KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **Emma J. Llansó**
Policy Counsel, Center for Democracy & Technology

Before the Committee on Arts, Entertainment, Sports, Tourism, and Internet Media
California State Assembly

COMMENTS ON SB 501: THE SOCIAL NETWORKING PRIVACY ACT AND SB 568, REGARDING PRIVACY RIGHTS FOR CALIFORNIA MINORS IN THE DIGITAL WORLD

25 June 2013

Chairman Calderon and Members of the Committee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. While we appreciate the privacy and safety concerns that have motivated the legislature to consider the important issue of minors' online privacy, we have concerns about the potential for these bills to unduly burden minors' First Amendment rights by limiting their access to information while also limiting their access to platforms for their own speech.

As a note of introduction, I am an attorney and serve as Policy Counsel for CDT, one of the leading civil liberties organizations in the United States focused on the application of the First Amendment to speech on the Internet. CDT has offices in Washington, DC, San Francisco, and Brussels. In 1996, CDT led one of the consolidated legal challenges to the federal Communications Decency Act that resulted in the 1997 U.S. Supreme Court ruling that speech on the Internet warrants the highest level of First Amendment protection. Since then, CDT has brought and litigated constitutional challenges to a number of state laws that sought to regulate or restrict speech over the Internet. CDT is also an active advocate for comprehensive consumer privacy legislation, both in the United States and in Europe, and we regularly engage with both companies and the Federal Trade Commission in efforts to improve protections for users' privacy.

Our primary concern with SB 501 is its potential burden on minors' own First Amendment rights. By providing parents with a potential veto over minors' social networking posts, the bill would restrict minors' exercise of their right to free expression. And, because of the challenge of verifying identity online, the procedure imagined in SB 501 would be vulnerable to abuse, potentially leading to fraudulent takedown demands that site operators will have no incentive to challenge. Further, the right-to-removal proposed in SB 501 is not narrowly scoped and would allow one user to demand the removal of content about him that is posted by another user, even if that content only included true, factual information. This is a limitation on First Amendment rights that is unlikely to withstand scrutiny.

Similarly, we are concerned that SB 568 would also burden minors' First Amendment rights. While the right-to-remove proposal in this bill is more narrowly drawn and avoids several of the issues posed by the right-to-remove described in SB 501, the bill's focus on websites or online services "directed to minors" creates significant challenges because of the vagueness of this term. Sites that have an audience "primarily comprised of minors" could include many general-audience sites or sites that aim to appeal to young adults. When faced with obligations to treat minors' content differently or to restrict certain marketing or advertising material to minors, many operators unsure of their status under this bill will opt to bar minors from their sites and services altogether. This will restrict minors' access to constitutionally protected material, limit their opportunities for speech, and discourage development of content designed for younger audiences. This will also encourage minors to lie about their age to gain access to popular sites and services, leaving operators of these sites unable to tailor their services to better protect minors' privacy and online safety. This is the unfortunate but likely consequence of both SB 501 and SB 568, and thus CDT urges Committee Members to reject both bills.

SB 501 Burdens the First Amendment Rights of Minors and Adult Users of Social Networking Websites

Rights of Minors

The Supreme Court has consistently recognized that minors, particularly older minors, have independent First Amendment rights to speak, associate, and access information. As the Supreme Court has stated, "constitutional rights do not mature and come into being magically only when one attains the state-defined age of majority."[1] By providing for a potential parental veto to minors' speech, SB 501 would unconstitutionally limit minors' exercise of their own right to freedom of expression. The information covered by the bill includes address, phone number, and mother's maiden name, all information minors may have a First Amendment interest in disclosing. For example, SB 501 would give a parent a blanket veto right over a 17-year-old's decision to provide her cell phone number on a Facebook page she has created to coordinate a political rally. This would be a clear violation of that young woman's right to political speech.

Parental takedown demands could have adverse effects on youth speech and participation in a wide variety of online forums, including independent outreach and support sites for LGBTQ youth such as the Trevor Project, or the social-network pages of groups such as the Rape Abuse & Incest National Network (RAINN) and the National Suicide Prevention Lifeline. While clearly not the intent of SB 501, the bill's creation of a parental veto right would leave vulnerable minors without control over their own communications and would potentially empower parents to suppress minors' statements about sexual identity, reproductive choice, religion, political affiliation, and similarly intimate and sensitive matters.

