The Electronic Frontier Foundation

MEMORANDUM

To: Lee Tien
From: XXXX
Re: Preemptive impact of the proposed Kerry/McCain Commercial Privacy Bill of Rights
Date: May 4, 2011

I. Summary

This memo addresses the preemptive effect of Senators Kerry and McCain's Commercial Privacy Bill of Rights[1] on state privacy law and enforcement efforts. I find the following:

- Section 405(a), the preemption clause, adopts a construction that many judicial authorities have already interpreted to be "expansive" in its preemptive effect;
- The key statutory terms defining the substantive scope of preemption are sufficiently general to reach a very wide range of activity (collection, use, disclosure of information) undertaken by persons, firms, and non-profits, among others;
- A significant body of carefully tailored, industry- and technology-specific state privacy laws, as well as some states' unfair competition and "Little FTC" Acts, are likely to be preempted by § 405(a);
- Victims of privacy harms will have to rely on a single federal standard (and to-be-determined FTC rules), enforced only by the FTC and state attorneys general, and will lose important private rights of action and many alternative forms of relief.

In short, the Commercial Privacy Bill of Rights effects a drastic federal overhaul of privacy protections, preempting carefully-crafted state privacy laws. The following sections of this memo describe: (1) preemption doctrine and case law as it applies to the construction of § 405(a), (2) the substantive scope of the key terms contained in § 405(a), and (3) its likely preemptive effect on four specific laws in California. The Appendix contains a table listing a number of other California laws likely to be preempted.

II. Analysis

A. Section 405(a) is likely to be interpreted as broadly preemptive

Section 405(a), the preemption clause of the proposed Act, holds:

> The provisions of this Act shall supersede any provisions of the law of any state relating to those entities covered by the regulations issued pursuant to this Act, to the extent that such provisions relate to the collection, use, or disclosure of—
>
> (1) covered information addressed in this Act; or
> (2) personally identifiable information or personal identification information addressed in provisions of the law of a State.

[1] Commercial Privacy Bill of Rights, S. __ , 112th Cong. (2011), *available at* http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Text.pdf.

454 Shotwell Street, San Francisco, CA 94110 USA
+1 415 436 9333 (v) +1 415 436 9993 (f) www.eff.org

§ 405(a). This basic construction is likely to be interpreted as expansively preemptive. Courts that have considered identical statutory constructions in the context of similar legislative schemes, where the federal objective was to create a single legal standard, have found state laws touching the same subject to be widely preempted. The proposed Act's narrow carve-outs from preemption, and relatively limited enforcement mechanisms (compared to state law), are likely to reinforce further the judgment that many state laws could interfere with federal objectives and must be preempted. Unlike some other federal privacy-protecting laws, such as HIPAA, the proposed Act does not preserve state laws that provide more stringent protections that are fundamentally consistent with federal objectives. *Cf.* 45 C.F.R. § 16.203(b) (Health and Human Services regulation under HIPAA preserving any "provision of State law [that] relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted" under federal law).

The statutory language of an express preemption clause provides the best evidence of legislative intent as to preemption. *CSX Transp., Inc. v. Easterwood*, 507 U.S. 658, 664 (1993). However, even with an express preemption provision, "the question of the substance and the scope of Congress' displacement of state law still remains." *Island Park, LLC v. CSX Transp.*, 559 F.3d 114, 101 (2d Cir. 2009), *citing Altria Group, Inc. v. Good*, 129 S.Ct. 538, 543 (2008). To answer this latter question, the courts ultimately query the objectives of the relevant federal law to determine "the scope of state law that Congress understood would survive." *New York State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 656 (1995). The relevant inquiry in this regard is not whether the state law may be characterized as "consistent" or "inconsistent" with federal regulation, nor whether the state law's impact on federal regulation is said to be "direct" or "indirect." *Rowe v. N.H. Motor Transp. Ass'n*, 552 U.S. 364, 370-71 (2008). Rather, any state law that actually interferes with federal objectives—in the neutral sense that it is has a "'significant impact' related to" Congress' purpose—is preempted. *Id.*

Any future Committee reports and floor debates would of course help to clarify further the substance and scope of the preemption clause. However, the plain language of § 405(a) and the findings of the bill strongly suggest that the proposed Act is intended to be broadly preemptive of state law.[2] The bill finds, for example, that "the laws of the Federal Government and State and local governments provided inadequate privacy protection for individuals engaging in and interacting with persons engaged in interstate commerce." § 2(6). Thus, although online behavioral advertising may have been a motivating factor behind the bill's introduction, the title ("Commercial Privacy Bill of Rights") and the findings of the law make it clear that the proposed Act is intended to sweep very broadly, well beyond the Internet. *See, e.g.,* § 2(2) ("Trust in the treatment of personally identifiable information collected *on and off the Internet* is essential for business to succeed." (emphasis added)). *See also* §§ 2(9), 2(15).

