Facebook and the Biometric Information Privacy Act Litigation

Lesley Rice Montgomery, MLIS
Catalog Librarian II, Tulane University

Abstract

This article will discuss a class action lawsuit that initially was filed in 2015 against – and ultimately was settled by – the social media giant Facebook, Inc. (hereinafter referred to as Facebook), alleging that Facebook had collected and stored Illinois users' biometric data without prior notice or consent, with the action basing the plaintiffs' claims on statutory information found within the Illinois Biometric Information Privacy Act (BIPA) (Gilardi, 2025; IGA, n.d.). "Biometrics" is defined as "the automated recognition of individuals based on their biological and behavioral characteristics from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition" (DHS, 2025). Fingerprints, iris patterns, or facial features can be used for automated recognition, and Facebook's automated facial recognition templates that were created using these features are considered to be biometric data under BIPA (Guariglia, 2021). Discussions first will focus on definitions of facial recognition technologies; on the scope of biometrics collection and use with regard to existing library privacy policies and ALA stances on privacy; and on Facebook's litigation with the Illinois class action plaintiffs *In re Facebook Biometric Information Privacy Litigation Case* No. 3:15 CV 03747 JD, Dkt. No. 537 (N.D. Cal. Feb. 26, 2021) (Feinstein, Nelson & Martens, 2021). The class action privacy case was settled on February 26, 2021, in California federal court. Facebook was ordered to pay $650 million for running afoul of the Illinois BIPA law that was designed to protect Illinois residents from invasive privacy practices. This legal audit will introduce the Illinois BIPA as it relates to the Facebook lawsuits; will discuss how Facebook's development of a face template using facial recognition technology without consent led to plaintiffs' claims of an invasion of social media users' private affairs and concrete interests; and will briefly discuss how the court actions' movements from local Illinois courts to the U.S. District Court for the District of Northern California with consolidation and attainment of class action status allowed both Facebook users and nonusers to seek compensation for privacy violations. The article's conclusion will reemphasize how important it is for academic library staff and other information specialists to become acquainted with legal matters of online privacy, like those raised in the Facebook litigation, as these issues might very well impact the searching habits, online intellectual pursuits or autonomy of patrons who are engaged with libraries' social media or other applications.

Keywords*:* automatic facial recognition tagging features; biometric data; online privacy; social media

Article Type: Research Paper

Endnotes: The Journal of the New Members Round Table
Volume 13, Issue 1, 2025
pp. 71-82
Published by the American Library Association
© Retained by the Authors
ISSN: 2159-0591

Introduction

The timelines of Facebook’s acquisitions of Instagram and WhatsApp and of the implementation and later shutdown of Facebook’s facial recognition automatic tagging feature followed an interesting path, and a brief summary of events might lead the reader to a greater understanding of when and why social media users filed numerous lawsuits that addressed issues of user privacy (“History of Facebook,” 2025). Facebook first introduced its facial recognition tagging application in December 2010. This feature automatically identified people individually or in a group setting from uploaded photographs and suggested tags to other users. Problems arose when Facebook users realized they were being tagged without their permission by *other* Facebook users. Initial complaints were filed by the Irish Data Protection Commission (IDPC) in 2012, the same year that Facebook acquired Instagram. Complaints by the IDPC led to Facebook suspending the facial recognition feature in Europe. Interestingly, Facebook reinstated facial recognition in Europe in 2018, but added a user-opt-in mechanism to comply with the General Data Protection Regulation (GDPR). GDPR is a European Union law that regulates how personal data is collected, processed and stored (Wolford, 2025). In the meantime, Facebook acquired WhatsApp in February 2014, and by 2015 the Illinois users’ class action lawsuit was underway, due to allegations that Facebook had collected and stored Illinois users’ biometric data without their prior notice or consent. The subsequent lawsuits led to the discontinuation of this feature in November 2021, when Facebook opted to delete facial recognition templates of more than a billion users (Pesenti, 2021). As a footnote, in 2023 Facebook – now under the control of Meta as of October 28, 2021 – announced via its CEO Mark Zuckerberg, that Meta would start selling verification badges on Instagram and Facebook (Cowley, 2023). These blue “verified” badges assure social media users that they are following a legitimate person. For example, many celebrities now use these badges on their personal social media sites, due to the proliferation of online imposters.

