Social Media Privacy: The Risks, Responsibilities, and Regulations

Bella S. Baldessari

Department of Journalism and Media Management, University of Miami

Abstract

This paper investigates the privacy risks social media users face, the responsibilities of the platforms, and the regulations surrounding these services. In addition, it discusses privacy law, relevant legislation, and notable court cases to help understand the growth of social media platforms and shed light on protections put in place to keep personal information safe. Due to a vast majority of social media users not reading terms and conditions agreements in full, users may be unaware that their data is being collected and used, thereby raising the risks of using social media.

Keywords: social media, privacy, platforms, regulations, risks, legislation

Social Media Privacy: The Risks, Responsibilities, and Regulations

The rapid growth of social media platforms in today's digital age has changed the way personal information is used and protected. Social media is an integral part of many lives, as it is an easy way to stay in touch with family members and friends. These platforms have completely transformed the way individuals share information, engage with the society around them, and how they interact with each other. The second stage of development of the World Wide Web called Web 2.0 is widely credited with the growth of social media use. Van Dijck (2013) noted "For many early adopters, belief that Web 2.0 was a communal and collaborative space inspired their endeavors to build platforms, and echoes of this early idealistic spirit resound to this day" (p. 11). Through agreements made with platforms to use their service, users agree to all kinds of things like: data collection and usage, permissions for third-party access, and use of one's personal information for training artificial intelligence models.

Social media has become important in shaping popular culture, marketing strategies, and political discourse as these platforms offer unique ways for communication and entertainment. While they are integral to everyday life for most people, the growth of social media usage in recent years raises concerns about privacy. According to Gottfried (2024) at the Pew Research Center:

> YouTube by and large is the most widely used online platform measured in our survey. Roughly eight-in-ten U.S. adults (83%) report ever using the video-based platform. While a somewhat lower share reports using it, Facebook is also a dominant player in the online landscape. Most Americans (68%) report using the social media platform. Additionally, roughly half of U.S. adults (47%) say they use Instagram. (p. 3)

The majority of social media platforms operate worldwide and depending on their location, users may be subjected to more or less protection. Operating worldwide creates a large amount of responsibilities for not only the platforms but the governments. Through examining existing regulations such as the Federal Trade Commission (FTC) Act, Section 230 of the Communications Decency Act (CDA), and the Children's Online Privacy Protection Act (COPPA), this research will comprehensively review the current state of social media privacy laws. Additionally, important court cases such as Snapchat's class-action lawsuit in Illinois, the United States' Justice Department suing TikTok and Parent Company ByteDance for widespread violations of children's privacy laws, and the arrest of Telegram's Co-Founder, Pavel Durov will help explain how privacy is governed. In another Pew Research Center study, McClain et al. (2023) found that "The public increasingly says they don't understand what companies are doing with their data. Some 67% say they understand little to nothing about what companies are doing with their personal data, up from 59%" (p. 4). The authors also suggested that the majority of people feel that they have minimal or no influence on how companies or the government control their personal data. Thus, properly understanding the ways to protect one's individual rights is integral to using social media safely and also an important part of the future of ethical usage of social media.

Overview of Privacy Law

"Privacy law can't easily be defined, but it refers very generally to the laws regulating the collection, storage, and use of personal information" ("Privacy Law," n.d.). Privacy law is extremely important today in the digital age. Many scholars agree that there are two types of privacy: autonomy and social privacy. These two opposing views have forced scholars into choosing one of the two sides. Autonomy scholars believe that privacy is an individual right to

be “left alone” and that an individual is allowed to limit access to personal information. The right to privacy dates back to as early as the *Katz v. United States* case, which established privacy in the United States, is violated when an individual has a “reasonable expectation” to be left alone. On the other hand, for social privacy scholars understand that there is a limitation in how privacy can be controlled through social media and raise concern on how personal information is shared in these contexts (Kuenzler, 2021). Privacy law is essential in protecting users from collection of personal data, control over who collects this data, and it requires big corporations to be transparent about their data collection practices. Sarikakis and Winter (2017) describe their study of European social media users as testing their understanding of privacy and their overall awareness of legislation that affect privacy. They used focus groups to conduct this research and during the middle of their study, the European Court of Human Rights ruled against Google on the basis of the “Right to be Forgotten” after testimony from whistleblower Edward Snowden. Essentially this law allows for private information about someone to be removed from the internet. But, the “Right to be Forgotten” does not exist in the United States, Sarikakis and Winter (2017) concluded:

