Want To End The Litigation Epidemic? Create Lawsuit-Free Zones

By Eric Goldman

Forbes Tertium Quid blog, April 10, 2013

You already know the legal system is screwed up, but I'd like to be more specific about why. When we say lawyers are "litigious," what we really mean is that too many lawyers spend too much time thinking about how to sue someone else. Similarly, legislators spend their time manufacturing new laws, which usually create more opportunities for people to sue each other. Law professors typically do the same; the typical law review article focuses on a social problem and proposes to solve it with a new legal rights. (Just take a look at the torrent of recent academic articles about privacy and you'll see what I mean).

I don't understand why we as a society spend so much time thinking about suing people. I'm much more interested in figuring out how we can *stop* suing each other. If we could create "lawsuit-free zones," we'd avoid the individual and social costs of adjudicating disputes, including the' settlements payments to get rid of nuisance and otherwise meritless lawsuits. Plus, lawsuit-free zones stimulate business investments by providing more legal certainty to entrepreneurs, which should translate into more jobs. So finding ways to dial down litigation might be the best "jobs stimulus" effort our legislators could undertake.

The way to create lawsuit-free zones is through "immunities" and "safe harbors." Immunities categorically eliminate legal liability in the specified contexts. Safe harbors allow defendants to avoid liability if they take the specified steps. Both help motivate socially beneficial and job-creating activity. Three examples:

* 47 USC 230, an immunity that says websites aren't liable for user-generated content (UGC) except with respect to intellectual property claims and a small number of other specified circumstances. This immunity has become the foundation of the UGC industry, which has created lots of jobs and improved the flow of socially beneficial information.

* 17 USC 512, a safe harbor for websites to avoid liability for user-committed copyright infringement. While this safe harbor has some serious flaws (especially when compared to 47 USC 230), it has still provided enough legal certainty to help the UGC industry grow.

* California Business & Professions Code (B&P) 16600, which voids non-compete clauses in California in most circumstances. In her book *Regional Advantage: Culture and Competition in Silicon Valley and Route 128*, Prof. Annalee Saxenian persuasively demonstrated that this immunity plays an essential role in Silicon Valley's success.

While technically not immunities and safe harbors, two other examples of legal doctrines that help create a lawsuit-free zone:

* the "standing" requirements in Article III of the Constitution, which requires (among other things) that plaintiffs show they have suffered a cognizable harm before they get access to the Federal court system. In particular, Article III standing efficiently kills meritless Internet privacy

cases where plaintiffs have suffered no real harm. In turn, the lawsuit-free zone created by Article III standing facilitates experimentation and innovation on privacy-related matters.

* Anti-SLAPP laws applicable to lawsuits brought to suppress socially beneficial speech. Anti-SLAPP laws end those lawsuits quickly and put plaintiffs on the hook for the defendant's attorneys' fees. California has a strong anti-SLAPP law, and it's dramatically reshaped many litigation areas.

Based on these examples, it's possible to reverse-engineer some key attributes of immunities/safe harbors that help create strong lawsuit-free zones:

* **Minimal Formalities/Prerequisites.** Immunities and safe harbors work best when they don't require technical steps that might be inadvertently overlooked or mishandled. Thus, Section 230 automatically protects every UGC website; and B&P 16600 automatically protects every employee and future employer. In contrast, Section 512 has a long list of technical prerequisites (what we call "formalities") that can disqualify well-meaning but sloppy or uneducated entrepreneurs–or, at minimum, prompt expensive legal fights over whether the formalities have been satisfied.

* **Drafting Brevity**. The longer the statute, the more things that plaintiffs can fight over. Section 230(c)(1)'s main operative language is only 26 words, which doesn't give plaintiffs a lot of bases to fight. In contrast, Section 512 runs for thousands of words, creating dozens of different vectors to attack a safe harbor defense. As a result, with so many more words to fight over, Section 512 judicial opinions are typically much lengthier–and more expensive to the litigants–than Section 230 opinions.

* **Global Preemption**. Because too many legal doctrines overlap, an immunity/safe harbor that protects defendants against only one legal doctrine is typically useless; plaintiffs can just focus their energies on other overlapping causes of action that might apply to the same behavior. Thus, an effective immunity/safe harbor eliminates the defendant's liability completely, regardless of what cause of action the plaintiff asserts. For example, Section 230 and Article III standing work so well because they usually categorically preempt all causes of action asserted by the plaintiff, no matter how many or wide-ranging.

* **No Weasel-Words**. Subjective elements of an immunity or safe harbor, such as the requirement that the defendant act in "good faith" or "innocently," are tautological. They give judges an opportunity to inject their normative views, and they create more opportunities for plaintiffs to fight. As a result, weasel-words can destroy the effectiveness of an immunity or safe harbor. For example, one part of Section 230 (Sec. 230(c)(2)) depends on the defendant's "good faith" conduct; that part has been comparatively useless to defendants as a result.

