BIOMETRIC PRIVACY LAWS

How a Little-Known Illinois Law Made Facebook Illegal

Jane Bambauer, Associate Professor of Law
James E. Rogers College of Law
University of Arizona

The future of data security may be in our irises and fingertips. Banks and retailers are increasingly interested in using biometric information to authenticate that a user is who they claim to be by converting a scan of the user's biological features into an elaborate password.

The benefits of biometric authentication are obvious: passwords can be very strong (in the sense of being long enough to withstand brute force attacks) without requiring the user to actually remember them. But the drawbacks are also obvious: since the systems use scans of irises, fingers, and even facial structures, a user's biometric passwords are on public display every time they leave the house.

Some states have passed biometric privacy laws to help facilitate the development of biometric authentication technologies. Illinois's law, which is a pioneer in the field, prohibits companies from collecting the measurements of any individual's biological features without the individual's consent. But these well-intentioned biometric privacy laws showcase the problems that arise when public policy tries to keep up with technology.

First, they are wildly overbroad, exposing online platforms like Facebook and Google, and even individual users of basic photo organization software, to civil liability based

on conduct that poses no risk to data security. Their scope contravenes good policy and, possibly, the First Amendment and the Dormant Commerce Clause.

Moreover, the laws are also unlikely to be necessary to accomplish their intended goals. Biometric authentication will require something more than an image or measurements of a person's face, iris, or fingerprints. They use systems that can ensure the person requesting access is physically present, rather than using measurements or photographs of somebody who isn't there. After all, hackers and other criminals will not be deterred by biometric privacy laws if they can simply use a photograph of a victim to impersonate them. Thus, the companies that are developing biometric authentication systems to protect sensitive personal data are already using technological solutions to manage the security risks, rendering the legal solutions obsolete.

Yet as the narrow data security purposes of biometric privacy laws have waned, courts and class action litigants are converting these laws into general prohibitions on unconsented data collection. The purpose of these nascent laws is laudable, but so far they have spurred technical noncompliance claims that are likely to harm, rather than help, the interests of the average consumer.

This paper explains how biometric privacy laws can and should be right-sized. Part I describes the current set of state statutes designed to protect biometric privacy. Part II explains the varied privacy goals that these laws can serve, and describes the policy pitfalls associated with each. Biometric privacy laws are likely to interfere with technologies that are helpful to consumers without doing a lot to prevent future harms. Part III describes the potential constitutional flaws in the design of biometric privacy laws, including conflicts with the First Amendment right to free speech and the Dormant Commerce Clause. Part IV suggests a path forward for both courts and legislators so that biometric privacy laws can be redesigned to serve their intended purposes.

PART I. WHAT ARE BIOMETRIC PRIVACY LAWS?

The archetype example of a biometric privacy law is the Illinois Biometric Information Privacy Act ("BIPA"). Illinois was the first state to pass a comprehensive biometric privacy law, and only one other state (Texas) has followed a similar course.[1]

---

[1] A few states have passed narrower biometric privacy statutes. California, North Carolina, Delaware, and West Virginia have placed legal constraints on schools and companies that collect biometric data from K-12 students. Missouri, Maine, and New Hampshire prohibit state agencies from using biometric data in connection with ID cards (although state and federal law enforcement agencies are not so constrained). See Ted Claypoole & Cameron Stoll, Developing

The Illinois BIPA first defines biometric identifiers and biometric information as follows.

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.[2]

A number of things are exempted from the definition of "biometric identifier," including photographs, writing samples, demographic data, and physical descriptions. But, as I explain below, courts that have interpreted these laws have consistently found that a photograph can be converted in to a "scan of … face geometry" if a piece of software uses the measurements and structure of a face to uniquely code or identify it.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.[3]

Any "private entity" that collects, captures, or obtains a person's biometric identifier or biometric information must first obtain the subject's consent through a "written release."[4] Moreover, the entity must provide notice about its purpose for collecting, storing, and using the information, and must post a publicly available retention and destruction schedule. And the entity may not sell the biometric data (though it can re-disclose the data with consent, as long as it doesn't "profit" from the disclosure).[5]

The law also creates a private right of action for any person whose rights under the statute were violated, and the statute provides $5,000 per violation in liquidated damages as well as the recovery of attorney's fees.[6]

Throughout, I will use the Illinois BIPA as the leading example for biometric privacy statutes because, as the first comprehensive law of its sort, it has now accumulated the largest collection of cases interpreting its scope and application.