Rights of Other Speakers

SB 501 would also violate the First Amendment rights of other users online. The bill would give a user a right to order the takedown of any "personal identifying information" (as defined in the bill) pertaining to him, regardless of whether he was the initial poster of the information. Thus, potentially any user would have the ability to order the takedown of any other user's content that happens to include his or her personal information. This is an extremely broad deletion right, which unduly interferes with other users' First Amendment rights. For example, this bill would

[1] Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 74 (1976) (concerning minors' right to abortion).

allow a business owner to demand the takedown of a post organizing a letter-writing campaign to him about his unfair labor practices. Under SB 501, a user could compel deletion of truthful information about himself even if the poster had lawfully obtained it, including information such as address, telephone number, and mother's maiden name. These types of information are likely to be matters of public record in any case, and bring SB 501 into direct conflict with Supreme Court precedent that "state action to punish the publication of truthful information seldom can satisfy constitutional standards."[2] These are also types of information that are likely to be shared by multiple people in a family or at a particular residence, giving rise to a broad ability for individuals to police the social network posts of those with whom they cohabitate or share family ties. In some cases, SB 501 would give siblings the right to demand deletion of each other's entire profiles because they share as a surname their mother's "maiden name".

SB 501 Places Impractical Burdens on Social Networking Operators and Would Likely Lead Operators to Bar Minors from their Sites and Services

An operator attempting to comply with SB 501 will face the significant challenge of verifying the identity of the user requesting that information be removed. Because the bill allows users to demand takedown of other users' content, and parents (who may not even be users of the site) to demand takedown of minors' content, operators will need to conduct some kind of identity-verification for every request they receive. To do this, operators will have to collect significant amounts of sensitive information from users, in the name of protecting their privacy. While some of the largest social networks may have the infrastructure and staffing to attempt to institute this kind of identify verification system, many smaller operators and start-up social networks will simply be unable to do so due to lack of resources.

The structure proposed in the bill requires users making takedown demands to "include sufficient information to verify [their] identity" and allows operators to require users to assert that the information they are providing is true and accurate. This structure is intended to help obviate the burden of identity verification for operators. But this creates an incentive structure where operators rely, on the one hand, on user assurances that the takedown request is valid, and face, on the other hand, upwards of $10,000 in fines for failure to comply. The vast majority of operators will almost certainly take down any information requested rather than face significant financial liability. This type of system is obviously vulnerable to abuse.

In comparison to existing law, while the Digital Millennium Copyright Act does outline a notice-and-takedown system for online operators seeking safe harbor from liability,[3] the DMCA's structure is quite different from that proposed in SB 501. The DMCA does not *require* operators to take down content; rather, it provides protection from potential copyright liability if operators voluntarily comply with the notice-and-takedown system described in the statute. This system, among other safeguards, provides the user who has originally posted the content with the opportunity to challenge the takedown or sue for misuse of the takedown process.[4] Operators who decline to comply with DMCA takedown demands have not necessarily violated any law; they may (or may not) be sued for copyright infringement, and they may (or may not) be found

[2] Smith v. Daily Mail Publishing Co., 443 U. S. 97, 102 (1979).

[3] 17 U.S.C. § 512.

[4] Of course, even the DMCA notice-and-takedown procedure is vulnerable to abuse. *See, e.g.*, CDT, Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech, September 2010, *available at* https://www.cdt.org/files/pdfs/copyright_takedowns.pdf.

liable. If an operator believes a DMCA notice is spurious or the risk of actually being held liable for infringement is otherwise low, the operator is under no obligation to take down the content. This is a sharp contrast to SB 501's promise that operators who fail to comply with takedown requests face up to $10,000 in fines.

The issue of identity verification is compounded for information requests pertaining to minors, where SB 501 allows for either the person to whom the data pertains *or* her parent to file the demand. As difficult as it is to verify a given user's identity, verifying that one individual is the lawful parent of guardian of another is much more challenging. There is a real risk that, rather than attempt such complicated identity verification, website operators will simply prohibit users from creating accounts if they are younger than 18. As we have seen with the federal Children's Online Privacy Protection Act,[5] which requires operators of sites directed to children to obtain verified parental consent before collecting children's personal information, operators presented with potential regulatory burdens for dealing with children's data often seek to bar children from their sites entirely. SB 501 could yield the same result for all minors under age 18, which would create an environment in which minors are barred from honestly participating in social networking web sites. As discussed below, this would discourage operators from tailoring content and privacy controls to younger users, and would likely diminish the opportunities for age-appropriate participation in social networking sites for Internet users under the age of 18.