Facebook and the Biometric Information Privacy Act: A Broad Overview of Facial Recognition Technologies and BIPA Litigation

Facial Recognition Technologies

The Illinois Biometric Information Privacy Act (BIPA) was passed on October 3, 2008, with the intent to regulate the collection, storage, use and handling of biometric identifying information by private entities (IGA, n.d.; Kozak, 2021). “Biometrics” is an automated recognition and verification of people, either by themselves or in a group setting, that is based on their biological or behavioral characteristics from which biometric features can be located, identified, analyzed, extracted, compared to stored data of other individual’s faces, and later used in various ways (DHS, 2025). Biometric facial recognition identifies or verifies individuals by capturing a template of their face – a digital “faceprint” – and compares it to a database of already known faces. A “face template” or “faceprint” is data that corresponds to an image of someone’s face that is unique to their face and is used in a facial recognition system (Guariglia, 2021).

Considered to be a secure alternative to PINs or passwords, this technology is used widely today in a variety of applications, including unlocking smartphones and controlling access to buildings, such as corporate offices, airports or government installations. For example, the U.S. Department of Homeland Security uses biometrics to enforce federal laws, to facilitate legitimate travel and trade, and to enable verification for visa applications to the U.S. (DHS, 2025). The Illinois BIPA litigation that pushed for regulation of this type of identifying information has implications for libraries, ethics of library policies and use, and patron privacy, especially with regard to facial recognition technology, whereby users can unknowingly and without providing any consent be identified on social media platforms they might be using at the library, such as Facebook

(IEEE, 2025). Given the current climate in all types of libraries across the nation where patron privacy is endangered, as well as the increasing presence of law enforcement that is compromising the safety of faculty and students who might be visiting the country on education visas, it is of paramount importance to understand the application of these visual identification techniques (IFLA, 2025).

The technology is quite sophisticated. Facebook previously utilized facial recognition to identify faces – either individually or in groups – that had been uploaded to the platform. The system scanned photos and videos; identified arrangements of features such as eyes, noses and mouths as well as skin tone; extracted unique features like the distance between eyes or the shape of the nose and mouth; and ultimately used a complex algorithm to create a numerical duplicate of each face known as a "faceprint" that was compared to a database of tagged users. Facebook's facial recognition system was extremely accurate at identifying faces. It is important to note that user privacy potentially was compromised whenever the system suggested to other Facebook users that they could tag the person who was both unaware of and had not given consent to the fact they had been identified by this facial recognition technology (Guariglia, 2021). So, while Facebook's facial recognition data collection and surveillance is not used by libraries per se, the availability and use of this information on social media platforms and other applications does raise privacy concerns and ethical considerations because of the potential for misuse (IEEE, 2025).

Facebook's facial recognition relates to library patron privacy in numerous ways, including the erosion of anonymity and autonomy, whereby patrons might be discouraged from or even afraid of exploring library resources, feeling they are being watched or judged. This chilling effect can prevent patrons from freely pursuing their intellectual activities and can hamper free expression and association (IEEE, 2025). Although Facebook's system is not used in libraries, the widespread use of these technologies can lead to breaches of facial recognition databases, leaving individuals working on library computers potentially vulnerable to data collection by outside entities (IFLA, 2025). Indeed, ethical considerations vis-à-vis facial recognition are far reaching, from privacy concerns to questions of data security and consent (IEEE, 2025; IFLA, 2025).