Laws Address Flourishing Commercial Use of Biometric Information, ABA Business Law Today (May 2016), at https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

[2] 740 ILCS 14/10.

[3] *Id.*

[4] 740 ILCS 14/15(b)(3).

[5] 740 ILCS 14/15(a),(c)-(d).

[6] 740 ILCS 14/20(2)-(3).

PART II. WHAT DO BIOMETRIC PRIVACY LAWS INTEND TO ACCOMPLISH?

There are three ways to understand the purpose and design of the Illinois BIPA statute, and others like it.

A. Facilitating New Methods of Authentication

The first, most narrow, purpose that a biometric privacy statute can serve is to help cultivate and support a new system of authentication and data security. The logic is as follows: If banks and other critical services begin to use iris scans and fingerprints to ensure that a user is the person they claim to be, then these new forms of biometric passwords need to be protected from haphazard collection by other people and entities who may sell, spill, or misuse them.

". . . the plain text and the nascent case law interpreting the Illinois BIPA suggest that the law will have a much wider application than merely preserving the security of biometric passwords."

For example, in *Sekura v. L.A. Tan*, a plaintiff class sued a tanning salon franchise under the Illinois BIPA because the salon was using fingerprint scans as keys to track its customers' use of services rather than using RFID chips or key fobs that are commonly used in other spas.[7] The plaintiffs did not allege that L.A. Tan had actually shared or spilled the fingerprint data, nor had it used it in an inappropriate way. But by collecting the fingerprint scans without consent, and without publicly posting the required data retention policies, L.A. Tan violated the BIPA.

This case anticipates problems that could arise down the road if the L.A. Tan customers' fingerprint data can later be used to access their credit card and banking accounts. As the plaintiffs attorney explained,

> That type of information is incredibly sensitive. . . You can get a new social security card if it's stolen, but you can't go get a new fingerprint or a new face. This information was incredibly sensitive and it should be treated as such.[8]

---

[7] Gabe Friedman, First Settlement Reached Under Illinois Biometric Law, Bloomberg Law Big Law Business (December 5, 2016).

[8] *Id.*

If, in the future, fingerprint data is used the way social security numbers are used today, then it will not be great for consumers that a tanning salon has this particularly precious piece of personal information.[9]

This purpose—to facilitate future authentication technologies—is the primary goal of the Illinois statute. The first five (out of seven) clauses in the statute's legislative findings and intent center around the current and future development of biometric authentication processes.[10] For example, the legislature noted that "Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias" and "Despite[11] limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions."[12]

However, the plain text and the nascent case law interpreting the Illinois BIPA suggest that the law will have a much wider application than merely preserving the security of biometric passwords. Several cases have found that software that uses photographs of peoples' faces to differentiate between them, organize photos, and predict the identification of the subject must create biometric identifiers in the process, in the form of a scan of facial geometry. Thus, Facebook[13], Shutterfly[14], and Google[15] have all become ensnared in litigation under the Illinois BIPA even though a simple photograph of a person's face (and the "face scan" that can be created from it) would never be used as a biometric password.

If the facial structure of a still photograph were used as a password to access financial records and other sensitive accounts, imposters would be able to break into other accounts very easily. Recognizing this problem, companies that are considering using face scanning to authenticate a user are incorporating "liveness detection" that force a

---

[9] As I explain later, even this rationale for the BIPA exaggerates the risk, since technology is developing to distinguish between a live finger and an image or raw code.

[10] 740 ILCS 14/5(a)-(e).

[11] It is unclear whether the use of "Despite" is an error, as "Because of" seems a more appropriate opening clause.

[12] 740 ILCS 14/5(b),(e).

[13] In re Facebook Biometric Information Privacy Litigation, 185 F.Supp.3d 1155 (N.D. Cal. 2016).

[14] Norberg v. Shutterfly, Inc., 1:15-cv-05351 (N.D. Ill. 2015).

[15] Rivera v. Google Inc., , 2017 WL 748590 (N.D. Ill. 2017).

user to take a selfie with particular instructions (like winking)[16] or that can sense whether a fingerprint is coming from a live hand.[17] In fact, since millions of fingerprints have already been leaked by events like the U.S. Office of Management & Budget breach, companies are well aware that biometric security requires much more sophistication than the simple metrics of a face, iris, or finger. The broader point is that technological innovations will moot many of the security concerns that biometric privacy laws are meant to address.[18]

In any case, if the statute is intended to facilitate biometric authentication processes, the current laws sweep much too broadly, and are causing collateral damage to the development of photo organizing tools along the way.