For these reasons, CDT urges Members of the Committee to reject SB 501.

SB 568 Is Unconstitutionally Vague, Will Limit Minors' Access to Constitutionally Protected Material, and Violates the Commerce Clause of the Constitution

CDT has similar concerns that SB 568 would burden minors' First Amendment rights, in part by creating significant disincentives for operators to provide content and services geared toward minors. Further, the bill's content restrictions for advertising and marketing, which are based on state standards of what is appropriate for minors, likely violate the Commerce Clause in much the same way that previous state attempts to regulate minors' access to indecent or 'harmful to minors' content have been found to.

Section 22580 – Marketing and Advertising to Minors

There are several aspects of SB 568's prohibition on marketing and advertising certain products and services on sites "directed to minors" that are vague or unclear. The resulting lack of clarity for operators will likely lead them to bar minors from their sites in order to establish that they are not sites "directed to minors". Sites that do attempt to comply will likely need to prohibit the covered advertising and marketing material to all of their users, implicating the First Amendment rights of minors in other states and of adult users. Laws that result in restricting adults' access to constitutionally protected material online are unlikely to withstand strict scrutiny.

"Directed to minors" is a vague standard that leaves operators with no certainty of their obligations under the law.

SB 568 defines a site or service (or portion thereof) directed to minors as one "that is created for the purpose of reaching an audience that is primarily comprised of minors." The notion of a site or service "directed to minors" mirrors the federal COPPA law's application to operators of sites

[5] 16 C.F.R. 312. COPPA also requires operators to obtain parental consent when they have actual knowledge that a specific user is a child. "Child" is defined as a person under age 13. 16 C.F.R. 213.2.

or services "directed to children", but there are several key distinctions. First, COPPA applies to the personal information of children under age 13, not to all minors under age 18. The FTC, in defining "directed to children", has created a look-and-feel test that considers a number of quantitative and qualitative factors.[6] Further, operators can refer to more than 10 years of enforcement actions under COPPA for further guidance on how the FTC applies its definition.[7] The COPPA standard of "directed to children" works, to the extent that it does, because it is relatively easy to identify content intended for young children, as distinguished from content intended for older minors, young adults, or a general audience.

It is much more difficult to draw a bright line between content aimed at 16- and 17-year-olds and content that is intended for young adults and older audiences, and there is no comparable federal guidance or precedent describing sites or services "directed to minors". Thus, many operators of services that are popular with teenaged Internet users as well as adults, from social networking platforms such as Tumblr and Instagram, to news-aggregating sites such as Reddit and BuzzFeed, to popular apps such as Angry Birds and Pandora Radio, will be left uncertain as to whether their sites fall under SB 568's definition of "directed to minors".

Further, because the bill would apply to *portions* of sites that are directed to minors, many general-audience sites would find that ads or other marketing that is constitutionally protected on parts of its site would violate California law on other parts. For example, Hulu.com is a popular general-audience site that allows users to watch streaming video of television shows and movies, the majority of which have previously aired on broadcast, cable, or in theaters. Some of the content Hulu streams could likely be considered "directed to minors" under SB 568; in order to determine which portions of its site fall under the scope of this bill, Hulu would need to evaluate each of the programs it hosts, which are typically created and produced by entities other than Hulu, to verify which were "created for the purpose of reaching an audience that is primarily comprised of minors."[8] It is not clear, under the bill, whether portions of its site that happen to attract a significant number of minors, even if the content was not developed with minors in mind, would still be subject to SB 568's prohibitions.

Assuming Hulu can confidently identify which of the programs it streams would be considered "directed to minors" by the state of California, it would then be legally prohibited from showing certain commercials during its online streaming that would be completely legal for a broadcaster or cable operator to air alongside their transmission of the same content. And, while the term "marketing" is not defined in the statute, a plain-meaning understanding of the term would likely encompass such advertising efforts as product placement deals within television shows and movies. Thus, online content providers such as Hulu would be legally prohibited from displaying precisely the same material that receives full First Amendment protection in other media – a

[6] These include the subject matter and language used on the site, age of models on the site, use of cartoon characters and child-oriented activities, as well as reliable empirical data about audience composition, and information about intended audience for the site. 16 C.F.R. 312.2.

[7] The new COPPA Rule, which goes into effect July 1st, adds several additional elements to the look-and-feel test, including musical content, the presence of child celebrities, and celebrities who appeal to children.