* **Specifically Described Scienter**. "Scienter" means the amount of the defendant's bad knowledge or intent. I favor immunities and safe harbors that protect defendants regardless of their scienter. Section 230 does that; websites aren't liable for third party content no matter what the plaintiff alleges about the website's knowledge of the content. Realistically, though, legislators typically will not excuse defendants who have sufficiently bad scienter. If so, the

statute should spell out precisely when the defendant has the requisite scienter. For example, Section 512 defines exactly when the defendants have disqualifying scienter about user-caused copyright infringement–defendants must have actual knowledge or awareness of apparent infringement–and it defines the elements of a copyright owner's takedown notice that is sufficient to provide actual knowledge. Unfortunately, Section 512 has been a failure at circumscribing disqualifying scienter. Courts have added other types of disqualifying scienter ("inducement" and "willful blindness" are two examples) that have encouraged plaintiffs to sue over behavior that should be plainly protected by the safe harbor. Thus, Section 512 has become a good cautionary tale of how an immunity or safe harbor's failure to adequately circumscribe disqualifying scienter properly can undermine the immunity/safe harbor's efficacy.

* **Quick Resolution**. An effective immunity/safe harbor ends unmeritorious lawsuits quickly and cheaply. At minimum, it should keep the case out of discovery, where the costs grow so quickly that the lawsuits punish even successful defendants. Veoh provides a good example of how a safe harbor can become useless if it takes too long. The Ninth Circuit ruled Veoh had properly qualified for a Section 512(c) safe harbor, but the ruling came too late. By the time the Ninth Circuit blessed Veoh's practices, Veoh was already dead due to its unsupportable litigation costs. In contrast, Section 230 cases are usually decided on motion to dismiss grounds and thus are comparatively quick and cheap for defendants, making the immunity a more useful tool for entrepreneurs.

* **Sanctions for Bogus Claims**. Plaintiffs should internalize the costs of their bad choices. For example, anti-SLAPP lawsuits make plaintiffs pay defendants for bring anti-social lawsuits. This risk that the plaintiff will write a check to the defense–for a lawsuit initiated by the plaintiff–raises the strategic stakes for plaintiffs. It also makes defendants financially whole.

California's Latest Effort To 'Protect Kids Online' Is Misguided And Unconstitutional

By Eric Goldman

Forbes Tertium Quid blog, Sept. 30, 2013

California recently enacted SB 568 (Business & Professions Code 22580) to prevent certain types of online advertising from being shown to kids. Like so many other state efforts to regulate the Internet, the new law takes an understandable regulatory objective and turns it into a sloppily drafted and misguided law that will not survive judicial challenge intact.

What the Law Does

The new law says websites/apps directed to minors may not advertise items that minors (under 18) cannot legally purchase. Restricted items include the usual suspects (alcohol, guns, tobacco products and lottery tickets) and less obvious items, such as diet pills containing ephedrine, spray paint and etching cream. All other websites/apps must take "reasonable actions in good faith" to avoid specifically directing ads for restricted items to known minors. Kid-directed websites/apps can shift the compliance burden to their advertising services simply by notifying the service they are kid-directed. The law also prohibits using, disclosing or compiling a minor's personal information to help advertise restricted items to minors.

Like its "online eraser" cousin (enacted in the same bill), this law is riddled with ambiguities. I'll identify four:

First, the law protects minors' "personal information" but doesn't define the term. Without a definition, the term is meaningless. We know that just about any data can be combined with other data to personally identify individuals.

Second, the law doesn't define who is an "advertising service." Surely it covers ad networks like Google AdSense, but do the obligations extend to other players in the online ad industry: ad serving technology providers, ad agencies, buyers of remnant ad inventory, etc.?

Third, the law restricts "specifically directing" an ad to a minor, but I have no idea what that means. The law suggests that "run of site" ads should be OK, but I'm not sure when other targeting efforts trigger the restriction.

Finally, like its online eraser counterpart, the law establishes a potentially illusory distinction between teen-oriented websites and adult websites.

Legal Problems With the Law

Some of the more obvious legal deficiencies of the law:

The Dormant Commerce Clause. As I've mentioned before, I think state attempts to regulate Internet activity categorically violate the Dormant Commerce Clause, the Constitutional doctrine that says only Congress can regulate interstate commerce. For example, does a website/app with

no physical connection to California have to comply with this law simply because a California minor uses it? If yes, that's a problem under the Dormant Commerce Clause.