Consistent with these findings, § 405(a) of the bill explicitly preempts "any provisions of the law of any State relating to [the] covered entities," to the extent that those provisions "relate to" the

[2] Notably, § 405(a) does not make any reference to state constitutions, unlike some express preemption clauses contained in federal law. *Cf.* Federal Deposit Insurance Act, 12 U.S.C. 1831d(a) (2006) (preempting "any State constitution or statute"). Given that the plain language of the preemption clause is the clearest indicia of intent and that the courts start with the presumption that state law is valid, *Pharmaceutical Res. & Mfrs. Of America v. Walsh*, 538 U.S. 644, 661-62 (2003), particularly in fields traditionally occupied by the states, *California v. ARC America Corp.*, 490 U.S. 93, 101 (1989), it is likely that the Act would not be interpreted to preempt state constitutional rights to privacy. *See* CAL. CONST. ART. I, § 1.

collection, use, or disclosure of "covered information," "personally identifiable information" (PII) or "personal identification information." § 405(a). The courts are very likely to interpret this general construction to have expansive preemptive effect—and, in fact, they have already done so in numerous cases construing identical or highly similar preemption clauses. These cases are likely to control any judicial analysis § 405(a). *Rowe*, 552 U.S. at 370 ("[W]hen judicial interpretations have settled the meaning of an existing statutory provision, repetition of the same language in a new statute indicates, as a general matter, the intent to incorporate its judicial interpretations as well." (citations omitted)).

For instance, the Southern District of New York recently offered the first judicial construction of identical preemption language appearing in the federal Homeowners Protection Act (HPA). *Compare* § 405(a) ("The provisions of this Act shall supersede any provisions of the law of any State *relating to* [the covered] entities … to the extent that such provisions *relate to* the collection, use, or disclosure of," *inter alia* "information addressed in this Act" (emphasis added)), *and Fellows v. CitiMortgage, Inc.*, 710 F. Supp. 2d 385, 399 (S.D.N.Y. 2010) (HPA "shall supersede any provisions of the law of any State *relating to*," *inter alia*, "any *disclosure* of information addressed by [the HPA]" (emphasis in original)). Ultimately, the court concluded that the HPA broadly preempted application of New York's "Little FTC Act," the Deceptive Trade Practices Act (DTPA), N.Y. Gen. Bus. L. § 349(a) (McKinney 2004). The only significant structural difference between the two statutory provisions is the proposed Act's repeated use of the key phrase, "relating to," "relate to."

That phrase has not been understood as providing much limitation by the courts. Citing Supreme Court constructions of extremely similar preemptive language appearing in ERISA and the Airline Deregulation Act (ADA), the Southern District held that "relating to" is "clearly expansive" and may be defined as, "having a connection with, or reference to," the purpose of federal regulation. *Id.* (citing Supreme Court constructions of "relating to" under ERISA and ADA). *See also Mizrahi v. Gonzales*, 492 F.3d 156, 159 (2d Cir. 2007) ("Congress's use of the phrase 'relating to' in federal legislation generally signals its expansive intent."). The district court found further support for its expansive reading of the preemption clause in the statute's limited carve-out for protected state laws, as well as its legislative history. *Fellows*, 710 F. Supp. 2d at 401. *Compare with* § 405(b)(2) (proposed Act excepting certain limited state laws from preemption). The *Fellows* court also noted that Congress' apparent intent was to provide a uniform national standard for mortgage insurance cancellation and disclosure requirements. *Cf.* § 2 (existing state and federal laws provide inadequate protections and inconsistent standards). *Id.*

In *Fellows*, notwithstanding the Supreme Court's general disfavor toward preemption and its specific finding that both the ERISA and ADA preemption clauses left some "room for state actions 'too tenuous, remote, or peripheral to have pre-emptive effect," the Southern District ultimately found the DPTA to be preempted. *Id.* at 403 (noting that ERISA and the ADA have also been found to preempt state unfair competition laws). In particular, the court found that permitting the plaintiff mortgagor to proceed with his DPTA claim against CitiMortgage, for its failure to disclose his insurance cancellation rights under the mortgage agreement, would impose cancellation and disclosure requirements on the mortgagee not countenanced in the federal HPA. *Fellows*, 710 F. Supp. 2d at 402. The plaintiff's state law claim therefore had "a connection with" the disclosure requirements and cancellation provisions under the HPA that was "direct and substantial," not "tenuous, remote, or peripheral." *Id.* Permitting the suit to go forward, the court found, would be

"fundamentally at odds with the goal of uniformity that Congress sought to implement," and "interfere with the civil enforcement mechanisms provided by the HPA." *Id., citing Ingersoll-Rand Co. v. McClendon*, 498 U.S. 133, 142 (1990).