B. Thwarting Facial Recognition Technology

The second plausible purpose for a biometric privacy statute like the Illinois BIPA is to preserve a certain level of obscurity so that our faces and bodies cannot be used to instantly identify us.

This purpose serves a much wider range of privacy interests beyond protecting the security of our bank accounts. It concerns not just impersonations, but also correct identifications of individuals who would otherwise remain anonymous. Under this conception, the Illinois BIPA is designed to interfere with the development and use of facial-recognition technologies so that a person will not be recognized by anyone other than his or her real life acquaintances.

A burgeoning literature describes the perils of facial recognition technologies. Some projects focus on the use of facial recognition technologies by law enforcement.[19] Others are critical of private uses of the technology, arguing that facial recognition encroaches on a zone of quasi-privacy (or obscurity) that we've grown to expect even

---

[16] Amazon filed a patent, published in March 2016, for a program that will allow users to authorize purchases by taking selfies while performing actions at the program's request, such as smiling or winking, to demonstrate the subject is the living user and not a photograph of him or her. See Claypoole & Stoll, supra note 1.

[17] For example, face recognition systems are being designed to distinguish a live face from a photo using "liveness detection" that requires the user to make a particular type of facial expression during the scan of their face. Other companies like Goodix use fingerprint scanners that sense whether they are being used by a human finger or not. Meg Graham, Illinois Biometrics Lawsuits May Define Rules for Facebook, Google, Chicago Tribune (January 17, 2017).

[18] Moreover, the problems were never as grave as the state legislatures and plaintiffs attorneys suggest. If a person's fingerprints are compromised due to a data breach, no reasonable company could continue to use the prints alone as a means of authenticating access to his or her accounts.

[19] Georgetown Law Center on Privacy & Technology, The Perpetual Line-up: Unregulated Police Face Recognition in America (October 18, 2016).

when we are out in the public street or our images are published on the public World Wide Web.[20] These critics are concerned about the chilling effects that may result if every photograph of a person online is linked to his name, or if he must carry his identity and reputation around for all to see every time he leaves the house. Most commentators believe these technologies violate the implicit bargain that was struck between exposure and privacy, and they resist any overly simple conception that "public is public." But these critiques of facial recognition technology ignore another important implicit bargain that has historically been struck by the public/private divide: a zone of uninhibited curiosity and information-gathering.

The privacy literature too quickly adopts a descriptive account as a prescriptive one. The descriptive account is undeniable; it was once very difficult to identify a stranger based only on their face or appearance while they were out in public unless you happened to know him. But the prescriptive account ("therefore we *should* be free from easy identification of our faces") is less convincing. It is an instantiation of status quo bias—an assumption that the amount of obscurity and exposure we have become accustomed to is just the right amount. It also assumes, wrongly in my view, that in the future we will be unable to harness the benefits of facial recognition technology while eliminating the most harmful uses through targeted laws.

Surely there are some contexts where the harms from identifying a previously unidentified person clearly outweigh the benefits. A narrow law prohibiting the use of facial recognition technologies near the entrance of doctor's offices or by online services offering sensitive and confidential advice would probably be good policy and may comfortably fit within the reasoning of existing First Amendement precedent.[21] And I have proposed laws that would criminalize the reidentification of research subjects whose sensitive data is included in anonymized research databases.[22] But prohibiting the identification of people as a default puts serious constraints on facial recognition without an understanding of its risks and benefits.

In the cases against Facebook, the Illinois BIPA has been called to service for the purpose of obstructing the development and use of facial recognition technology. Facebook argued that photographs and facial measurements that come from them are

---

[20] Joel R. Reidenberg, Privacy in Public, 69 U. Miami L. Rev. 141 (2014); Evan Selinger & Woodrow Hartzog, Opinion: It's Time for an About-Face on Facial Recognition, Christian Science Monitor (June 22, 2015).

[21] McCullen v. Coakley, 134 S.Ct. 2518 (2014); Hill v. Colorado, 530 U.S. 703 (2000) (upholding bans on expressive conduct near the entrance to abortion clinics).