> Interestingly, although no participant withdrew completely from social media, several reported changes in their behaviors, which ranged from posting less, posting differently, and engaging in active ways of protecting their privacy after the “Right to be Forgotten” ruling and the Edward Snowden revelations. (p. 11)

Breach of Privacy

Although, in the United States, the “Right to be Forgotten” law does not exist, there is one key legal case that shaped privacy rights in social media: the Facebook-Cambridge Analytica data scandal. As previously mentioned, social media has become a driving force in political

discourse and this case brought up concerns in 2018 that Cambridge Analytica (an elections consulting agency) and Facebook used data to influence the outcome of the 2016 U.S. presidential election.

In 2010, Facebook launched a platform called Open Graph. Through this platform third-party apps would "have access to a user's name, gender, location, birthday, education, political preferences, relationship status, religious views, online chat status and more. In fact, with additional permissions, external sites could also gain access to a person's private messages" (Meredith, 2018). Meredith goes on further to say that in 2015 *The Guardian* revealed that Cambridge Analytica was assisting Texas Senator Ted Cruz's political campaign. The story implied that Cruz was leveraging psychological data from research of tens of millions Facebook users to gain a competitive edge over his opponents. Despite being asked to remove all of the data by Facebook, Cambridge Analytica did not, and this refusal led to a Federal Trade Commission (FTC) investigation into whether Facebook had violated a 2011 agreement with the U.S. government over privacy violations.

This case set the precedent for legal consequences for violations of privacy on social media platforms in several ways. First, the scandal had a huge media following that led to public scrutiny which in turn, increased the attention for regulatory bodies to investigate how corporations use personal data. Furthermore, the FTC fined Facebook for $5 billion for its role in the scandal, showing that massive financial repercussions could be imposed for those who fail to protect user data. Additionally, the eventual fallout from the case destroyed many people's trust in social media platforms in general. While Facebook vowed to increase transparency with users by giving users more ways to personally manage their privacy settings and implement changes to privacy policies, the scandal completely ruined the public's trust in Facebook.

Looking at the $ 5 billion fine that the FTC gave Facebook, one might begin to think that social media platforms have the full responsibility in protecting user data and regulating the content posted on their sites. According to Marwick (2023), that was not the case:

> The Supreme Court's "reasonable expectation" test uses two criteria to determine whether a privacy violation has occurred. First, the person must subjectively believe that their privacy was violated. Second, they must have been in a place or situation where they reasonably expected to have privacy. But while courts have ruled that people can reasonably expect privacy in their home or car or in a telephone call or paper letter, legally there is no reasonable expectation of privacy in any internet communication, including email, GPS coordinates, or bank records. (pp. 28-29)

Moreover, Section 230 of the Communications Decency Act (CDA) essentially shields platforms from liability. According to this section of the law, social media sites are not held responsible for content in users' posts, including material that is defamatory or infringe on an individual's copyright. Hickey (2021) explained the Communications Decency Act by comparing it to a market selling bad fruit, where both the market and the grower could be held liable. However, social media platforms like Facebook and Instagram don't "sell" content; instead, they simply provide a space for others to share it.

Privacy regulations outside the United States. look very different, specifically those for minors. In general, U.S. federal legislation around social media privacy has taken much longer than international law to be put in place. A leader in this type of legislation internationally has been the European Union with their Digital Services Act. Kelly (2024) explained: "Perhaps one of the biggest changes in the EU for children, as a result of the law, is that platforms are forbidden from targeting them with personalized advertising." In addition, it is important to note

that depending on the size of the social media entity, more or less protections can be put in place. Later, the author expanded on more laws internationally, explaining that India's Personal Protection Bill, "requires parents to consent to the collection of their child's data and bans targeted advertising to minors." It is hard to pinpoint why the U.S. does not move as quickly with protecting their citizens' privacy as much as other countries.