Section 405(a) is constructed identically to that of the HPA, and *Fellows* will likely be read as highly persuasive authority, given that its analysis, in turn, rests on considerable, recent Supreme Court authority directed to the scope of very similar statutory language. Many of the elements present in that case would also factor an analysis of § 405(a)'s preemptive effect on state laws. For example, the findings contained in § 2 of the proposed Act suggest that the federal objective underlying the legislation is very broad: to set a single federal standard for the online and offline collection, use, disclosure, and transfer of "covered information," with few exceptions. Any state law that has a "'significant impact' related to" this purpose will be preempted. Likewise, the limited carve-outs contained in § 405(b)(2) imply broad preemption. Finally, to the extent that state laws provide enforcement mechanisms that depart from those available in the proposed Act, courts are likely to regard these disparities as interference with federal regulation, and a further justification for preemption.

For the reasons discussed above, the broad phrasing of § 405(a), and the backdrop of expansive judicial constructions of virtually identical statutory language, set the stage for the proposed Act to preempt a very significant, accumulated body of industry- and technology-specific consumer protection, privacy, and unfair competition state laws. The next section details the substance to which state laws must "relate" to be preempted under § 405(a), the range of specific state laws that arguably fall within its ambit, and the enforcement mechanisms that will be unavailable as a result.

B. Substantive scope of § 405(a) and preempted state laws

1. Substantive scope of § 405(a) preemption

The precise substantive scope of the preemption clause in the Kerry/McCain bill is tied to the definition of several key terms—general terms, none of which, notably, limit application of the law to the Internet. Rather, § 405(a) specifies that preemption shall apply to any state law provision "related to" the "covered entities" defined by the proposed Act, "to the extent that such provisions relate to the collection, use, or disclosure of (1) covered information addressed in this Act; or (2) personally identifiable information or personal identification information addressed in provisions of the law of a State." § 405(a). The preemption clause does contain carve-outs for state laws concerning the collection, use, or disclosure of health or financial information, required notifications pursuant to a data breach, and state laws that "relate to acts of fraud." § 405(b)(2). Nonetheless, the substantive scope of the preemption clause ultimately implicates a very wide range of activities by firms, non-profits, and individuals that are currently regulated by state law.

a. Covered entities

Under § 3(3) of the proposed Act, "covered entity" refers to a broader class of entities than are normally subject to FTC jurisdiction. Specifically, the term denotes any person who "collects, uses, transfers, or stores covered information concerning more than 5,000 individuals during any consecutive 12-month period," and: (a) is amenable to FTC jurisdiction under § 5 of the FTC Act, or (b) is a common carrier under the federal communications laws, or (c) a non-profit, as defined by the tax laws. § 401. Thus, to be "covered," an entity must first meet the (relatively low) 5,000-

person collection threshold. Many ordinary "customer relationship management" databases maintained by small businesses such as retailers will qualify, as will most membership lists maintained by non-profits like local, listener-supported radio stations.

Once this threshold requirement is met, there are three basic ways an entity might then fall within the ambit of the Act. First, any entity that is a subject to FTC jurisdiction under § 5 of the FTC Act will fall under the proposed Act's provisions. *See* § 401(2)(A), *citing* 15 U.S.C. § 45(a)(2) (2006) (reaching persons, partnerships, and corporations, except certain financial institutions and other limited parties). Of course, entities that do qualify under § 401(2)(A) will only be subject to regulation under the proposed Act to the extent permitted by the FTC Act and the Commerce Clause. An interesting and open question is whether the commercial activities of unincorporated citizens groups, such as informal political groups, which may not fall under the FTC Act's coverage of "persons, partnerships, or corporations," are nonetheless covered by the bill.

Second, and alternatively, an entity may fall under the Act if it is defined as a common carrier subject to the Communications Act of 1934. *See* § 401(2)(B), *citing* 47 U.S.C. § 151 (2006), *et seq*. Finally, a 501(c)(3) non-profit that collects information on 5,000 individuals will fall under the proposed Act. *See* § 401(2)(C) (citing § 501(c)(3) of the IRS code). Notably, common carriers, and non-profits are *not* normally subject to FTC jurisdiction under the FTC Act, but will be regulated by the agency under the Commercial Privacy Bill of Rights. This expanded jurisdiction is contemplated, in the language of the proposed Act, "notwithstanding the definition of 'Acts to regulate commerce'" and the express exemptions from jurisdiction these organizations enjoy under the FTC Act. *See* §§ 401(2)(B)-401(2)(C).