The potential impacts on libraries and on patron privacy, autonomy and use of resources are based in part on the erosion of key principles of entities such as the American Library Association and the International Federation of Library Associations and Institutions. Library users have a right to anonymity and library staff have a mandate not to disclose the identity of users or the materials they use to third parties, and these key tenets are relevant today due to increasingly pervasive online surveillance (ALA, 2025; IFLA, 2025). In fact, the American Library Association published a resolution opposing the use of facial recognition technologies in libraries stating, "The use of facial recognition technology is inherently inconsistent with the *Library Bill of Rights* and other ALA policies that advocate for user privacy, oppose user surveillance, and promote anti-racism, equity, diversity, and inclusion" (ALA, 2025). This resolution arose out of a survey distributed in 2020 by the Intellectual Freedom Committee's Facial Recognition Working Group to ascertain the library community's overall level of knowledge and concern about facial recognition software (ALA, 2025). The working group created the detailed resolution using information received from 628 respondents and additional clauses were adopted by ALA's Council on January 26, 2021, subsequent to endorsement by the Committee on Library Advocacy Intellectual Freedom Round Table (ALA, 2025). It should be emphasized that the *Library Bill of Rights'* policies firmly support user privacy and confidentiality, which "…is necessary for intellectual freedom and fundamental to the ethics and practices of librarianship" (ALA, 2025). Interpretations of the *Library Bill of Rights* maintain that this includes advocacy for and education about the issue of library users' right to be protected from surveillance of their lawful library use (ALA, 2025; IFLA, 2025). Additional clauses state in part, that "use of facial recognition systems is invasive and outweighs any benefit for library use" and ALA "opposes the use of facial recognition software in libraries of all types on the grounds that its implementation breaches users' and library workers' privacy and user confidentiality, thereby having a chilling effect on the use of library resources" (ALA, 2025). While it is beyond the scope of this article to delineate the entire resolution, it should be noted that the American Library Association provides a thorough literature review reference list and a detailed analysis of the resolution on their facial recognition resolution site (ALA, 2025).

BIPA Litigation

Regarding the BIPA litigation, Illinois is not the only state that has recognized and addressed the issue of user privacy on social media platforms. Several other U.S. states besides Illinois have biometric privacy laws, including Texas, Washington, California, New York and Arkansas, but aside from Texas and Washington State, Illinois is the only other state that enforces biometric protection and its BIPA regulations are the most stringent (BIPA, 2024; Channick, 2021; Kozak, 2021). The Act requires companies to obtain users' permission prior to utilizing facial recognition technologies to identify platform users (Channick, 2021). Private entities must formulate "a written policy, schedule, and guidelines about collection, retention, and destruction" of biometric identifier data; must provide disclosures and obtain written releases prior to collecting the data; must restrict biometric information dissemination; and must provide for private rights of action (Kozak, 2021). Typically, BIPA claims provide "…private right[s] of action to recover potentially astronomical damages for inadvertent use or disclosure of biometric data like fingerprints, face scans, or voiceprints by businesses" (KDW, 2021). In *re Facebook Biometric Information Privacy Litigation* class members alleged that Facebook had collected, stored and subsequently used digital facial scans "…without prior notice or consent in violation of Sections 15(a) and 15(b) of the Illinois Biometric Information Privacy Act… 740 Ill. Comp. Stat. 14/1 et seq. (2008)" (Feinstein, Nelson & Martens, 2021). Specifically, the complaint alleged that "Facebook violates the statute by virtue of its facial recognition software that collects and stores biometric information, in the form of face templates extracted from photographs uploaded to the website, in connection with its 'Tag Suggestions' feature without first obtaining informed written consent" (LS, 2021).

The class members who are eligible to benefit from the settlement are defined as residents of the State of Illinois who lived in the state for at least six months who are also "Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011" (Gilardi, 2025). The case initially was filed in 2015 in Cook County Circuit Court, Illinois; subsequently was moved to Chicago federal court; and finally was litigated in California federal court, at which time it attained the class action status (Channick, 2021). On February 26, 2021, Judge James Donato granted final approval of the proposed class action settlement, with the U.S. District Court for the Northern District of California entering a final judgment on this biometric privacy class action lawsuit brought against Facebook on April 12, 2021 (Feinstein, Nelson & Martens, 2021; Gilardi, 2025). Facebook was ordered to pay $650 million for running afoul of the Illinois BIPA law that was "designed to protect the state's residents from invasive privacy practices" when "Facebook's practice of tagging people in photos using facial recognition without their consent violated state law" (Hatmaker, 2021). The Court approved payments in the amount of $345 for each of the 1.6 million class members who are Illinois residents (Channick, 2021; Osborne, 2021). The U.S. District Judge Donato called this settlement, "…one of the largest privacy settlements ever and a 'major win for consumers in the hotly contested area of digital privacy' with more than one in five eligible Illinois Facebook users" participating in the settlement (Channick, 2021; Osborne, 2021).