The Dormant Commerce Clause problem is even more pronounced for advertising services located outside California. Assume a Florida-based website tells a Massachusetts advertising service to block ads for restricted items because it's a kid-directed site and might have California minors using it. At that point, the restriction would impact all non-California users of the Florida-based website–even if some items may be legal for minor users to purchase outside California. Thus, the California law regulates communications between two non-California parties, which California cannot do constitutionally.

The First Amendment. This law tries to suppress speech on the basis of its content and possibly the identity of its speaker (i.e., kid-oriented websites). Under the Supreme Court's recent Sorrell decision, the law might be subject to the highest level of scrutiny, which would almost certainly ensure its unconstitutionality. If the Sorrell precedent doesn't apply, the law will be subject to the lower, but still rigorous, scrutiny applicable to advertising. This analysis is unpredictable; courts usually support legislative efforts to protect the kids, but (as discussed below) courts also have good reason to question this law's efficacy. (For a possibly analogous discussion, see the recent Fourth Circuit ruling striking down a Virginia law restricting college newspapers from running alcohol ads).

47 USC 230 Even if the law survives the Constitutional challenges, much of it is preempted by 47 USC 230, the 1996 federal law that says websites and apps aren't liable for third party content or advertising. The law explicitly hold websites and apps responsible for third party ads–exactly what Section 230 prohibits. Other state laws attempting to hold online publishers responsible for third parties' online ads have failed due to Section 230. See, e.g., the Backpage cases and the battle over online prostitution ads. From my perspective, Section 230 preemption for the law's application to third party ads isn't even a close legal question.

Implications

Protecting kids online remains a perennial regulator rallying cry, but does this law actually help minors? Any website or app that cares about its public reputation voluntarily wouldn't target ads to kids for restricted items. How many examples of bad publisher/advertiser behavior have we seen that this law would correct? If the answer is "not many," we have some reason to question the cost-benefit of the law.

Furthermore, even if the prohibited advertising reaches the minors, that doesn't change the fact that *the minors still can't buy the advertised items legally*. I recognize that retailers aren't always careful about age verification and black markets exist, but suppressing the ads is just a prophylactic to support the existing sales bans. It's not clear if the benefits of the prophylactic step outweighs the costs of suppression.

It's not surprising this law both has questionable merit and is undermined by weak drafting. Simply put, over the past 15+ years, state legislatures have proven that they suck at regulating the Internet. Worse, state legislatures don't learn from their mistakes. They systematically make

avoidable drafting errors, ignore Section 230 and Constitutional considerations, and pass high-cost/low-benefit Internet regulations.

Knowing that state legislatures can't avoid this trap, Congress needs to cut them off. Section 230 already should squelch many of the bad regulatory impulses of state legislators, but it's clearly not enough (as evidenced by this law, which unreservedly disregards Congress' plain instructions). Just like Congress once imposed a moratorium on state taxation of the Internet, Congress should enact a broad moratorium on new state efforts to regulate the Internet. Basically, until states learn how to treat their Internet regulatory power with more respect, Congress should give them a regulatory time-out.

Congress' intervention is especially important because leading Internet companies like Google and Facebook won't always defend the Internet from overzealous state legislators. Here, Google and Facebook let the California legislature enact a lousy law with an impossible-to-miss Section 230 problem. Why didn't Google and Facebook fix or kill the law? I imagine it's because Google and Facebook plan to comply with it. After all, compliance won't cost them too much while their rivals might not be so fortunate. It's a reminder that Internet incumbents won't necessarily look out for us when our legislators go rogue. That makes it even more paramount that we as Internet users communicate our legislative priorities during election season.

California's New 'Online Eraser' Law Should Be Erased

By Eric Goldman

Forbes Tertium Quid blog, Sept. 24, 2013

People mocked Google CEO Eric Schmidt for his 2010 suggestion that teenagers should change their names when they turn 18 to avoid the indiscreet and ill-advised Internet posts they made as youths. The California legislature thought it had a better solution for this problem and enacted a law, SB 568 (California Business & Professions Code Sec. 22581), that allows kids to use an "online eraser" to wipe away some of their past posts. Unfortunately, California's solution is no less mockable than Schmidt's.

What the Law Does

The new law says that websites and apps "directed" to minors, or that have actual knowledge that a user is a minor, must allow registered users under 18 to remove (or ask the provider to remove or anonymize) publicly posted content and make certain disclosures to these users. A website/app is "directed" to minors when it is "created for the purpose of reaching an audience that is predominately comprised of minors, and is not intended for a more general audience comprised of adults."

The law is riddled with ambiguities, so let me explore just three:

First, it may not be clear when a website/app is "directed" to teens rather than adults. The federal law protecting kids' privacy (Children's Online Privacy Protection Act, or COPPA) only applies to pre-teens, so this will be a new legal analysis for most websites and apps.