Particularly with respect to non-profits, the FTC's expanded authority raises interesting Commerce Clause questions that will need to be examined by the bill's supporters. Non-profits are not ordinarily subject to FTC jurisdiction. *See, e.g., Cal. Dental Assoc. v. FTC*, 526 U.S. 756 (1999) (no jurisdiction unless non-profit provides "substantial economic benefit" to its members). Since jurisdiction over non-profits under the Commercial Privacy Bill of Rights is not tied to the FTC Act, one might well ask: how can the Act establish proper jurisdiction under the Commerce Clause over the intrastate, non-economic activities of non-profits? Consider, for example, the private, internal maintenance and use of a members' mailing list by a local, non-profit political organization that does not address economic or commercial matters: does such activity have any cognizable impact on interstate commerce? At least in its current form, the proposed Act does not contain a jurisdiction finding stating that the Commerce Clause provides the constitutional basis for its validity, and (unlike the FTC Act) there are no other provisions in the bill suggesting that it is intended to be so limited. Interestingly, this is only an issue for non-profits and common carriers. Individuals, by contrast, are generally subject to FTC jurisdiction so long as their bad acts are commercial, in the necessary sense. To the extent that individuals or others, are not engaged in commercial activity, so defined, they would appear to be beyond the reach of the federal law.

Notwithstanding these complications, and given that the vast majority of entities in the U.S. already fall under FTC jurisdiction, the legal meaning of "covered entity" is unlikely to provide significant limits to the preemptive effect of § 405(a). Preemption may reach laws directed to most individuals, non-profits, as well as firms in an extremely wide array of industries, which, although already subject to the FTC's general § 5 jurisdiction, have not previously been subject to specific *federal* rules relating to their collection, use, disclosure, or transfer of privileged information.

b. Covered information, PII, personal identification information

Section 405(a) preempts state laws directed to "covered" entities' collection, use, or disclosure of "covered information," PII, "personal identification information." As detailed below, the definition of "covered information," is defined more narrowly than PII, and its variant, "personal identification information." The important effect of this is that state law directed to any of the three types of information is preempted; meanwhile, the substantive notice and opt-out provisions of the bill, *see* §§ 201(a)(1)(A), 202(a)(1)-202(a)(2), apply *only* to "covered information." As a result, the proposed Act wipes out state privacy protections for PII and "personal identification information," and substitutes federal protective measures for an even narrower range of "covered information."

"Covered information" includes PII, and "unique identifier information"—that is, "a unique, persistent identifier associated with an individual or a networked device," such as a cookie or device serial number. *See* § 3(3) (covered information, generally) *and* § 3(9) (defining unique identifier information). "Covered information" also includes any information that, when merged with PII or unique identifier information, could be used to identify specific individuals. § 3(3)(A)(iii). The definition of PII under the proposed Act generally corresponds to the definition adopted by the Network Advertising Initiative's Principles,[3] and includes, among other things, first and last names, telephone numbers, postal email addresses, credit card numbers, as well as biometric information. § 3(5). "Covered information" encompasses all of the above.

Critically, the bill specifically exempts from the definition of "covered information" any PII that is (a) available in public records, or (b) has been publicly reported, (c) PII that is work-related contact information, as well as (d) PII that is voluntarily disclosed or obtained with authorization from a public forum (such as a social network) that is itself (i) "widely and publicly" available, (ii) unrestricted with respect to access or viewing. § 3(3)(B). Accordingly, some PII, such as PII that is publicly available, may not be "covered." It is important to remember, however, that the preemption clause extends not just to state regulation of "covered information addressed in this Act," § 405(a)(1), but also to state regulation of PII and "personal identification information" (a similar term of art used in some state laws). § 405(a)(2). As a result, state laws that are directed to "covered information, PII, and "personal identification information," are all preempted. At the same time, the bill's substantive notice and opt-out provisions apply to *only* to "covered information." The effect of all this is that the proposed Act provides protection to a much narrower class of information than previously countenanced by state law.

Considered in conjunction with the bill's findings, discussed *infra*, these terms effectively define the substantive scope of the preemption clause. In sum, these terms expand the jurisdiction of the FTC over specific entities, thereby enlarging the bill's preemptive effect, wipe out state laws directed to a wide range of private information, and substitute federal protections for a narrower class of private information ("covered information").

2. Preemption of specific California laws

Honoring the broad objectives of the proposed Act will likely require preemption of a large array of long-standing and important state laws relating to consumer protection, privacy, and unfair competition. It is well beyond the scope of this memo to detail every state law that might be

[3] *See* Network Advertising Initiative, 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT (2008), at 5 (defining PII), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf.

impacted by the preemption clause of the proposed Act, but a review of relevant California law gives some indication of how just sweepingly the preemption doctrine might apply. It is important to note that, regardless of any changes made during the review and enactment process to cabin the scope of the preemption clause, residual uncertainty over the precise scope of preemption is likely to limit the efficacy of many state laws.