The settlement was indeed record-breaking in amount, yet it was "still significantly below the statutory damages of $1,000 and $5,000 provided by BIPA" (Perdew & Trifon, 2020). This lesser settlement, which was largely a result of the court-awarded attorneys' fees of $97.5 million, led to a couple of class members filing an appeal with the Ninth Circuit Court of Appeals. That meant payments could not be made to other class members. The objections by class members Dawn Frankfother and Cathy Flanagan concerning whether the settlement amount was large enough resulted in a delay (Channick, 2021; Gilardi, 2025). The appeals court initially scheduled oral arguments for February 17, 2022. As one might imagine, other class members were not happy about this situation and asked Class Counsel to expedite the docket schedule, but Counsel said, "Frankfother and Flanagan have refused to expedite the appeal and the Ninth Circuit rejected Class Counsel's request to do so" (Gilardi, 2025). Ultimately, on March 17, 2022, the United States Court of Appeals, Ninth Circuit stated in part that it held, "the $5,000 incentive awards to Named Plaintiffs were not an abuse of discretion [when paying the attorneys' fees]" (Casetext, 2022).

Facebook's Facial Recognition Software: How its use led to BIPA Violations and Continuing Infractions of Personal Privacy

In the matter of *Facebook Biometric Information Privacy Litigation*, Facebook denied that it had violated any law when the plaintiffs brought their claim against the platform. Class action litigants stated that Facebook's "Tag Suggestions" feature, among other features, used facial recognition technology (Gilardi, 2025). Plaintiffs alleged that Facebook's facial recognition technology not only violated Illinois' Biometric Information Privacy Act, but also that they had been subjected to "…a concrete and particularized harm… because BIPA protected the plaintiffs' concrete privacy interest, and violations of the procedures in BIPA actually harmed or posed a material risk of harm to those privacy interests. Specifically… the development of a face template using facial recognition technology without consent (as alleged in this case) invades an individual's private affairs and concrete interests" (EPIC, 2021).

It should be noted that as a result of yearlong FTC investigations and subsequent court actions, in 2019 Facebook disabled its automatic facial recognition tagging features by making this an optional application; promised users that they can control their personal information through Facebook's privacy settings; and thereby addressed some of the privacy issues that Illinois plaintiffs initially raised in their class action suit (FTC, 2019; Hatmaker, 2021). However, in August 2020, yet another class action lawsuit was filed in a San Mateo, California state court by a user of Instagram – a platform also owned by Facebook. New allegations stated that via Instagram, Facebook was "…actively collecting, storing, disclosing, profiting from, and otherwise using biometric information of… more than 100 million users without any written notice or informed written consent, including millions of Illinois residents" (TFL, 2020). These allegations were particularly concerning, because the FTC's 2019 order-mandated privacy program, which covered Facebook's WhatsApp and Instagram, required Facebook "to conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy" (FTC, 2019). While this San Mateo court filing will not be discussed in this case study, the Instagram users' allegations shed some light on how and why the social media giant used the biometric gathering features. For example, whenever users upload images to Instagram or Facebook, the biometrics are used to "…bolster its facial recognition abilities across all of its products, including the Facebook application, and shares this information among various entities," including Facebook's IT teams as well as third parties, such as "…other apps, websites, and third-party integrations, [and] Facebook's partners, including vendors and service providers" (TFL, 2020). This is a possible indication that financial benefits of facial recognition technologies trumped the costs of potential litigations. In fact, the Instagram litigant asserted that profits obtained from the use of protected biometrics helped the company “…to expand the datasets which enable its facial recognition software, and to cement its market-leading position in facial recognition and social media” (TFL, 2020). It should be noted that while Facebook stopped using facial recognition technologies on its platform in November 2021, Meta, Facebook’s parent company, is still researching biometrics and can incorporate face signatures and track facial or users’ eye movements in virtual reality headsets, as an example (Heilweil, 2021). Virtual reality technology is relatively new, and there are no specific regulations regarding the collection, storage and use of biometric data from VR headsets (Bloomberg, 2025). Also, in July 2024, the Texas Attorney General secured a $1.4 billion settlement with Meta. The 2022 lawsuit filed in state court alleged that Meta had been collecting and using biometric data from photographs that had been uploaded to Facebook without Texans’ consent (Paxton, 2024). Proposals are ongoing at both local and federal levels to regulate how facial recognition is used by private companies.