[22] Jane Yakowitz (Bambauer), Tragedy of the Data Commons, 25 Harv. J. L. & Tech. 1 (2011).

exempted by the BIPA, but every court considering the argument has rejected it.[23] Even though photographs cannot be an appropriate basis for account security, the courts have consistently interpreted "face scans" to include measurements derived from photographs that can be used to uniquely code a person's face. Thus, the BIPA serves more than security goals. It also interferes with innocuous identification programs, even when (as is the case with Facebook) the service only labels a picture with a name after receiving the authorization of the photograph's poster.

To be clear, these systems mark a compromise between privacy and other social activities. Facebook allows a photograph's poster and other end users to upload and identify a portrait's subject even if the subject would prefer to not be identified. But this is not unusual. In fact, it is how the bargain is almost always struck between First Amendment speakers and subjects. Outside of special, confidential relationships, people are generally free to say whatever they want about others without their cooperation or consent.[24]

The Illinois BIPA departs from this standard compromise. Because the Illinois BIPA locates the legal right of control in the photograph's subject rather than the poster, Facebook's protocol is inadequate.[25]

In fact, the scope of the Illinois BIPA sweeps wider still. As the next subsection will show, the BIPA not only prohibits the unconsented identification of a face for any reason, it prohibits even the measurement of faces without subsequent reidentification.

---

[23] One court interpreted the exemption of photographs to apply only to "paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet." In re Facebook Biometric Information Privacy Litigation, 185 F.Supp.3d. at 1171. The better understanding from the totality of the cases is that uploaded digital photographs are also exempted, but once software creates measurements of faces that can be used to differentiate them, a face template has been created and the BIPA applies.

[24] Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Impilcations of a Right to Stop People From Speaking About You, 52 Stan. L. Rev. 1049 (2000); Jane Bambauer, The Relationships Between Speech and Conduct, 49 U.C. Davis L. Rev. 1941 (invited response to Jack Balkin); but see Jack Balkin, Information Fiduciaries and the First Amendment, 49 UC Davis L. Rev. 1183 (2016).

[25] The Federal Trade Commission's report on facial recognition similarly places control with the subject of the photograph and encourages companies to obtain consent anytime they intend to identify a person who might not be recognizable to the recipient of the information, although Facebook's practice of waiting for its users to decide to publish the identity of a subject (rather than automatically supplying it) may be consistent with the FTC's recommendations. The FTC recommends that companies obtain subject's express consent before collecting or using faceprints in two situations: (i) before using an image or faceprint in a materially different way than the company represented at the time of collection; and (ii) when using a faceprint to identify anonymous images of a subject to someone who could not otherwise identify the subject. Federal Trade Commission, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies 5 (2012).

C. Restrictions on Measuring and Sorting

Shutterfly and Google are defending against Illinois BIPA lawsuits based not on facial recognition, but on the creation of a facial map in the course of automatically organizing users' photographs. By measuring the facial features in a photograph to create unique (or near-unique) template for each individual's face, Shutterfly's and Google's programs create a "biometric identifier" requiring consent from the subject. The photo programs do not attempt to match unique maps to an actual identity, but this fact cannot save them. The definition of "biometric identifier" (unlike "biometric information") is not dependent on identifying the subject.

"The law is explicitly designed to stymie innovation and maintain a technological status quo."

This application of biometric privacy laws is technologically-dependent. We all create subconscious mental maps of our friends' and acquaintances' faces so that we can recognize them later. (In fact, people afflicted with face blindness are impaired in this precise way—they do not log these "biometric identifiers" and therefore lack the library needed to recognize people later.) Illinois law of course does not forbid a person from making a mental map of a person's face, so it applies only to technologically-aided facial scans.

It is clear that companies like Google, Shutterfly, and even Facebook (not to mention the individual consumers who willingly use software to organize and identify the subjects of photographs) will not be able to rely on consent to avoid liability. The subjects of the photographs do not necessarily have a relationship with the company developing the photo organization software. Indeed, the subjects don't necessarily have a relationship with the photographer.

The law is explicitly designed to stymie innovation and maintain a technological status quo. For example, the court hearing the claims against Facebook relied on one of the statute's stated purposes for limiting biometric data, which reads simply that "the full ramifications of biometric technology are not fully known."[26]

The fact of the matter is that if you use one of the many popular photo organizing programs that attempts to sort the faces in your photographs, and if you have ever taken a picture of somebody who currently lives in Illinois, there's a good chance that you've

[26] In re Facebook Biometric Information Privacy Litigation,185 F.Supp.3d at 1171. See also 740 ILCS 14/5(f) ("the full ramifications of biometric technology are not fully known.").

violated the Illinois law and could be liable for up to $5,000 per photo subject.[27] This is, in a word, absurd.