Second, the law is unclear about when the minor can exercise the removal right. Must the choice be made while the user is still a minor, or can a centenarian decide to remove posts that are over 8 decades old? I think the more natural reading of the statute is that the removal right only applies while the user is still a minor. If that's right, the law would counterproductively require kids to make an "adult" decision (what content do they want to stand behind for the rest of their lives) when they are still kids.

Third, the removal right doesn't apply if the kids were paid or received "other consideration" for their content. What does "other consideration" mean in this context? If the marketing and distribution inherently provided by a user-generated content (UGC) website is enough, the law will almost never apply. Perhaps we'll see websites/apps offering nominal compensation to users to bypass the law.

The law takes effect January 1, 2015. That gives plenty of time for court challenges or the legislature to rethink its errors, though I'm not sure either are likely.

Why It's A Bad Law

I don't believe any state has ever passed a beneficial Internet regulation, so it's hardly surprising I dislike this law too. Some of my objections to this law:

Dormant Commerce Clause. My position is that states categorically lack authority to regulate the Internet because the Internet is a borderless electronic network, and websites/apps typically cannot make their electronic packets honor state borders. In this case, unless they ask for geographic information, many websites/apps don't know what state a registered user comes from. Now what? Do all websites/apps around the country have to comply with California's law on the chance that some users may come from California? That would violate the Dormant Commerce Clause, a Constitutional doctrine that says only Congress can regulate interstate commerce. Or does this law only apply to websites/apps with physical operations in California? The law doesn't clarify its jurisdictional nexus, leaving that question open for future fights and a potential Constitutional challenge.

The Illusion of Control. The law only allows minors to remove their content from the site where they posted it; and the removal right doesn't apply where someone else has copied or reposted the content on that site. Removing the original copy typically accomplishes the minor's apparent goal only when it's the only copy online; otherwise, the content will live on and remain discoverable. Given how often publicly available content gets copied elsewhere on the Internet–especially when it's edgy or controversial–minors' purported control over the content they post will be illusory in most circumstances.

Collateral Damage. Removing content from the Internet can create collateral damage. Many UGC websites encourage users to engage each other in conversations through comments and threaded discussions. Removing a piece of the discussion can make the entire thread nonsensical. To avoid this bad user experience, the website/app might choose to delete the whole thread, in which case the minor's decision to remove his/her content will detrimentally affect other people's content too. Even if the website/app preserves other people's contributions, the content removal breaks incoming links from around the web and may render those remote discussions nonsensical.

Admittedly, these adverse consequences are currently possible when websites/apps voluntarily allow users to remove their content, as many UGC websites/apps do. Indeed, I think UGC industry best practices give users substantial control over publishing, editing and removing their content because users demand such controls.

But websites sometimes justifiably restrict users' content removal, especially when other users have responded to or build upon the content. For example, Tumblr restricts its users' removal rights when other users have "reblogged" the content. (For what it's worth, I believe Tumblr's reblogging functionality fits within an exception in the new law, so perhaps more websites/apps will replicate the functionality). This law reduces websites/apps' discretion on how to maintain the editorial integrity of their databases, and odd consequences will surely follow.

More generally, consistent with the "right to forget" meme generally, this law mandates that minors can try to rewrite history….but rewriting history hinders society's ability to understand where we came from and why things are the way they are.

Extending COPPA. For over a decade, we've know how to deal with COPPA: if at all possible, avoid dealing with kids 12 and under, in which case COPPA doesn't apply. This law creates a new class of websites/apps that can ignore COPPA but must comply with this law because they deal with teens. Thus, the law burdens a large swath of websites with the obligation to research if the law applies to them, and it will impose compliance costs on some of those.

First Amendment. The law completely ignores the possibility that UGC websites/apps have their own First Amendment interests independent of its users' First Amendment interests. By forcing UGC websites/apps to stop publishing users' content when the websites/apps might view that content as contributing to their own expressive statements, the law creates a potential First Amendment collision. Two examples should illustrate the point:

Example 1: A newspaper prepares a collection of stories, written by teens, about their first-hand experiences with cyber-bullying. These stories are combined with other content on the topic: articles by experts on cyberbullying, screenshots of cyberbullying activity online, and photos of victims and perpetrators. After the newspaper publishes the collection, one of the teenagers changes his/her mind and demands that the newspaper never reprint the collection, and seeks a court order blocking republication. Does the newspaper have a potential First Amendment defense to the court order? Yes, and I don't think the question is even close.