[8] While this will be a subjective evaluation that could leave the operator with some significant uncertainty, Hulu, at least, has the advantage of entering into negotiated contracts with content producers material streams on its site. A user-generated content platform such as YouTube or Vimeo has no such relationship with its millions of user/content-providers. Such sites do not screen, filter, or evaluate material prior to it being made publicly available on their sites, and so would be in an even worse position to determine which portions of their sites have become "directed to minors" through the actions of users/third-party content-uploaders.

double-standard the Supreme Court unequivocally rejected in *Reno v. ACLU*,[9] finding that online speech receives the highest level of First Amendment protection.

Except in narrow circumstances, minors have a right to receive information that is protected under the First Amendment.

Preserving the right to fully exercise the rights of speech, press, and political freedom serves a vital role in minors' intellectual development. "[M]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them."[10] Permissible content-based restrictions on minors' access to information typically relate to a narrow category of sexual content; otherwise, minors have a right to receive information just as adults do.[11] The marketing or advertising described in SB 568 is speech that is protected by the First Amendment; in evaluating SB 568, the Court would need to decide that the state has a compelling interest in restricting minors' access to the newly enumerated 21 categories of speech in the bill.[12] While regulations of advertising or "speech proposing a transaction" receive a lower level of scrutiny from the courts,[13] SB 568's under-inclusivity (not covering other media transmission of identical content) and over-inclusivity (prohibiting such communications even to minors whose parents would consent, e.g. marketing about handgun safety certificates) will make it difficult for the state to demonstrate that the bill is tailored to its interest in keeping from minors advertising that may be inappropriate for them.[14]

Further, minors in other states may have a full right to purchase some of the items that are prohibited to minors in California, including tanning services, laser pointers, and spray paint. Because geo-targeting of content online can be imprecise and also adds additional costs to the serving of that content, sites seeking to avoid liability under the California law will likely choose to simply bar these types of advertisements to all minors, perhaps even to all users. Thus, a minor in a state who has full right to receive information, including marketing, about spray paint or laser pointers, or an 18-year-old user of a site "targeted to minors", will be prevented from accessing information which she has a constitutional right to receive.

---

[9] 521 U.S. 844 (1997).

[10] Erznoznik v. Jacksonville, 422 U.S. 205, 212–213 (1975) (citation omitted).

[11] Board of Education v. Pico, 457 U.S. 853, 867-868 (1982) (plurality opinion). *See also* In re Gault, 387 U.S. 1, 13 (1967) ("[W]hatever may be their precise impact, neither the Fourteenth Amendment nor the Bill of Rights is for adults alone.")

[12] The Supreme Court recently declined to expand the categories of content that the state may permissibly bar minors from accessing to include violent content, in its opinion striking down the California state law restricting minors' access to violent video games. *See* Brown v EMA, 564 U.S. 08-1448 (2011) ("[California] wishes to create a wholly new category of content-based regulation that is permissible only for speech directed at children. That is unprecedented and mistaken."). *Id.* at 6.

[13] Central Hudson Gas & Electric Corp. v. Public Service Commission, 447 U.S. 557 (1980).

[14] *See* Brown v. EMA, (holding "As a means of protecting children from portrayals of violence, the legislation is seriously underinclusive, not only because it excludes portrayals other than video games, but also because it permits a parental or avuncular veto. And as a means of assisting concerned parents it is seriously overinclusive because it abridges the First Amendment rights of young people whose parents (and aunts and uncles) think violent video games are a harmless pastime. And the overbreadth in achieving one goal is not cured by the underbreadth in achieving the other. Legislation such as this, which is neither fish nor fowl, cannot survive strict scrutiny.")

Compliance with SB 568 may paradoxically result in operators collecting more information from all users.

Operators who make a good-faith effort to restrict advertising of prohibited material to California minors will either need to ban all such advertising from their site or service,[15] or collect information about each of its users in order to distinguish minors from adults and California residents from users elsewhere in the country and world. This would require operators to collect and maintain richer profiles about the users of their sites (many sites do not ask age or location). Further, users may be deterred from accessing online content because of operator demands for them to disclose personal information. This would interfere with users' right to access information anonymously and could chill their access to information online, particularly for users accessing sensitive, personal, or controversial information.[16]

State-level Regulations of Online Content Violate the Commerce Clause

Courts across the country have routinely struck down state laws that seek to regulate online content, labeling them unconstitutional burdens on interstate commerce.[17] As a leading case applying the Commerce Clause to the Internet explained:

> The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. *The Internet represents one of those areas*; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations.[18]

For example, while California and Vermont prohibit indoor tanning services to all minors, Oregon and Connecticut prohibit tanning only to minors under 16, and Washington and Pennsylvania have no statewide restrictions on tanning.[19] Similarly, while several states and cities have restricted the sale of aerosol paint to minors,[20] many other states have no such restriction. Operators of websites, apps, and advertising networks will face a patchwork of inconsistent state laws if additional states follow California's lead in prohibiting certain categories of advertisements to minors online.