The Issue of Complaints Filed on Behalf of Both Users and Nonusers of Facebook

After researching Facebook’s infractions of the 2008 Illinois Biometric Information Privacy Act, it is clear why some users filed lawsuits against the social media platform for its collection, use and handling of biometric identifiers and users’ personal information without prior notice or consent. What is not readily apparent is why both class members and *nonusers* of Facebook would merit damage reparations. In part, this has to do with court jurisdiction, but the overriding factor is whenever Facebook’s actions lead to privacy violations, misuse of personal data, or whenever harm is caused by Facebook’s algorithms and business practices, then both users and nonusers potentially can be granted damage reparations (TGC, 2025). Also, types of damages can vary, depending on each case’s circumstances. For example, Facebook nonusers can seek compensation for privacy violations via class action lawsuits (LS, 2021).

In re Facebook Biometric Information Privacy Litigation included people who were not direct users of the platform. In the instance of the Illinois BIPA litigation, nonusers had grounds for receiving reparations when Facebook collected, stored or used their biometric data without their knowledge or consent. Initially filed in 2015 in Cook County Circuit Court, Illinois, the case subsequently was moved to Chicago federal court, and finally was litigated in California federal court, at which time it attained the class action status (Channick, 2021). The *In re Facebook* settlement was reached by three law firms that represented the plaintiff class. A Chicago law firm, Edelson PC, filed the first suit against Facebook for its alleged Illinois Biometrics law violations. Labaton Sucharow LLP is known for prosecuting precedent-setting class and direct actions and is the law firm that filed a class action complaint on April 21, 2015, on behalf of Illinois Facebook users and nonusers who were negatively impacted by alleged violations of the Illinois BIPA by Facebook (LS, 2021). Robbins Geller Rudman & Dowd LLP also filed against Facebook; the cases were consolidated and transferred to the U.S. District Court in San Francisco; and thereafter the three firms jointly litigated *in re Facebook* before Judge James Donato, the Ninth Circuit Court of Appeals, and the U.S. Supreme Court which declined to hear the case (Channick, 2021; LS, 2021).

The *In re Facebook* cash settlement was the largest ever for resolving a privacy-related lawsuit. However, because the settlement was on behalf of a class of consumers, it was “subject to and not effective until [it was] approved by the District Court presiding over the case” (Channick, 2021; LS, 2021). On February 26, 2021, Labaton Sucharow did obtain final approval of the $650 million settlement *In re Facebook* after five years of litigation before the Honorable Judge James Donato, the Ninth

Circuit Court of Appeals, and the U.S. Supreme Court (LS, 2021).

Final Considerations: Ramifications of In re Facebook on Social Media Use in Libraries

Since modern libraries and other information entities provide news and events, information services and resources digitally, it is of paramount importance that library staff and other information technology specialists are fully cognizant of legal issues that might impact the privacy of online users (Sumadevi & Kumbar, 2019). Unraveling some of the knotty issues raised during various litigations pertaining to *In re Facebook* would prove useful for professional library staff and other information specialists as they attempt to follow best practices when assisting online patrons. Additionally, modern libraries occasionally have "sign up for social media" classes that specifically encourage patrons to use social media. Many libraries also have an institutionally based social media presence and often will encourage patrons to "follow" the libraries. Given that patrons primarily interact with these platforms by posting photographic images and/or videos of themselves, an investigation of the legal responsibilities of libraries vis-à-vis First Amendment considerations, third-party responsibility, data collection, and user privacy, would provide much beneficial advice for librarians and other information technology professionals who need to be familiar with these issues when working online, when providing reference services, or when otherwise aiding their library users in the online environment.