Example 2: a UGC website creates a topical area on cyberbullying and asks its registered users, including teens, to submit their stories, photos, screenshots and videos on the topic. The website "glues" the materials together with several articles written by its employees. Does the website have a First Amendment interest in continuing to publish the entire collection? Yes, and like the newspaper example, I don't think it's close.

The First Amendment analysis gets more complicated because we're dealing with teenagers, who typically have the legal right to void their contracts if they choose. So, even if a website gets an irrevocable copyright license from the teen, the teen should be able to change his/her mind. However, once the contract is "complete," it's no longer voidable. For an example of how publication of a copyrighted work might "complete" a website's contract with a teen, see the 2008 AV v. iParadigms case. Alternatively, the website could obtain parental ratification for the copyright license (required under COPPA for under-13 users). It's interesting the online eraser law doesn't address the possibility that parents may supervise, approve or ratify their kids' publications that are subject to the removal right.

As a practical matter, most websites/apps won't assert First Amendment protection for continuing to publish their users' content. (It's clear Google and Facebook won't because they acquiesced to the law). Indeed, the constitutional issue will only come up if (1) the website/app seeks an irrevocable license from users, which most websites/apps don't do, (2) minor users can't void that license, and (3) the website/app doesn't provide technological tools that permit users ongoing access to edit or delete their content. It's a rare situation where all three of those requirements will be satisfied. Plus, those websites/apps could avoid the issue by paying the kids a nominal amount for their contributions.

Still, by disrespecting the possibility that the website/app may have its own First Amendment interests, the law should be vulnerable to a First Amendment challenge in some circumstances.

What Should Businesses Do?

Let's assume the law survives any court challenges, and the California legislature doesn't backtrack. What should UGC websites do?

Don't Collect Age Information. To avoid being obligated to comply with COPPA, it's already a standard recommendation that websites shouldn't collect age information unnecessarily or casually. This law reinforces that advice. Websites/apps should NEVER ask for age information unless they have a good business reason for doing so; in which case, they must be prepared to deal with the consequences of knowing users' ages (such as bouncing under-age users).

Unfortunately, the law doesn't address the possibility that websites/apps might learn a user's age involuntarily (another sign of sloppy drafting). For example, a user might self-report his/her age to customer service representatives, or one user might reveal that another user is under-age. What then? Apparently, the legal obligation will spring into effect in any of those circumstances, which leads to my other suggestion….

Content Removal Doesn't Have to Be Automated. The law implicitly anticipates, but doesn't require, that most websites/apps will provide automated removal tools to their users. Instead, websites/apps can require users to manually request content removal, such as making the request via physical mail and providing adequate information to authenticate age. Content removal needs to be available to minors, but it doesn't have to be easy.

Conclusion

This law is just the latest attempt by legislatures to tell content database managers how to manage their databases–an endeavor that legislatures have repeatedly proved that they are terrible at doing (see, e.g., the Fair Credit Reporting Act). Given how the law substantially overlaps with current industry best practices, it's mostly annoying because it imposes extra compliance costs for little benefit. However, to the extent it overrides the limited cases where websites/apps would justifiably choose to restrict content removal, the law may harm the information ecosystem. It's a legislature's choice to preference the individual interests of minors over these social considerations, though it's probably a poor choice. Given that it won't actually provide minors with a well-functioning digital eraser, the choice appears even more puzzling.

This law also reminds us that regulators cannot resist loving the Internet to death. California alone considered an astounding 215 bills containing the word "Internet" this legislative session. The sheer volume of this regulatory frenzy, combined with sloppy drafting we see in state legislation all too frequently, will undoubtedly harm the Internet industry, even if any single proposal might have been in our interests.

How California's New 'Do-Not-Track' Law Will Hurt Consumers

By Eric Goldman

Forbes Tertium Quid blog, Oct. 9, 2013

California enacted a new law (AB 370) requiring many websites to disclose more information about how they track users. Websites that collect personal information about their users must disclose (1) how they respond to a web browser's "do not track" (DNT) signal, and (2) if third parties can collect personal information across a network of sites. The law doesn't require websites to honor browser DNT signals or block third party tracking; it simply tries to increase transparency about the website's practices. Despite that intent, the law almost certainly doesn't help consumers, though the law is a win for other constituents. An assessment of winners and losers from this new law:

Winner: California's Department of Justice's Privacy Enforcement and Protection Unit. A couple of years ago, the California Attorney General's office assigned a group of prosecutors to work the Internet privacy beat. The unit has struggled to find good cases to prosecute; its flagship prosecution has been the low-stakes claim that Delta Airline's mobile app didn't adequately display a privacy policy. The new law vastly expands the unit's potential enforcement targets–basically, every California website that doesn't promptly update its privacy policies.

