 2003).

[9] American Civil Liberties Union v. Ashcroft, 534 F.3d 181, 197 (3d Cir. 2008).

These bills would do even more First Amendment harm. COPA generally excluded online services that passively provided a forum for user-generated content,[10] effectively mandating age verification only for *accessing* content deemed "*harmful to minors*" that a website affirmatively selected for publication. In contrast, these bills cast a much wider net, mandating age verification for any use of social media. Where COPA required age verification only for "accessing" content, these bills would also require it for *communicating*. Anonymity allows users to discuss personal, sensitive, and controversial topics safely and candidly without fear of reprisal or harm. As the Supreme Court noted when striking down a ban on anonymous pamphleteering: "Anonymity is a shield from the tyranny of the majority . . . [and] thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society."[11]

Today, users can create pseudonymous social media accounts by providing nothing more than an email. They can use that account to comment publicly and message privately. But under these bills, users could no longer trust their pseudonyms to protect themselves, especially from government actors and powerful figures who would seek to stifle criticism. In striking down a Virginia analogue to COPA, the Fourth Circuit noted: "the stigma associated with [controversial content] may deter adults from [accessing it] if they cannot do so without the assurance of anonymity."[12] The effect of mandatory age verification on communication will be even more pronounced, and likewise "would unduly burden protected speech in violation of the First Amendment."[13]

---

[10] 47 U.S.C. § 231(b)(4). COPA applied to such platforms so long as they did not "select" or "alter" content in any way inconsistent with Section 230.

[11] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

[12] Psinet, Inc. v. Chapman, 362 F.3d 227, 236–37 (4th Cir. 2004). *See also* Southeast Booksellers Ass'n v. McMaster 371 F. Supp. 2d 773, 782 (D.S.C. 2005) (age verification creates a "First Amendment problem" because "age verification deters lawful users from accessing speech they are entitled to receive."); American Civil Liberties Union v. Johnson, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998) (mandatory age verification "violates the First and Fourteenth Amendments of the United States Constitution because it prevents people from communicating and accessing information anonymously.").

[13] Psinet, Inc. v. Chapman, 362 F.3d 227, 236–37 (4th Cir. 2004).

An age verification mandate will violate the First Amendment rights of *all* Americans. These bills will have effects far beyond Utah. S.B. 152 defines a "Utah resident" as a person who "resides" and "has their "primary residence" in Utah. H.B. 311 defines the term as a person "who currently resides in Utah." Other than demanding identification from all users, platforms have no way to know whether a user resides in Utah. Assumptions based on IP addresses would be unreliable, sweeping up visitors from out of state and missing users who use a VPN service or create an account while outside Utah—or even those who might live close to the state's border and whose phones connect to cell towers in a neighboring state. Nor will a person's physical presence at any given moment give platforms any indication as to whether their primary residence is in Utah. Utah cannot impose an unconstitutional age-verification mandate on its own citizens, let alone on the entire country.

Age verification poses serious privacy and security risks. Under the proposed legislative regime, platforms would be required to retain information collected for age verification purposes.[14] Indeed, platforms would be unable to prove compliance without retaining this information. The bills attempt to address privacy and security concerns about data retention by limiting its use and requiring such data to be stored "securely." But the danger of such widespread collection and retention of sensitive identity information cannot be addressed with an adverb. Platforms should collect less data about us, not more. They certainly should not be required to tie government identification records to each user's account. Such requirements are classic features of authoritarian governments like China and Iran.[15]

Identification documents are among the most sensitive categories of personal information, allowing not only identity theft but also locating specific users at home. Someone who gained access to such information could use it to find someone who had criticized them online and commit real-world violence against them. Despite years of growing concern about data collection and security, there is as yet no comprehensive federal privacy law. Social media companies are already rich targets for malicious actors; requiring them to collect and retain

---

[14] Presently, S.B. 152 directs the Division of Consumer Protection to "establish requirements for retaining" such information.

[15] AFP, *China Demands Internet Platforms Verify Users' True Identity*, SECURITY WEEK (Aug. 28, 2017), https://www.securityweek.com/china-demands-internet-platforms-verify-users-true-identity/; *Iran's Requirement for Internet Users to Verify Their Identity Would Further Erode Privacy Rights*, CENTER FOR HUMAN RIGHTS IN IRAN (Nov. 15, 2017), https://iranhumanrights.org/2017/11/irans-requirement-for-internet-users-to-verify-their-identity-would-further-erode-privacy-rights/.

even more sensitive data about users will increase the risks involved in data collection and exploitation, not reduce it.[16]

—

The goal of protecting minors from harm is laudable and important—and it need not be in tension with the First Amendment. But how to achieve that protection is a question our state and federal legislatures have struggled with for a quarter century *because* of its exceptional complexity. Likewise, state regulation of social media services cannot easily be limited to the boundaries of any one state. Utah lawmakers should leave these questions to Congress and instead focus on ensuring proper funding for state law enforcement and education aimed at increasing the digital literacy of both minors and their parents. But if Utah does find that it needs state-level legislation, it must ensure that its laws are carefully drafted and comport with constitutional limitations.

Sincerely,

Ari Cohn
Free Speech Counsel, TechFreedom

Brian Frye
Spears-Gilbert Professor of Law
University of Kentucky College of Law

Eric Goldman
Associate Dean of Research & Professor of Law
Co-Director, High Tech Law Institute
Santa Clara University School of Law

Dorit Reiss
Professor of Law
UC College of the Law, San Francisco

Berin Szóka
President, TechFreedom

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law
Director, Berkeley Center for Law & Technology
UC Berkeley School of Law

Rebecca Tushnet
Frank Stanton Professor of the First Amendment
Harvard Law School

[16] Jason Kelley et al., *Victory! ID.me to Drop Facial Recognition Requirement for Government Services*, ELECTRONIC FRONTIER FOUNDATION (Feb. 9, 2022), https://www.eff.org/deeplinks/2022/02/victory-irs-wont-require-facial-recognition-idme.