In California alone, enforcement of scores of industry- and technology-specific privacy-protecting laws may be preempted by passage of the proposed Act. *See* Appendix (table listing state laws likely to be preempted). The following analysis focuses on four specific laws that exemplify the likely substantive reach of preemption: Cal. Bus. & Prof. Code § 17200 (West 2011) (prohibiting unfair competition); § 22575 (requiring that any operator of a commercial website or online service that "collects personally identifiable information through the Internet" must "conspicuously post its privacy policy on its Web site"); Cal. Pub. Util. Code § 2891 (prohibiting telephone companies from disclosing personal calling patterns and lists, as well as subscriber "demographic information," without written consent); Cal. Gov. Code § 6218, *et seq*. (prohibiting online posting of personally identifiable information of reproductive health care providers, employees, volunteers, and family members, in certain circumstances).

California privacy laws provide a wide variety of enforcement mechanisms and remedies, ranging from private actions for injunctive and monetary relief, to public prosecutions that may result in fines or imprisonment. Under the proposed Act, however, only the FTC and state attorneys general may bring actions that sound "in whole or in part" upon violations of the proposed Act. § 404(b)(1). To ensure uniformity of application of the law, FTC enforcement preempts state attorney general enforcement actions against the same parties, § 403(2)(c), and the FTC retains the right to intervene or appeal cases originally brought by the states. § 403(2)(b). No private right of action is created under the law, § 406, and no party other than the FTC or a state attorney general may bring an action under the law. § 405(b)(1). State attorneys general also may not bring an action to enforce any of the provisions under Title III of the Act, including the provisions concerning data minimization, data integrity, and constraints on distribution of information. § 401(a).

Although the Act generally incorporates the FTC's usual enforcement powers, § 402(b)(1), including the existing scienter norms, the FTC's enforcement options are still narrowed by the Act. *Compare* § 402(a) ("knowing or repetitive violations"), 15 U.S.C. § 57b (consumer redress available for acts "which reasonable man would have known under the circumstances was dishonest or fraudulent"), *and* § 45(m)(1)(A) (civil penalties available for violations with "actual knowledge or knowledge fairly implied" in light of the circumstances). Notably, enforcement actions are authorized only in cases of economic or physical harm. § 403(a). This provision drastically limits application of the law, and effectively narrows the definition of privacy interests, as traditionally conceived by the FTC and others.[4] Civil penalties for actions brought by state attorneys general are also limited, § 404(a), and no criminal sanctions are contemplated. Finally, because there is no private right of action, damages and injunctive relief are not available to private parties. It therefore seems clear that the bill very significantly weakens the relief available for privacy-related harms.

a. Preemption of Cal. Bus. & Prof. Code § 17200

[4] FTC PRIVACY REPORT at 9 (agency's "harm-based model targeted practices that caused or were likely to cause physical or economic harm, or 'unwanted intrusions in [consumers'] daily lives'"). *But see* FTC PRIVACY REPORT, APPENDIX E-5 (Concurring Statement of Comm'r Rosch) (FTC has historically brought cases predicated on tangible harm).

Significantly, following the logic of *Fellows*, the proposed Act could be interpreted to preempt application of the states' various unfair competition laws,[5] at least to the extent they do not "relate to acts of fraud." § 405(b)(2)(C). California's own unfair competition law, Cal. Bus. & Prof. Code § 17200, is a heavily litigated statute that broadly proscribes "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Although § 17200 could arguably fall under the proposed Act's exemption from preemption for "laws that relate to acts of fraud," the issue presents a close call.

On the one hand, the plain text of § 17200 uses the term "fraudulent" and claims under the statute are often characterized as "consumer fraud." The mere mention of the term "fraudulent" could well prove persuasive to a court considering the applicability of § 17200 under § 405(b)(2)(C)'s fraud exemption. On the other hand, as an historical matter, the statute began as a common law trademark and trade name infringement law and grew to its current scope largely through judicially created doctrines. *Id.* at 2-A. Today, it is referred to by the state Supreme Court as California's "Unfair Competition Law" (UCL), *see, e.g., Kasky v. Nike, Inc.*, 27 Cal.4th 939, 949 (2002), and the "fraudulent" prong of § 17200 now turns on whether "members of the public are likely to be deceived." *Committee on Children's Television v. General Foods Corp.*, 35 Cal.3d 197 (1983).