Winner: Plaintiffs' Lawyers. I doubt plaintiffs' lawyers will sue websites for failing to make the required disclosures. Instead, I expect plaintiffs' lawyers will troll through the new disclosures looking for litigation-bait. Because a browser's DNT signal communicates ambiguous information to the website, a website's explanation of how they treat that signal necessarily will be ambiguous as well, leaving room for plaintiff lawyers to misinterpret and over-interpret the website's disclosures. Furthermore, I expect plaintiffs' lawyers will try to establish liability for websites that admit they don't honor the browser's DNT signal.

Winner: Reporters. Reporters will surely generate good link-bait by writing articles mocking and shaming some high-visibility websites.

Winner: Do-Not-Track Advocates. For years, industry representatives, advocates and technologists have been trying to define what it means to "track" online behavior so that industry could build solutions to effectuate consumers' tracking preferences. Those negotiations broke down spectacularly last year, and efforts to revitalize the process this year have failed. This law bypasses all of those efforts. In effect, the law lets browser manufacturers create and self-define their DNT signals, and websites must explain what they do with those signals. While this outcome gives a lot of power (too much?) to browser manufacturers, it does break the negotiation logjam while giving privacy advocates some tangible output for their efforts.

Loser: Websites. Websites will incur numerous costs due to the law: (1) determining what, if anything, they have to do to comply with the law, (2) figuring out how to describe their practices, (3) keeping those descriptions current over time, even as browsers change their signals and websites evolve their service offerings, and (4) dealing with the inevitable enforcement actions and lawsuits, meritorious or not. Most privacy advocates would scoff at these costs (or secretly

celebrate them), but these costs are yet another de facto tax on the Internet ecosystem. The tax might be justified if it produces commensurate social benefit, but…

Loser: Consumers. We already know consumers don't read privacy policies, so putting new disclosures into privacy policies won't lead to more informed consumers. Consumers also routinely acquiesce to browsers' default DNT signals, so consumers today aren't making informed choices about their desired tracking. Will the new disclosures required by this law improve either situation? No.

Worse, the concept of "tracking" is murky to consumers. Beyond the reference to browser DNT signals, the law specifically applies to only one type of tracking: the use of "personally identifiable information" to track users across time and over multiple websites. Thus, the law doesn't address a website's internal tracking like Amazon's personalized recommendations; the use of third party analytic services; tracking based solely on IP addresses (or browser settings) if that tracking information isn't combined with personally identifiable information; and many other types of behavior that might constitute "tracking."

Due to the semantic ambiguity of "tracking," consumers might mistakenly infer that a website publicly declaring that it is honoring browsers' DNT signal isn't "tracking" them. To the extent consumers even see the disclosures, it will almost certainly mislead them, and perhaps cause them to overestimate their protection. This reminds me of how California's current requirement that websites display "privacy policies" misled consumers into thinking those documents protected them.

Loser: The California Legislature. Mandatory disclosure laws rarely succeed. And state legislatures suck at regulating the Internet.

California's New Law Shows It's Not Easy To Regulate Revenge Porn

By Eric Goldman

Forbes Tertium Quid blog, Oct. 8, 2013

California enacted a new law (SB 255, codified as California Penal Code 647(j)(4)) against "revenge" porn, sometimes called "involuntary" porn. The law says it is "disorderly conduct" for a defendant to take intimate and confidential recordings, such as photos or videos, and then distribute them to intentionally cause serious emotional distress to the victim.

The final version of the law is significantly less ambitious than earlier drafts, and there's fairly widespread agreement the law as passed doesn't do much. It's easy to see the law's limited scope by enumerating what it doesn't cover:

* *"selfies."* If the victim makes the recording him/herself, the law doesn't apply.
* *redistributors*. The law only applies to the person who makes the recording. Everyone else who might redistribute the recording, including operators of websites that encourage users to post revenge porn, are not covered by the law.
* *hackers*. If a malicious third party obtains a recording by hacking into the victim's computer or cellphone and then distributes the recording, the law doesn't apply.
* *confidentiality disputes*. The law applies to "circumstances where the parties agree or understand that the image shall remain private." This might be obvious if the victim never consented to being recorded at all. In other cases, the defendant and victim may disagree about their expectations for the recording, which would make conviction difficult or impossible.
* *insufficient intent to cause emotional distress*. The law only applies when the defendant intends to cause the victim severe emotional distress. It may be hard for prosecutors to prove the defendant's intent without an admission from the defendant or a piece of "smoking gun" evidence.

In sum, California's new revenge porn law only covers one category of involuntary porn. As a result, I would be surprised if we see many prosecutions under the statute.