Understanding Terms and Conditions

With many social media platforms being classified as open platforms, where anyone can sign up for free and post to the internet, the openness brings up concern about the action a user takes just before creating an account; what does the "accept terms" button actually mean? When signing up to use one of these platforms a user has to either accept the terms and conditions or choose to not use the app. The lack of options creates a requirement, where one has no choice but to accept the terms and conditions agreement in order to not be left out of social culture. There is virtually no other place to get the content posted on those platforms but those platforms. "While these contracts generally don't give ownership of published content to the social media companies, the agreement does usually secure the companies a broad license to use anything users post to their platforms" (Thompson 2015). The majority of privacy policies are the same for social media platforms; they say that the user is granting them a free transferable license and they can do what they want with users' personal data (location, messages, service provider, etc.), among other things. Many new changes to terms and conditions agreements have included sections on training artificial intelligence models. Hidden under thousands of words, written in legalese, are minimal but impactful changes. Google, for example, changed just eight words. Under European law, Meta had to alert users to the fact that their public posts would be used to train A.I. However, after many complaints, these plans were paused. "In the United States, where

privacy laws are less strict, Meta has been able to use public social media posts to train its A.I. without such an alert" (Tan, 2023).

While social media platforms are a great tool to stay connected with friends and family, there is a possibility that one could overshare. Oversharing on social media could put your personal information at risk. Through online tracking, social media companies use their users' online activity to better prepare their algorithms to personalize user preferences. According to Berrios et al. (2022), "This has, in turn, contributed to a loss of trust and changes in how people interact (or not) on social media, leading some users to abandon certain platforms altogether or to seek alternative social media platforms that are more privacy focused" (p. 116).

So, how can users protect their personal information? Some basics are: keep their accounts set to private, do not accept follow requests from strangers (even mutual friends can put you at risk), and do not post your current location. For those who use Snapchat, it is important to remember that stories do not disappear. Although it looks like the story goes away after 24 hours it can be stored on their server. University of Kentucky ITS Cybersecurity Analyst Jackie Campbell stated that "Snapchat states in their terms and conditions that they have the 'right to retain the message if they want to' (Boyer, 2023). Terms and conditions agreements can be tricky so it is important to take the time to read them and understand what information may be collected.

Legal Landscape: Relevant Legislation and Court Cases

Similarly to terms and conditions agreements, understanding the relevant legislation and court cases surrounding social media privacy can be difficult to fully grasp because of the legalese. The United States governs social media privacy differently than the rest of the world. Generally, the United States gives more power to its states to govern their residents how they

would like unlike other countries where legislation directly from the federal government is the end all be all.

An example of the U.S. states having power is when lawmakers in Florida and Texas put into place state laws, banning social media sites from banning or restricting the reach of political candidates (Allyn & Totenberg, 2024). These laws came after the U.S. The Supreme Court returned cases from both states (*Moody v. NetChoice* and *NetChoice v. Paxton*) to lower courts for further review. These laws brought questions and lawsuits over First Amendment rights. Section 230 of the Communications Decency Act is supposed to protect social media companies, however many Conservatives have been fighting the law; claiming that it gives platforms the authority to censor right-wing perspectives.

An important law in social media privacy is the Federal Trade Commission (FTC) Act. Specifically, Section 5 of the Act focuses on prohibiting unfair or deceptive acts or practices in commerce and unfair methods of competition. The FTC currently has the broadest federal jurisdiction over protecting consumer privacy. Chao et al. (2019) argued that "as an agency created to focus primarily on commerce and consumers, the FTC may not be best positioned to tackle the full breadth of privacy issues, especially those that go beyond commerce and affect more than just consumers" (p. 9). In order for the FTC to be respected as an agency that could properly protect U.S. citizens, the U.S. Congress could choose to grant them more authority. A more unlikely option would be the creation of a new agency. A brand new agency could "improve relations with authorities abroad 'in terms of having [an equivalent] chairman ... and a central focus in the United States government for them to deal with'" (Chao, 2019, p. 13). Unfortunately, the downside to creating an entirely new agency would be that it is very expensive and time-consuming.

The United States is falling behind when trying to protect children's privacy online. The House of Representatives was supposed to pass updates aimed at increasing online privacy protections for minors after their August 2024 recess, but have not yet. The new legislation package would include the Kids Online Safety Act (KOSA) and the Children's Online Privacy Protection Act (COPPA). "KOSA is designed to hold social media companies more accountable for potential harm caused to minors using their platforms. It also would enable the federal government to investigate and sue websites believed to cause children 'psychological distress'" (Modrich, 2024). On the other hand, COPPA is more focused on data protection. Because there is no comprehensive federal law in the United States specifically meant to govern online privacy, children's privacy laws vary incredibly across its fifty states. Additionally the Senate bill has differences from the House bill. Modrich (2024) explains:

> The Senate's bill applies broadly to all online platforms, including social media, messaging apps and multiplayer video games. The House version of KOSA only applies to the largest 'high impact' platforms, defined as companies with at least $2.5 billion in annual revenue or more than 150 million global monthly active users.