Invasive privacy practices threaten online patrons who use social media platforms. This is an unfortunate modern day truism, borne out by the simple fact that Facebook is not the only online entity that regularly compromises online users' private affairs and anonymity. In 2020, numerous lawsuits were filed that accused Microsoft, Google and Amazon of breaking BIPA mandates after Illinois residents' faces were used by these entities' software programs to train the companies' facial recognition systems without having first obtained explicit consent (Hatmaker, 2021). Also in 2020, Baer Law LLC filed the first BIPA class action lawsuit in the United States against TikTok for allegedly collecting facial data from users without their consent, which was preliminarily approved for a proposed $92 million settlement on behalf of TikTok users in twenty-one class action cases (Baer Law LLC, 2021). Indeed, the list of lawsuits is ongoing to this day, with a wide variety of companies being brought to court for violating individuals' privacy and control over personal identifiers. That being said, while library staff already adhere to the *Library Bill of Rights* and other ALA policies and principles, they need to be mindful of any legal obligations to protect their patrons' privacy. For example, libraries are considered to be a public space with no clear expectation of privacy, so can libraries that use Facebook and other social media be held legally liable for utilizing tagging biometrics?

First and foremost, the American Library Association's *Library Bill of Rights* is considered the primary source of protection for library users' privacy, confidentiality and intellectual freedom. Libraries are protected from liability pertaining to third-party content and social media postings by the Communications Decency Act (CDA), §230 (Zeigler, 2024). However, with the consultation of legal counsel, they must ensure that their own policies and practices are succinct and updated, outline the collection and use of patron data, and comply with privacy laws (ALA, 2019). Libraries must comply with federal and state laws that apply to the collection, record-retention, use and sharing of personally identifiable information, such as when law enforcement officers request information with a proper court order (ALA, 2019; IFLA, 2015). Library staff are advised to encourage users to be aware of their privacy when they are posting online, yet libraries cannot restrict First Amendment speech on private social media platforms as per the CDA, §230 (Zeigler, 2024). Limiting freedom of speech also can potentially compromise civil engagement and democracy (IFLA, 2015). Library data collection and use on social media including the creation of user profiles should align with their organization's privacy policies. Regarding best practices, libraries should refrain from storing personal data, such as information written on patron sign-in sheets, and should only collect data that is absolutely necessary to provide library services. For example, it is not a good idea to file sign-in sheets with personal information on an unprotected shelf or under a reference desk or digitize the sheets and upload them to a shared computer. Large scale data collection can have a chilling effect on users, who might self-censor their search behaviors or intellectual pursuits, so user information should be protected digitally and physically (IFLA, 2015).

Conclusion

The Illinois Biometric Information Privacy Act is one facet of a regulatory system that is increasingly threatening the way tech companies have done business for a couple of decades. Regulatory agencies at the federal and state levels are attempting to rein in tech giants and the landmark Illinois law presents a compelling framework to mitigate some of the more blatant infringements on users' privacy by social media platforms like Facebook (Hatmaker, 2021). Modern librarians, library staff and other information entities heavily rely on the American Library Association's *Library Bill of Rights* for guidance when implementing organizational best practices. Due to a lack of federal oversight vis-à-vis patron privacy and because libraries increasingly use social media to provide useful and timely information about resources, services, news and events, and even to promote library branding, it is of paramount importance that library staff and other information technology specialists are fully cognizant of issues that might impact the privacy of online users (Sumadevi & Kumbar, 2019; Xie & Stevenson, 2014). An important caveat to the increased use of social media by patrons and branding of libraries via visually based online platforms is that libraries should approach social media sites and other applications cautiously, taking into account previous egregious breaches of patron privacy and autonomy. Library administrators must acknowledge the definition of biometrics that the Illinois General Assembly noted in legislative documentation when creating the Illinois BIPA: "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions" (IGA, n.d.). It is a simple fact that posts containing an image or images tend to attract more users (Joo, Choi, & Baek, 2018). Users who are increasingly engaging with libraries' social media sites and other applications need to have their privacy protected against facial recognition technologies that are being misused by tech companies, and this is even more critical when the patrons are posting their facial images online or using "tag suggestion" features or other biometric identifier applications. These crucial protections are delineated in the *Library Bill of Rights* which firmly asserts, "All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information (ALA, 2025)." These key tenets along with the American Library Association's resolution opposing the use of facial recognition technologies in libraries will guide librarians and library staff as they continue to advocate for user privacy, to oppose user surveillance, and to promote anti-racism, equity, diversity, and inclusion within their institutions.