It is widely accepted that "the type of 'fraud' contemplated by this section, however, bears little resemblance to common law fraud or deception." William L. Stern, BUS. & PROF. CODE SEC. 17200 PRACTICE (Rutter Group), Ch. 3-H (2011). *Accord Schnall v. Hertz Corp.*, 78 Cal. App. 4th 1144, 1167 (2000) ("The 'fraud' prong of [the UCL] is unlike common law fraud or deception"). In fact, under § 17200, none of the usual elements of common law fraud (misrepresentation, scienter, actual reliance, damage) are required to prove that "members of the public are likely to be deceived." *Schnall*, 78 Cal. App. 4th at 1167. "A violation can be shown even if no one was actually deceived, relied upon the fraudulent practice, or sustained any damage." *Id*. Unfortunately, I was unable to find any case law directly addressing whether § 17200 has been specifically preempted, or excepted from preemption, by other federal statutes as a law governing fraud.

Nonetheless, the uncertainty raised by the foregoing question is likely to significantly undermine the ability of private litigants, as well as local authorities, to enforce not just § 17200 itself, *see* § 17204 (authorizing enforcement actions by attorney general, district attorneys, county counsels, city attorneys and private citizens in certain circumstances), but also other state privacy laws for which § 17200 provides an implied remedy. *See, e.g.,* Cal. Bus. & Prof. Code § 22575 (discussed in next section). It is also worth noting that, regardless of whether § 17200 qualifies as a law that "relate[s] to acts of fraud," many other state unfair competition laws and "Little FTC" Acts do not use the statutory term "fraudulent," and are therefore significantly less likely to survive preemption analysis. *See infra* note 4. As a political matter, moreover, it seems quite likely that the drafters of the proposed Act intended to preempt these regulations and confine enforcement of privacy law to the FTC and state attorneys general. This intent may be clarified in any future Committee Reports and floor debates.

[5] At least 29 states have enacted so-called "Little FTC Acts" that mimic the substance and form of the FTC Act. Twenty-one states (including California) have unfair competition laws that differ in some respects. Justin J. Hakala, *Follow-On State Actions Based on the FTC's Enforcement of Section 5* at 5-6 (Wayne State Univ. Law Sch. Working Paper, Oct. 9, 2008), *available at* http://www.ftc.gov/os/comments/section5workshop/537633-00002.pdf.

The loss of § 17200 and other state consumer protection laws will, of course, significantly disrupt the ability of litigants to vindicate their privacy interests in the commercial context.

b. Preemption of Cal. Bus. & Prof. Code § 22575

The passage of the Commercial Privacy Bill of Rights will also likely preempt many core privacy regulations. Another California law that may be preempted by § 405(a) is the Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22575, which requires that any operator of a commercial website or online service that "collects personally identifiable information through the Internet" must "conspicuously post its privacy policy on its web site." The privacy policy must (1) identify the categories of PII collected, as well as any third-parties with whom PII is shared, (2) describe the process by which consumers can review and change collected PII, if one exists, (3) describe the process by which the operator notifies consumers of material changes to the privacy policy for its commercial Web site or online service, and (4) provide the effective date of the privacy policy. §22575.

To be considered in violation of § 22575, an operator must fail to post the policy within 30 days of receiving notice of noncompliance. *Id.* In addition, only knowing and willful, or negligent and material, failures to post a policy are considered to be violations. § 22576. That is, both a significant (e.g., material) misstatement, even if mistaken (e.g., negligent) will incur liability, as will a knowing misstatement—even if minor (e.g., immaterial). Although the statute does not specify what enforcement mechanisms or remedies might be available for violations, liability is presumably available under § 17200, which permits both state and local law enforcement authorities as well as private parties to bring enforcement actions under statutes that do not otherwise provide for a particular remedy.

As a threshold matter, § 22575 plainly "relate[s] to the collection, use, or disclosure of … personally identifiable information." Therefore federal law will completely preempt § 22575, except with respect to non-"covered entities." Although not all website or online service operators that collect PII will reach the 5,000-person threshold to qualify as a "covered entity" under the proposed Act, the information practices of every major website and Internet service will easily qualify as "covered" under § 3(2). Because the 5,000-person threshold is low, most start-ups will also be considered "covered entities."

As a result, all major websites and Internet websites, as well as most smaller operators, will be exempt from "*conspicuously*" posting a privacy policy under California law. Instead, under the Commercial Privacy Bill of Rights, covered entities will be required to provide only "*clear, concise, and timely*" notice, in "*readily accessible* form," of their information practices and the purpose of such practices (unless the FTC chooses to elaborate further on the law's requirements pursuant to the mandated rulemaking). § 201(a)(1). Current federal law does not affirmatively require website and online service operators to maintain a privacy policy, and it is uncertain what kind of disclosure might be required by the FTC and what leeway covered entities will retain. *Cf.* § 201(b) (FTC "shall consider the types of devices and methods individuals will use to access the required notice," and "may provide that a covered entity unable to provide the required notice which information is collected may comply … by providing an alternative time and means for an individual to receive the required notice."). Perversely, under preemption, only smaller, less pervasive online services and less-trafficked websites that do not qualify as "covered entities" will be required by California to maintain a "conspicuously" posted privacy policy.