The conflict between the two bills is most likely due to differing parties in control. The U.S. House currently has a Republican majority while the Senate has a Democratic majority, and until there is some change in leadership it is unlikely that the package will be passed.

Snapchat Class-Action Lawsuit

Expanding further on the United States giving power to its states to govern their residents' social media privacy as they would like, Illinois takes online privacy seriously. In November 2022, a settlement was reached in *Boone et al. v. Snap, Inc*. where Snapchat was found in violation of Illinois' Biometric Information Privacy Act (BIPA). The BIPA "requires

prior notification and consent before a private entity can collect and save biometric data" (Soglin, 2022). The Illinois' BIPA is considered to be one of the most strict laws on protecting biometric information in the U.S. and it is different from other privacy laws because it allows private citizens to sue companies. Snapchat was specifically accused of using their lenses and filters to collect biometric data that could be used to identify a specific person or be used in facial recognition (Soglin, 2022). In this case, Snapchat had to pay users $35 million. Snapchat has had other related issues stem from their filters; in May 2022 a federal lawsuit was filed against them for their use of augmented reality filters. Other platforms like Facebook and Google Photos have also been sued under the Illinois' BIPA, for their facial recognition features. The Illinois' BIPA could potentially be used as an example for other states' privacy legislation or possibly be used as inspiration for a new federal law.

With the rise of new technologies that work with facial recognition, like artificial intelligence, a federal law could be extremely important to ensure social media privacy is standardized across all platforms. Additionally, these high-profile cases could help manage to decrease social media companies' ability to exploit the lack of legislation in certain states. These companies could stay out of biometric trouble by offering an opt-in feature for facial recognition instead of having the feature automatically activated when using the platform. Due to the lack of consistent authority for social media platforms, they have adapted quickly to changes made in regulations and have been able to avoid repercussions.

Justice Department Sues TikTok and Parent Company ByteDance

After determining to ban TikTok in the U.S. if it is not sold to a non-Chinese owner, the Justice Department on behalf of the FTC in August of 2024 filed a lawsuit against TikTok and their parent company, ByteDance for failing to comply with the United States' Children's Online

Privacy Protection Act (COPPA). This is the second lawsuit filed against TikTok and ByteDance by the U.S. Justice Department in under a year. The FTC claimed that TikTok and ByteDance did not comply with COPPA because they failed to notify and get parental consent before collecting and using the personal information of children under age 13. According to the FTC (2024), "The company continued to collect personal data from these underage users, including data that enabled TikTok to target advertising to them—without notifying their parents and obtaining consent as required by the COPPA rule." Depending on the outcome of this case, TikTok as well as other platforms might consider implementing a more rigorous age verification process than the current self-reporting system.

As a part of this case, TikTok's heavy reliance on algorithms to personalize their users' feeds is being investigated as well. If they are found liable for using childrens' personal data to make more engaging feeds, other platforms could take measures to create or update their restrictions for collecting underage user data in order to not lose their engagement. Additionally, transparency from platforms on how data is collected/stored could be brought up as a possible solution. A successful case against TikTok could be the big push needed for other countries to take action to protect their citizens' data.

Arrest of Telegram Co-Founder, Pavel Durov

The arrest of Telegram Co-Founder and CEO, Pavel Durov, in France at the end of August 2024 raised many questions about the current state and future of social media privacy and more. Durov is facing allegations that his platform "is being used for illicit activity including drug trafficking and the distribution of child sexual abuse images" (Ortutay, 2024). While Telegram is not widely known or used in the United States, it is popular in Durov's home country of Russia, as well as in France, India, and Indonesia, among others. The messaging platform

allows one-on-one conversations, group chats that can have upwards of 200,000 people, and lets users broadcast messages to subscribers (Ortutay, 2024). Moreover, these group chats and broadcast channels do not have end-to-end encryption by default, meaning Telegram can access their users' messages. If users want that protection, they have to manually switch it on. During their investigation, French authorities have found evidence that the app is being used by Islamic extremists and drug traffickers. Durov was released on bond and it is unclear if the case will go to trial or if the charges will be dropped.