Nevertheless, other laws already apply to other involuntary porn categories. For example, hacking into someone's computer or cellphone is already illegal; if the victim made the recording him/herself, copyright law protects it; and if the parties had confidentiality expectations, privacy doctrines may apply. Anti-stalking and anti-harassment laws also can apply to involuntary porn, especially where a defendant distributes recordings to hurt the victim. Indeed, we have so many laws and crimes already on the books, it's challenging to find any examples of incivil or anti-social behavior that isn't already illegal under multiple overlapping laws.

This helps explain why it's hard to develop new laws to combat involuntary porn. California's new law wasn't very ambitious, but an ambitious law seeking to criminalize behavior that isn't already illegal will run into at least two major limits on legislative power.

First, California's new law probably sidesteps First Amendment problems by requiring an intent to cause serious emotional distress. Without such a restriction, involuntary porn laws can face significant First Amendment limits. Intimate depictions are often part of other people's life

history–a story that person may want to tell in full. Further, by design, privacy laws suppress the flow of truthful information. For example, consider Anthony Weiner's sexting photos. California's new law wouldn't apply to them (they were selfies), but any law restricting a recipient's redistribution of those images may substantially hinder important social discourses. The recipient could publicly claim that she received sexting photos from a famous politician, but she may need to provide photographic proof to substantiate her claims–especially in the face of the politician's inevitable denials. Weiner's sexting photos provide crucial evidence of his dubious decision-making and recidivism, so any law that interfered with their disclosure may violate the First Amendment.

Second, involuntary porn laws would help victims more if they applied to website operators who republish user submissions. However, state legislatures cannot impose such liability due to 47 USC 230, the 1996 federal law that says websites aren't liable for third party content.

So where will the policy debates over involuntary porn go? Surely California's small incremental step isn't the final word on the matter. However, the legal limits that curbed California's ambition provide helpful insight to other legislators who hope to strike more boldly against involuntary porn.

Big Problems in California's New Law
Restricting Employers' Access to Employees' Online Accounts
By Eric Goldman
Forbes Tertium Quid blog, Sept. 28, 2012

California Governor Jerry Brown signed two laws restricting demands for social media accounts or login credentials. Senate Bill 1349 restricts schools' access to students' social media accounts. Assembly Bill 1844 restricts employers' access to employees' social media accounts.

Superficially, both laws sound like a good idea. It's ridiculous to force people to disclose social media content if they don't want to do so; not only can that violate the accountholder's privacy, but it can violate the privacy rights of innocent third parties. Demanding access to a social media account can be just as invasive as demanding access to an email account, something we all already knows is off-limits.

Still, new legislation is a blunt tool, and it's not the right solution to every problem. In this situation, California's new laws create two problems, one big and the other bigger.

The Big Problem: "Social Media" Isn't Definable, So the Law Covers More Than Anyone Expects

Although the laws expressly say they are regulating "social media" like Facebook or Twitter, it's not possible to define "social media" as a subset of the Internet ecosystem. As evidence of this definitional challenge, look at the statutes' definition of "social media" (it's the same for both bills):

> "social media" means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations.

In other words, the law governs effectively all digital content and activity, both on the Internet and stored in local storage devices, not just social media. After all, what digital resource isn't "an electronic service or account, or electronic content"? The coverage of the law has focused only on its application to social media accounts, but the law's unexpectedly broad reach–including to locally-stored content–virtually ensures that the law will have unintended consequences.

The Bigger Problem: It's Often Not Clear When Social Media Accounts Are "Personal"

In addition to the breadth problem, AB 1844 (regarding employer/employee relationships) makes a serious conceptual error. The law restricts employers' access to "personal" social media, presumably in contradistinction to "business-related." Yet, the law doesn't define when a social media account is "personal," leaving all of us to speculate what that means.

Thus, the law assumes that social media accounts have only two states: personal or not-personal. Sadly, that's completely contrary to the cases I'm seeing in court right now. Instead, social media

accounts fit along a continuum where the endpoints are (1) completely personal, and (2) completely business-related–but many employees' social media accounts (narrowly construed, ignoring the statutory overbreadth problem) fit somewhere in between those two endpoints. Indeed, employers and employees routinely disagree about whether or not a social media account was personal or business-related. See, e.g., Insynq v. Mann, Eagle v. Sawabeh, Maremont v. SF Design Group, Kremer v. Tea Party Patriots, and PhoneDog v. Kravitz.

Meanwhile, employers can–and should–demand that employees provide them with the login credentials to business-related social media accounts. In fact, I've previously said "the cardinal rule about employee-operated social media accounts: get the login credentials BEFORE terminating the employee."