As discussed above, if operators attempt to comply with these laws without treating them as an outright ban on such advertisements, they will need to collect significant amounts of personal information from all users and will have strong incentive to maintain rich profiles on users once

---

[15] Because of the expertise and expense required to develop a system that allows the kind of fine-grained targeting of advertisements that SB 568 would require, it is highly likely that operators of start-up and smaller sites, services, and apps would be compelled to ban these kinds of advertisements altogether.

[16] ACLU v. Ashcroft, 322 F.3d 240, 259 (3d Cir. 2003), aff'd, 542 U.S. 656 (2004).

[17] *See, e.g.*, PSINet v. Chapman, 362 F.3d 227 (4th Cir. 2004); American Booksellers Ass'n v. Dean, 342 F.3d 96 (2d Cir. 2003); ACLU v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999); American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997).

[18] American Library Association v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y. 1997) (emphasis added).

[19] National Conference of State Legislatures, Indoor Tanning Restrictions for Minors: A State-by-State Comparison, http://www.ncsl.org/issues-research/health/indoor-tanning-restrictions.aspx.

[20] National Conference of State Legislatures, Youth Use of Inhalants and Aerosols: State Laws 2010, http://www.ncsl.org/issues-research/human-services/youth-use-of-inhalants-and-aerosols-state-laws-201.aspx.

the user's age and state of residence has been established. Though not the intended outcome of the bill, this is SB 568's likely result.

Section 22581 – Deletion of Minors' Content and Information

The provision guaranteeing minors' ability to remove their own content and information from websites and online services "directed to minors" raises similar vagueness issues regarding the scope of sites and services covered. SB 568's removal provision is much more narrowly scoped than that in SB 501, which obviates many of the constitutional concerns. But, as discussed above, the vagueness of the "directed to minors" standard, combined with the provision's coverage only of minors' content and information, means that many operators will likely comply with the law by prohibiting minors from registering for their sites.

Of course, a prohibition in a site's terms of service that minors not use the site does not mean that minors will comply. As we have seen with sites that prohibit users under age 13 due to concerns over compliance with the federal COPPA law, children seeking to use sites such as Facebook sometimes lie about their age in order to circumvent the platform's age screen.[21] This is often done with parents' knowledge and assistance, as many parents confronted with an age-based prohibition on a website believe it to be related to some kind of content-appropriateness rating, not linked to stronger privacy protections for children.[22] The same would likely occur with an under-18 prohibition on popular sites.

One of the unfortunate consequences of minors lying about their age is that it circumvents efforts by operators to tailor privacy and content controls for different age groups. In a regime where minors' data comes with significant regulatory obligations while adults' data does not, operators have the incentive to maintain the fiction that age-based prohibitions actually keep younger users off of their sites. The state cannot compel operators to identify and safeguard minors' data without requiring operators to conduct invasive identity verification for all of their users, something the Supreme Court has rejected as an unconstitutional burden on the right to access information anonymously.[23]

Conclusion

CDT appreciates the concerns that motivate these two bills, and we applaud the California legislature's continued focus on issues of online privacy. Legislation singling out minors, however, is vulnerable to constitutional challenge and will create perverse incentives for operators to avoid creating content and privacy controls tailored to users under 18. Comprehensive consumer privacy laws that apply to all users, regardless of age, would provide a strong foundation for providing young people with a safe and positive online experience and for protecting the privacy of the young and old alike.

---

[21] danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey, Why parents help their children lie to Facebook about age: Unintended Consequences of the Children's Online Privacy Protection Act, November 2011, *available at* http://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075.

[22] *Id.*

[23] See, e.g., American Civil Liberties Union v. Gonzales, 478 F.Supp.2d 775 (E.D. Pa. 2007) (striking down the Child Online Protection Act), *aff'd sub nom.* American Civil Liberties Union v. Mukasey, 534 F.3d 181 (3d Cir. 2008), *cert. denied,* 129 S. Ct. 1032 (Jan. 21, 2009).