Telegram's lack of moderation of content has led to the misuse of it for criminal activities. Just like in the U.S. Constitution, the French constitution protects Freedom of Speech except that right is not absolute in France. So, if the French authorities successfully access messages during their investigation, is it a violation of the constitution? It is not according to the General Data Protection Regulation (GDPR), which states that "processing is necessary for compliance with a legal obligation to which the controller is subject" (European Parliament & Council of the European Union, 2016, Article 6). Whether or not the authorities have the right to search through or read messages on Telegram even if the encryption feature is on becomes irrelevant after analyzing Europe's GDPR. Pavel Durov's arrest represents a long ongoing battle with social media platforms and pressure on governments to moderate content. This arrest and possible trial could affect future regulations on social media privacy, as the investigation may bring up questions about government involvement in user privacy.

Conclusion

Ultimately, this paper has shown the risks users face, the responsibilities of the platforms, and the regulations surrounding social media privacy. While social media has revolutionized the way we communicate, it has brought immense concern about our privacy.

Through discussion of privacy law it has demonstrated the importance of having a full understanding of its technicalities, today in the digital age. The two opposing viewpoints of the two types of privacy (autonomy and social privacy) have led scholars to choose one side, but both agree that privacy law is essential in protecting users of all ages. This protection includes safeguarding of personal data, control over who collects this data, and it forces major corporations to be honest about their data collection practices.

The relevant legislation detailed in this paper showed the key legal frameworks in the U.S. and around the world for social media privacy. Even though the United States does not have legislation such as the "Right to be Forgotten" approach in Europe, the Facebook-Cambridge Analytica data scandal has acted as a warning to social media companies to demonstrate that they can be held accountable for allowing third-party access to user data and interfering with the outcome of presidential elections. Also, understanding terms and conditions agreements is important because many social media platforms are classified as open platforms. Open platforms means that anyone with internet access can post to the internet for free. It's relevant to remember that the majority of privacy policies are identical, stating that each user is granting them a free transferable license if they press decide to agree to the terms. The risks associated with social media usage tend to increase because of the user's lack of education on what kind of a contract they are signing.

Lastly, the paper explored the impact that regulatory bodies play in properly addressing The court cases that were reviewed, showing real world examples of how their outcomes can affect the future of social media privacy. These court cases are helpful in understanding how much social media platforms have grown since their inception and shed light on the protections created to keep personal information safe.

In my opinion, the long-term effects of issues revolving around social media privacy might affect many things in the future, such as user trust, stricter regulations, government control, user mental health, and so forth. Distrust in social media platforms could lead to a significant decrease in user engagement which would mean less user-generated content if users decide they do not want to share personal information online anymore. Eventually, users will most likely move to platforms that do prioritize their privacy. In order to stay out of legal trouble with authorities, social media companies must take privacy seriously. They currently do not. With strict laws being enacted around the world it will not be long before they can no longer collect user data as freely as they do now. Europe is showing great promise with their GDPR law, cracking down on companies who do not comply. It is important to note that stricter regulations will probably cause tension and hinder the development of new technologies/services that use data collection, like web analytics platforms or online shopping.

Additionally, I think increased government control will cause surveillance and censorship concerns; similarly to the ongoing Telegram investigation. If governments use their authority over social media platforms and their data to track their citizens' activity it would become a threat to not only online privacy but privacy in the real world as well. Even if governments take measures to assure their citizens that their surveillance of their online activity is exclusively for public safety, I do not think that many will believe that their private information is used only for this purpose. There can no longer be unregulated exploitation and misuse from social media platforms. Governments must be able to properly balance protection and infringing on critical individual freedoms. The European Union has shown this balance through their GDPR. This expansive law effectively pushes social media companies to protect user privacy. The United States should look into creating a law similar to the GDPR to see similar results.

Furthermore, there are psychological impacts that invasion of privacy amplifies, with the most relevant being stress and anxiety. A loss of the sense of control is what many people perceive as stress. “Sharing personal information, pictures, and opinions with a broad online community entails a very real loss of control over such data—a loss of control over one’s own circumstances which has been described as *learned helplessness*” (Stevic et al., 2021, p. 333). Withdrawal from social media use can lead to the loss of important social interactions, as well. Users should always be informed about what privacy practices their most used platforms utilize, as it is virtually impossible for users themselves to protect all of their personal data. It is an unnecessary stress that does not need to be blamed on one side or the other. In the future, a collective effort is needed to protect each other. Social media should remain a place of connectivity and communication, not fear. As social media continues to grow rapidly and become more integrated into our daily lives users must remain aware of its consequences.