Biometric privacy laws like the Illinois BIPA are flawed in policy. They also pose serious conflicts with Constitutional law.

PART III. CONSTITUTIONAL INFIRMITIES

The biometric privacy statutes, as they are currently construed, raise significant issues under both the First Amendment and the so-called "dormant" Commerce Clause.

A. Biometric Privacy Laws Are Prohibitions on Speech

Shutterfly, Google, and Facebook all triggered legal liability the minute they "created" or "generated" a facial map.[28] By the law's own terms, the creation of this information is forbidden without the consent of a subject. Thus, the threshold question of whether the law infringes on speech is simple to answer: yes. As dull and dry as a facial map may be, the Supreme Court has long found that unadorned information like prescription drug data,[29] food ingredients,[30] and even price tags[31] are protected expression. Moreover, because the data derived from photographs are not used in connection with advertising or marketing, the

> *"Given the broad reach of the law . . . and given that the state was responding to the vague risk of 'unknown' technological intrusions, the Illinois BIPA and other similar biometric privacy statutes cannot withstand First Amendment scrutiny."*

---

[27] One Illinois court explained that the law "perhaps" will be interpreted "to not apply to the run-of-the-mill home-computer user who is not directly doing the collecting, capturing, purchasing, trading for, or obtaining of the protected identifier[.]" Rivera v. Google, 2017 WL at *8. But the court gave no strong assurance, and an argument can be made that the home computer user is the more direct collector or capturer when he downloads photos of friends into a program that sorts faces.

[28] For example, in the case against Google, the BIPA Act was triggered by creation of measurement data, not by the original collection of photographs. "Indeed, if Google simply captured and stored the photographs and did not measure and generate scans of face geometry, then there would be no violation of the Act." Rivera v. Google, 2017 WL at *7. Likewise, Facebook violated the Act because it failed to inform plaintiffs that the face geometry was "being generated." In re Facebook Biometric Information Privacy Litigation, 185 F.Supp.3d at 1159.

[29] Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011).

[30] Rubin v. Coors Brewing Co., 514 U.S. 476 (1995).

[31] Expressions Hair Design v. Schneiderman, __ U.S. __ (2017).

biometric privacy laws are a content-based discrimination on non-commercial speech. As such, the state must narrowly tailor the law to a compelling state interest in privacy or security.

Given the broad reach of the law described in Part II, and given that the state was responding to the vague risk of "unknown" technological intrusions, the Illinois BIPA and other similar biometric privacy statutes cannot withstand First Amendment scrutiny.

Narrower revisions of the statute that prohibit certain *uses* of biometric identifiers (i.e. for the purpose of identifying the subject or for the purpose of impersonating him or her) could avoid the constitutional problems if they narrowly target a particular, documented risk. In fact, use restrictions on biometric data may avoid First Amendment scrutiny altogether if the proscribed uses involve only conduct rather than the creation or communication of new knowledge. But as the laws are currently designed, they are needlessly strict prohibitions on the creation of speech.

B. Biometric Privacy Laws Regulate the Internet for Everyone

Biometric privacy laws overextend the authority of state legislatures. The courts interpreting the Illinois BIPA have insisted that the laws protect only Illinois residents, something that the state legislature is authorized to do. But the courts have not appreciated the full ramifications of their rulings.

For example, I am a resident of Arizona, but I have visited Chicago, and I have taken photographs of people who live there. These subjects make up a tiny fraction of the faces in my pictures, but nevertheless, if I upload a photograph to Facebook, Facebook risks violating Illinois law the instant it creates a face template. It will not matter if the subject in my Chicago photograph is a member of Facebook and has consented to have his face scanned because Facebook will not *know* whether the subject is a member of the Facebook community until after it has created the face template, the trigger for liability under the Illinois BIPA. As a precaution to avoid mapping Illinois residents who are not Facebook users, it may make sense to abstain from creating face templates altogether. If I upload photographs without metadata (as I sometimes do), Facebook won't even know whether I was in Illinois when I took the picture. Moreover, even if I took a picture here in Tucson, if one of the subjects in my photograph was visiting me from Chicago, Facebook's reliance on the photograph's geographic metadata will

suggest that the subject is not an Illinois resident when in fact she is.[32] *My* consent to allow Facebook to create a face template is insufficient; the rights belong to the subject. The only option, if Facebook intends to honor Illinois law, is to remove facial recognition for *everybody*. The same will be true for Shutterfly and Google.