Putting the two concepts together, employers should require that employees provide them with login credentials for social media accounts relating to their business; but the law makes it illegal for employers to ask for login credentials to "personal" accounts. This puts employers in an obvious squeeze: employers may not know which employee accounts are purely personal and which are a mix of personal and business-related; the statute doesn't expressly allow employers to access mixed account; and the statute doesn't give employers a defense if they demand the login credentials because they reasonably but mistakenly thought the account was all or partially business-related. Courts will likely have to create common law exclusions for employers trying to get access to mixed accounts, but only after much angst, confusion and costly–and avoidable–litigation.

Note: SB 1349 uses the same "personal" terminology as AB 1844, but it's more likely to be clear when a student's accounts are personal than with employees.

Lessons

Question for you: are you surprised to see a state legislature enact an Internet-related bill with obvious problems? (Please, answer that question honestly). Speaking for myself, I always assume that a state legislature trying to "fix an Internet problem" will botch the job. After all, state legislatures have a virtually unbroken history of poorly designed Internet regulations.

For now, you can see why I'm not cheering California's new laws, even though I support their motivations. It's hard to get enthusiastic about a new law–especially when it relates to the Internet–that, on day 1, has manifest problems that could have been avoided with more considered policy-making. I also wish that the many other state legislatures considering similar legislation will learn from California's drafting mistakes; but realistically, state legislatures never learn from each other's mistakes, especially when legislators are overeager to "do something about privacy."

Did California Unintentionally (?) Impose New Statutory Duties on Every Blogger?
A Post on the Newly Enacted California Reader Privacy Act

By Eric Goldman

Technology & Marketing Law Blog, Oct. 21, 2011

California recently enacted the Reader Privacy Act, This new California law seeks to protect online book reader privacy to the same extent reader privacy is protected by libraries, by requiring heightened process before the government or private litigants can get certain types of information about book readers/buyers. As a restriction on government action, I support the concept enthusiastically. Indeed, I count many supporters of this bill as friends (well, maybe not after they read this post). At minimum, I know the effort was well-intentioned. However, I continue to believe this law was misarchitected for the reasons I expressed in my prior blog post on the proposed legislation.

My concerns from my prior post still apply, but this post will walk you through a specific reason why this law could be bad news for people who don't realize their conduct is now regulated. Let's look closely at who is required to comply with the law–recognizing that the statute has a private cause of action that will be enforced by a rapacious privacy plaintiffs' bar. The law's requirements applies to "any commercial entity offering a book service to the public." A "book service" means "a service that, as its primary purpose, provides the rental, purchase, borrowing, browsing, or viewing of books."

OK, clearly this covers Amazon and other online book retailers. But in this day and age, what is a "book" and, more importantly, what isn't? The statute defines a book as:

> paginated or similarly organized content in printed, audio, electronic, or other format, including fiction, nonfiction, academic, or other works of the type normally published in a volume or finite number of volumes, excluding serial publications such as a magazine or newspaper

So, let's play a game and try to spot some book services in the field. Is YouTube a book service? It definitely has "electronic" books, but maybe that's not its "primary" purpose. Scribd? It has lots of books too and plenty of other long-form "book-like" content. iTunes? It has lots of audiobooks. Wikipedia? It markets itself as an online encyclopedia, but maybe it isn't commercial enough? Hmmm….this is a tough game.

But what about blogs? Are they "book services"? Before you discount the latter, consider that many blogs are, in fact, paginated (at least in the URL–see Blog Law Blog as an example). Perhaps mere pagination alone isn't enough; maybe the pagination needs to be essential to the content's organization. Perhaps many bloggers aren't "commercial entities," although I'm sure plaintiff lawyers will argue that a blog with AdSense and some Amazon affiliate links would satisfy that standard. Or perhaps bloggers will be excluded as "serial publications," although the statute could have–and should have–made clear that blogs fit into that exception. In fact, cases like the old It's in the Cards v. Fuschetto suggest that courts might read the statutory exclusion narrowly on the theory that the legislature knew what blogs were but didn't mention them.

The ambiguity of blogs as "book services" means it's possible California has imposed a new statutory obligation on bloggers (at least those based in California, but who knows if it will be so limited), and this obligation effectively puts bloggers' houses on the line if they don't hire lawyers to properly navigate through the statute when the government or private litigants ask for information. Gee, thanks.

Indeed, this law could do more than just sweep in bloggers; it might cover *every* website because of the ambiguity of the term "book" and the concept of pagination. I don't know what "pagination" means in the online environment, but the concept may become more problematic in the near future. See News.com, "Opera proposal brings a book look to the Web." Thus, it seems like the law's attempt to carve out books from the universe of online content could fail, in which case large swaths of web operators become unexpectedly governed by the law–with a swarming privacy plaintiffs' bar as the reward for the uninformed.

I have long believed that states categorically should not try to regulate the Internet. A law like this, as laudatory as its goals are, helps confirm my beliefs.