Should "covered" operators fail to fulfill their obligations, under the Commercial Privacy Bill of Rights, only the FTC or the California Attorney General would be permitted to sue—in contrast to § 17204, which permits enforcement of § 17200 by district attorneys, county counsels, and city attorneys. In addition, no private remedy would be available to individuals harmed or deceived by virtue of a missing privacy policy, as it may be currently under § 22575 and § 17200. Given the vast scope of the Internet, it seems quite possible that the lack of any private cause of action could have detrimental effects on enforcement, given that law enforcement agencies are unlikely to have sufficient resources to enforce this provision of the law against every "covered entity." The future of privacy policies is therefore uncertain under the proposed Act.

c. Preemption of Cal. Pub. Util. Code § 2891

To take another example, California law prohibits telephone companies from "making available" a subscriber's personal calling patterns, including numbers called, and "demographic information about individual residential subscribers," among other things, "to any other person or corporation without first obtaining the residential subscriber's consent, in writing." Cal. Pub. Util. Code § 2891(a), *et seq*. *See also* Cal. Penal Code § 638(a) (prohibiting any person from purchasing, selling, or offering or conspiring to purchase or sell "any telephone calling pattern records or list, without written consent of the subscriber").

Telephone companies will, in virtually all cases, qualify as "covered entities." *See* § 3(2). Personal calling patterns and lists of numbers called, as well as demographic information about individual subscribers, all clearly fall under the ambit of the proposed Act's "covered information." *See* § 3(5)(B)(vi). It therefore seems quite clear that if the proposed Act were enacted, § 2891 would be preempted.

As a result, telephone companies would be permitted to disclose this information; but what kind of consent would be required for disclosure, if not "written consent," as required by California law? If calling patterns and lists, and individual demographic information are deemed by the courts to be "sensitive personally identifiable information"—that is, "information which, if lost, or compromised, or disclosed without authorization … carries a *significant* risk of economic or physical harm"—then opt-in consent would be required. *See* § 3(6)(A). However, if these kinds of information are determined to be non-sensitive PII, the disclosure of which poses less than "significant" risks, then opt-out consent would be required for disclosure. As a practical matter, this latter determination would likely defeat the privacy-protecting purpose of § 2891 and permit telephone companies to freely disclose the information until consumers opt-out. To a court, either interpretation might well seem plausible.

Although the proposed Act does not provide any private right of action for harm that results from unwanted disclosures, the California legislature saw to it that § 2891 does. § 2891(e) provides grounds for a civil suit against the telephone company and its employees.

At best, then, the Commercial Privacy Bill of Rights casts doubt on privacy protections available under California's laws. At worst, it practically defeats a state law specifically directed at keeping subscriber demographic and telephone use information private by replacing a written consent regime with an opt-out consent option. Either way, the bill represents a significant threat to individuals' privacy interests.

d. Preemption of Cal. Gov. Code § 6218

Finally, the proposed Act would likely preempt, and render ineffective, state laws that specifically protect various vulnerable groups, such as reproductive healthcare workers targeted by anti-abortion activists. Cal. Gov. Code § 6218 prohibits "any person, business or association" from posting online the home address, telephone number, or image of any "provider, employee, volunteer, or patient of a reproductive health care services facility" (or others at the same address) with the intent to "incite a third person to cause [them] imminent great bodily harm," where harm is likely. *See also* Cal. Gov. Code § 6254.21 (prohibiting posting or displaying personal information of any elected or appointed official if the official has made a written demand not to have the information posted).

Once again, any anti-abortion activist or group that collects the personal information of 5,000 people (including, for example, its members), will likely fall under the proposed Act's definition of "covered entities." *See* § 3(2). Home addresses and telephone numbers are explicitly contemplated as PII under the Act, and images of individuals would almost certainly also be considered "covered information." *See, e.g.,* §§ 3(3)(A)(iii), 3(3)(A)(viii). Thus, § 405(a) would likely preempt application of § 6218 to a "covered" anti-abortion activist's online posting ("use") of a health worker's PII.

Regardless of whether such information would qualify as "sensitive personally identifiable information," and therefore require opt-in consent under the proposed Act, private victims of this behavior would not have any remedy available to themselves under the Commercial Privacy Bill of Rights. Currently, under § 6218, any affected party may themselves seek injunctive or declarative relief. Remedies include court costs, attorneys fees, as well as money damages (actual damages tripled, or $4,000). *See* § 6218(a)(2). Under the proposed Act, however, victims of such behavior would have to petition the FTC or California Attorney General for protection. To the extent that government enforcement takes more time and is less effective than private enforcement of § 6218, reproductive health care workers and patients, as well as their families, may be placed in danger by the proposed Act.