References

American Library Association (ALA). (2019). Guidelines for library policies. *American Library Association.* https://www.ala.org/advocacy/intfreedom/librarypolicyguidelines

American Library Association (ALA). (2025). Resolution in opposition to facial recognition software in libraries. *American Library Association.* https://www.ala.org/advocacy/intfreedom/facialrecognitionresolution

Baer Law LLC. (2021, March 10). Baer Law LLC initiated the first Biometric Information Privacy Act (BIPA) class action lawsuit in US against TikTok [Article]. *Baer Law Newsletter.* https://www.baerlawllc.com/blog/class-action-lawsuit-against-tiktok

Biometric Information Privacy Act (BIPA). (2024, September 27). In *Wikipedia*. https://en.wikipedia.org/wiki/Biometric_Information_Privacy_Act

Bloomberg. (2025). VR headsets give enough data for AI to accurately guess ethnicity, income and more. *Bloomberg Technology.* https://www.bloomberg.com/news/articles/2023-08-10/meta-s-virtual-reality-headset-quest-2-has-privacy-concerns

Casetext. (2022, March 17). Patel v. Frankfother (*In re Facebook Biometric Information Privacy Litigation*), 2022 WL 822923 (9th Cir. 2022). https://casetext.com/case/patel-v-frankfother-in-re-facebook-biometric-info-privacy-litig/

Channick, R. (2021, April 6). Waiting for your $345 from the Illinois Facebook privacy settlement? Here's why it's delayed. *The Pantagraph.* https://pantagraph.com/news/state-and-regional/crime-and-courts/waiting-for-your-345-from-the-illinois-facebook-privacy-settlement-here-s-why-it-s/article_32e7a39b-5d1b-5b85-931b-1ffd1dee175f.html

Cowley, S. (2023, February 19). Facebook parent plans to sell 'Meta verified' accounts. *The New York Times.* https://www.nytimes.com/2023/02/19/business/meta-facebook-instagram-verified-accounts.html

Department of Homeland Security (DHS). (2025). *Biometrics.* U.S. Department of Homeland Security. https://www.dhs.gov/biometrics

Electronic Privacy Information Center (EPIC). (2021). *Patel v. Facebook: U.S. Court of Appeals for the Ninth Circuit.* https://epic.org/documents/patel-v-facebook/

Federal Trade Commission (FTC). (2019, July 24). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. *FTC Newsletter.* https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

Feinstein, A., Nelson, P., & Martens, K. (2021, March 22). Judge allows Facebook to settle facial scanning suit for $650 million. *JD Supra.* https://www.jdsupra.com/legalnews/judge-allows-facebook-to-settle-facial-6231285/

Gilardi & Co. LLC (Gilardi). (2025). *Facebook biometric information privacy litigation.* https://www.facebookbipaclassaction.com/

Guariglia, M. (2021, November 2). Face recognition is so toxic, Facebook is dumping it. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2021/11/face-recognition-so-toxic-facebook-dumping-it?language=en

Hatmaker, T. (2021, March 1). Facebook will pay $650 million to settle class action suit centered on Illinois privacy law. *TechCrunch.* https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/

Heilweil, R. (2021, November 3). Facebook is backing away from facial recognition. Meta isn't. *Vox.* https://www.vox.com/recode/22761598/facebook-facial-recognition-meta

History of Facebook. (2025, May 17). In *Wikipedia.* https://en.wikipedia.org/wiki/History_of_Facebook