Illinois's biometric privacy law therefore has an outsize effect, and implicates the Dormant Commerce Clause. The archetype Dormant Commerce Clause violation involves protectionist statutes that favor in-state businesses over out-of-state ones.[33] Illinois' BIPA law does not on its face involve this sort of protectionist discrimination, and nothing in the record suggests that the spirit of the law was to penalize California-based companies like Facebook and Google, either. However, the other flavor of Dormant Commerce Clause cases is very relevant here. In another set of cases, the Supreme Court has made clear that when a state law imposes significant burdens on interstate commerce, it will be unconstitutional if the burdens outweigh the local benefits.[34] If photo organizing software is made illegal everywhere to serve the abstract privacy interests of Illinois residents, the scales are likely to tip toward a constitutional violation.

PART IV. WHAT NOW?

Existing biometric privacy laws need an overhaul. An earlier attempt to revise the Illinois law did not pass,[35] but as the wide application of the law becomes easier to appreciate, the legislature may become focused on revising the statute to exempt data produced from ordinary photographs or to more narrowly address security risks.

Some federal courts have already begun to pare back the reach of the Illinois BIPA. Citing the recent *Spokeo* decision, these cases have involved complaints surrounding failure to adhere to BIPA-required disclosures where there were no allegations that the

---

[32] One court claimed that the Illinois BIPA should not be interpreted to have "extraterritoriality." However, the factors used to assess proper Illinois jurisdiction include "the residency of the plaintiff, the location of harm, communications between parties (where sent and where received), and where a company policy is carried out." In the case against Google, as would be the case in a case against Facebook for a photograph that I uploaded in Arizona, the residency of the plaintiff (and the fact that the harm was felt by the plaintiff there) was sufficient to overcome a motion to dismiss. Rivera v. Google, 2017 WL at *9. The court also noted that in the case against Google, the photographs had been uploaded using a Droid device in Illinois (Id. at *1), but it is not clear which of the four factors this fact supports.

[33] Gibbons v. Ogden, 22 U.S. 1 (1824).

[34] Pike v. Bruce Church, Inc., 397 U.S. 137 (1970).

[35] Amendment to House Bill 6074, available at http://www.ilga.gov/legislation/99/HB/09900HB6074sam001.htm.

plaintiffs suffered any harm related to BIPA's core protections for the collection or sharing of data.[36] Although this approach may arrive at the right result in some cases, the standing doctrine will not be a cure-all salve. If Illinois intends to give all of its residents a property-style exclusive interest in the measurements of their face and fingers, then failure to provide BIPA-required notices will impair a person's legal interest in the control over their biometric information.[37] The real problem with the law goes to the heart of the policy that Illinois is attempting to create—exclusive control over information that should be a collective good.

Companies and individuals who are defending themselves in litigation can certainly make use of the cases disposed on standing grounds, but they should also make a wider range of arguments, including the First Amendment defense described above. If companies do not make these arguments themselves (perhaps out of fear of seeming insensitive to privacy concerns or of exploiting First Amendment rights), amici can make them.

Finally, and more generally, the problems with the Illinois BIPA are a byproduct of an effort to regulate ahead of technological development. The impulse to do so is entirely understandable; too often, legislatures are criticized for failing to keep up with technology. But when law is developed too early, the cure can be worse than the disease.

---

[36] Vigil v. Take-Two Interactive Software, 15-cv-8211 (S.D.N.Y. 2017); McCollough v. Smarte Carte, Inc., Case No. 16 C 03777 (N.D. Il. 2017) (citing Spokeo Inc. v. Robins, 136 S. Ct. 1540 (2016)).

[37] Just as an intentional trespass onto land or an intentional copy of a copyrighted work of art is a violation of an owner's rights even if no damages directly result, if a technical violation impacts a person's privacy rights, it should also confer standing. Also, the standing doctrine is limited to the federal judiciary. Even if federal courts lack jurisdiction to resolve Illinois BIPA cases, state courts are not bound to follow the Spokeo decision.