Examination of the foregoing state laws demonstrates that the preemptive effect of the Commercial Privacy Bill of Rights could have very serious, unintended consequences. The foregoing are only four of hundreds of state laws, application of which could be preempted by § 405(a). The Commercial Privacy Bill of Rights effects nothing less than a drastic federal overhaul of privacy protections that is likely to eliminate years of carefully crafted state regulations designed to protect Californians.

III. Conclusion

Section 405(a) of the Commercial Privacy Bill of Rights is likely to preempt a very broad array of carefully-tailored, context-specific state laws that protect privacy interests, as well as many key consumer protection laws. This drastic overhaul of privacy law is likely to deprive those who suffer privacy harms of any private right of action, as well as of many important alternative forms of relief.

Appendix: California Laws Likely Preempted By The Commercial Privacy Bill of Rights

Citation	Substantive provisions
Cal. Civ. Code § 1799.3	Prohibits videocassette sales or rental service from disclosing personal information without written consent.
Cal. Civ. Code §§ 1799.1-1799.1b	Requires credit card or telephone company that receives request for change of address, and then a new card or service request, to notify consumer at the former address of record.
Cal. Civ. Code § 1798.90.1	Prohibiting bars, car dealers, and others from collecting information when swiping driver's license for any purpose other than verifying age or authenticity of license, to verify a check, or when otherwise required by law.
Cal. Civ. Code § 1798.85	Regulates uses of individual social security numbers. Prohibits, *inter alia*, public posting of individual social security numbers, and requiring individuals to disclose social security numbers in certain circumstances.
Cal. Civ. Code §§ 1798.83-1798.84	Permits consumers to discover how their personal information is shared by companies for marketing purposes and encouraging businesses to allow individuals to opt-out.
Cal. Civ. Code §§ 1798.80-1798.81.5	Requires businesses to protect personal information with "reasonable security" measures and to shred, erase, or modify personal information when disposing of customer records.
Cal. Civ. Code § 1798.79.8	Prohibits domestic violence service providers from being required to reveal its clientele's personally identifying information as part of a funding application to grant providers.
Cal. Civ. Code § 1798.79, *et seq.*	Makes it a misdemeanor to intentionally remotely read or attempt to read another person's identification document that uses RFID without knowledge or consent of victim.
Cal. Civ. Code § 1749.60, *et seq.*	Prohibits issuers of supermarket club cards

	from requesting driver's license numbers or social security numbers, and from selling or disclosing consumer information, with limited exceptions.
Cal. Vehicle Code §§ 11713.3, 11713.25	Prohibits auto manufacturers and distributors, as well as computer vendors, from accessing, modifying, or extracting information from an auto dealer's computer system without providing safeguards to protect that information.
Pub. Util. Code § 2891-2894.10	Prohibits telecom companies from disclosing personal information of residential customers without written consent, with limited exceptions.
Cal. Labor Code § 226	Requires employers to print no more than last four digits of social security numbers on pay stubs, or to use unique employee identifier instead.
Cal. Penal Code § 638	Prohibits purchase or sale of any telephone calling records or list without written consent.
Cal. Penal Code § 637.9	Prohibiting use of child's personal information to directly contact child or parent to offer a commercial product or service and knowing failure to comply with parent's request to take steps to limit access to information. Marketers must comply with parent's written request withdrawing consent to use child's personal information.
Cal. Penal Code § 637.5	Prohibits satellite or cable television providers from providing third party with subscribers' individually identifying information without express written consent.
Cal. Penal Code § 502	Prohibits use of data, computer, or network wrongfully obtain data.
Cal. Bus. & Prof. Code § 17200	Prohibits unfair competition.
Cal. Bus. & Prof. Code § 22948	Prohibits online "phishing" for personal information.
Cal. Bus. & Prof. Code § 22947.2	Prohibits use of spyware that collects personally identifiable information.
Cal. Bus. & Prof. Code § 22575	Requires that any operator of a commercial website or online service that "collects

	personally identifiable information through the Internet" must "conspicuously post its privacy policy on its Web site."
Cal. Bus. & Prof. Code § 17538.41	Prohibits transmission of unsolicited text-message advertisements under certain circumstances.
Cal. Gov. Code § 6254.21	Prohibits posting or displaying personal information of any elected or appointed official if the official has made a written demand not to have the information posted.
Cal. Gov. Code § 6218, *et seq.*	Prohibits online posting of personal information of reproductive health care providers, employees, volunteers, and family members, in certain circumstances.