References

Allyn, B., & Totenberg, N. (2024, July 1). *Supreme Court puts Florida and Texas social media laws on hold*. NPR. https://www.npr.org/2024/07/01/nx-s1-4991108/supreme-court-netchoice#:~:text=The%20laws%20in%20both%20Texas,from%20content%20hosted%20by%20platforms

Berrios, S., Page, X., Wilkinson, D., & Wisniewski, P. J. (2022). Social media and privacy. In N. Proferes & J. Romano (Eds.), *Modern socio-technical perspectives on privacy*. (pp. 113-147). Springer Nature. https://doi.org/10.1007/978-3-030-82786-1

Boyer, C. (2023, October 13). *How oversharing on social media could put your personal information at risk*. University of Kentucky. https://its.uky.edu/news/how-oversharing-social-media-could-put-your-personal-information-risk

Chao, B., Null, E., & Park, C. (2019, November). Enforcing a new privacy law. New America Organization. https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/the-ftc-is-currently-the-primary-privacy-enforcer-but-its-authority-is-limited/

European Parliament & Council of the European Union. (2016). *Lawfulness of Processing (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 on the protections of natural persons with regard to the processing of personal data and on the free movement of such data.* (General Data Protection Regulation). https://gdpr-info.eu/art-6-gdpr/

Federal Trade Commission. (2024, August 2). *Justice Department sues TikTok and Parent Company ByteDance for Widespread Violations of Children's Privacy Laws* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-law suit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law

Gottfried, J. (2024, January 31). *Americans' social media use*. Pew Research Center. https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/

Hickey, B. (2021, February 10). *Can social media sites be held accountable for users' posts?* The Nexus; Thomas Jefferson University. https://nexus.jefferson.edu/business/can-social-media-sites-be-held-accountable-for-users -posts/

Kelly, S.M. (2024, February 13). *Outside the US, teens' social media experiences are more tightly controlled*. CNN. https://www.cnn.com/2024/02/13/tech/social-media-regulation-outside-us/index.html

Kuenzler, A. (2021, October 20). On (some aspects of) social privacy in the social media space. *International Data Privacy Law*, *12*(1), 63–73. Oxford Academic. https://doi.org/10.1093/idpl/ipab022

Marwick, A. E. (2023). *The private Is political: Networked privacy and social media*. Yale University Press. https://doi.org/10.2307/jj.2543560

Mcclain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). *How Americans View Data Privacy*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Meredith, S. (2018, April 10). *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Modrich, S. (2024 August 27). *Tech industry braces for impact of kids' online privacy laws*. S&P Capital IQ Pro. https://www.capitaliq.spglobal.com/apisv3/spg-webplatform-core/news/article?KeyProductLinkType=2&id=82951818

Ortutay, B. (2024, August 28). *What is Telegram and why was its CEO arrested in Paris?* AP News. https://apnews.com/article/telegram-pavel-durov-arrest-2c8015c102cce23c23d55c6ca82641c5

"Privacy Law." (n.d.). Georgetown Law. www.law.georgetown.edu. https://www.law.georgetown.edu/your-life-career/career-exploration-professional-development/for-jd-students/explore-legal-careers/practice-areas/privacy-law/

Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media + Society*, 3(1), 205630511769532. https://doi.org/10.1177/2056305117695325

Soglin, T. (2022, August 22). Snapchat parent reaches $35 million biometric privacy class-action settlement in Illinois. Chicago Tribune. https://www.chicagotribune.com/2022/08/22/snapchat-parent-reaches-35-million-biometric-privacy-class-action-settlement-in-illinois/

Stevic, A., Schmuck, D., Koemets, A., Hirsch, M., Karsay, K., Thomas, M. F., & Matthes, J. (2021). Privacy concerns can stress you out: Investigating the reciprocal relationship between mobile social media privacy concerns and perceived stress. *Communications, 0*(0). https://doi.org/10.1515/commun-2020-0037

Tan, E. (2024, June 26). When the terms of service change to make way for A.I. training. The New York Times. https://www.nytimes.com/2024/06/26/technology/terms-service-ai-training.html

Thompson, C. (2015, May 20). *What you really sign up for when you use social media*. CNBC. https://www.cnbc.com/2015/05/20/what-you-really-sign-up-for-when-you-use-social-media.html

van Dijck, J. (2013). *The culture of connectivity : A critical history of social media* (1st ed.). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199970773.001.0001