Illinois General Assembly (IGA). (n.d.). Civil liabilities (740 ILCS 14/) *Biometric Information Privacy Act.* https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Institute of Electrical and Electronics Engineers (IEEE). (2025). Ethical considerations in the use of facial recognition for public safety. *Public Safety Technology.* https://publicsafety.ieee.org/topics/ethical-considerations-in-the-use-of-facial-recognition-for-public-safety/

International Federation of Library Associations and Institutions (IFLA). (2015, August 15). IFLA statement on privacy in the library environment. *International Federation of Library Associations and Institutions.* https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment/

International Federation of Library Associations and Institutions (IFLA). (2025). Facial recognition, libraries, and intellectual freedom. *International Federation of Library Associations and Institutions.* https://blogs.ifla.org/faife/2019/08/19/facial-recognition-libraries-and-intellectual-freedom/

Joo, S., Choi, N., & Baek, T. H. (2018, September 13). Library marketing via social media: The relationships between Facebook content and user engagement in public libraries. *Online Information Review*, 42(6), 940-955. https://www.emerald.com/insight/content/doi/10.1108/OIR-10-2017-0288/full/pdf?title=library-marketing-via-social-media-the-relationships-between-facebook-content-and-user-engagement-in-public-libraries

Kelley Drye & Warren LLP (KDW). (2021, May 18). Court to decide if insurance covers biometric data claims in BIPA dispute. *JD Supra.* https://www.jdsupra.com/legalnews/court-to-decide-if-insurance-covers-4436095/

Kozak, N. I. (2021). *Global internet jurisdiction* [Lecture recording]. Canvas.

Kozak, N. I. (2021). *Internet-related privacy* [Lecture recording]. Canvas.

Labaton Sucharow (LS). (2021, February 26). *In re Facebook Biometric Information Privacy Litigation.* https://www.labaton.com/cases/in-re-facebook-biometric-information-privacy-litigation

Osborne, C. (2021, March 1). Judge approves $650m settlement for Facebook users in privacy, biometrics lawsuit. *Zero Day.* https://www.zdnet.com/article/judge-approves-650m-settlement-for-facebook-users-in-privacy-biometrics-lawsuit/

Paxton, K. (2024, July 30). Attorney General Ken Paxton secures $1.4 billion settlement with Meta over its unauthorized capture of personal biometric data in largest settlement ever obtained from an action brought by a single state [Press release]. https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture

Perdew, P. R., & Trifon, T. L. (2020, July 24). Locke Lord quick study: When half a billion dollars is not enough: What the Facebook settlement can teach us. *Troutman Pepper Locke.*

https://www.lockelord.com/newsandevents/publications/2020/07/facebook-settlement.

Pesenti, J. (2021, November 2). Facebook: An update on our use of face recognition [Press release]. https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

Sumadevi, S., & Kumbar, M. (2019, December). Use of social media to promote library services in the digital age. *ResearchGate.* https://www.researchgate.net/publication/337673976_Use_of_Social_Media_to_Promote_Library_Services_in_the_Digital_Age

The Fashion Law Media (TFL). (2020, August 13). Facebook is allegedly collecting, sharing Instagram users' biometric data without their consent [Law article]. https://www.thefashionlaw.com/facebook-is-allegedly-collecting-sharing-instagram-users-biometric-data-without-their-consent/

Today's General Counsel (TGC). (2025). Non-Facebook users sue Meta over facial data privacy. *Today's Legal Operations.* https://todaysgeneralcounsel.com/non-facebook-users-sue-meta-over-facial-data-privacy/

Wolford, B. (2025). What is GDPR, the EU's new data protection law? *GDPR.EU.* https://gdpr.eu/what-is-gdpr/

Xie, I., & Stevenson, J. (2014). Social media application in digital libraries. *Online Information Review*, *38*(4), 502-523. https://www-emerald-com.ezproxy.lib.uwm.edu/insight/content/doi/10.1108/OIR-11-2013-0261/full/pdf

Zeigler, S. L. (2024, July 5). Communications Decency Act and Section 230 (1996). *Free Speech Center at Middle Tennessee State University.* https://firstamendment.mtsu.edu/article/communications-decency-act-and-section-230/