PERMISSION NOT GRANTED: A DOMESTIC AND GLOBAL COMPARATIVE ANALYSIS ON SOCIAL MEDIA POLICIES, PRIVACY LAWS AND A PROPOSAL FOR THE UNITED STATES

Simran Saini[1]

I. INTRODUCTION

When you Google "TikTok's privacy policy," suggested searches that are displayed include things like: "Does TikTok have privacy issues?" "Does TikTok steal your data?" "What is TikTok's privacy policy?" "Is TikTok a spying app?"[2] These searches clearly portray the legitimate public concern of enforcing its right to privacy and being protected from any breaches in day-to-day life while using the popular social media platform and app. Specifically, these concerns started to become more prevalent as users of TikTok began discovering that their personal information was being used without consent. Social media and the internet, in general, have become more prevalent in the lives of individuals all over the world. Although many benefits are attached to utilizing the internet and social media platforms, there are also costs associated with them; specifically, the unauthorized exposure of personal information and data. The internet and social media are evolving rapidly and the laws associated with the two should keep up to protect citizens everywhere. The main case that will be examined in this note addressing these concerns is *In Re: TikTok, Inc., Consumer Privacy Litigation* "*In Re: TikTok*".

Data privacy is not highly regulated in the United States.[3] There are currently no comprehensive federal data privacy laws to protect citizens' data privacy rights.[4] Furthermore, there are no data privacy laws which

---

[1] J.D. Candidate, Southern Illinois University School of Law, Class of 2022. The author dedicates this note to her mother, Harprit Saini, for her constant love and support throughout the years; to her mentor, Jayanthi Sundararajan, for the positive influence she has had on the author's education; and to Bradley Neal for being the author's cheerleader throughout law school. Special thanks to Professor Cynthia Fountaine for her professional advising relating to this note and to the author's close friend, Micaylee Uhls, for devoting her time to making this Note reach its fullest potential.

[2] The author conducted this survey on her own and used the results of her findings.

[3] *The Differences Between the United States & European Data Laws*, FRONTIER TECH. (Oct. 12, 2015), https://www.frontiertechnology.co.uk/2015/10/12/the-differences-between-eu-and-us-data-laws/.

[4] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

specifically protect internet users.[5] With the growing use of social media, a comprehensive set of laws should exist to protect American users on the internet.

This note will focus on discussing the need for comprehensive internet data privacy laws, specifically pertaining to social media. Part II of this note will discuss the important definitions related to data privacy. Part III will follow with an analysis of internet data privacy laws in the United States, on both the federal level and state level, and the European Union. Next, Part IV of this note will examine recent private tort actions initiated against social media platforms, primarily focusing on TikTok. Lastly, Part V will conclude with a proposed solution focusing on the need for a federal comprehensive data privacy law in the United States.

II. DEFINITIONS

A. What is Data Privacy (i.e., Data Protection)?[6]

Data privacy, also referred to as data protection by the European Union, is defined as the right of individuals to have control over how their personal data is collected, shared, and used.[7] Data privacy gives users the opportunity to make their own decisions regarding who has access to their data, as well as how their data will be used.

B. What is Personal Data and Personal Information?

There is no single, comprehensive definition of what constitutes personal data and personal information. However, the European Union and the state of California have offered definitions that are useful in aiding our understanding of what is meant by the terms "personal data" and "personal information." The General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") are successful models of comprehensive data privacy laws. The European Union's GDPR defines personal data as:

> [A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one

---

5 *Id.*

6 Ben Wolford, *A Guide to GDPR Data Privacy Requirements*, GDPR.EU, https://gdpr.eu/data-privacy/ (last visited Dec. 24, 2021).

7 *What is Data Privacy?*, SNIA, https://www.snia.org/education/what-is-data-privacy (last visited Dec. 24, 2021).

> or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[8]

The CCPA defines personal information as:

> [I]nformation that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.[9]

C. What are Biometric Data and Biometric Identifiers?

Biometric data are unique physical characteristics of an individual, such as fingerprints or facial recognition, that can be used for automated identification.[10] Biometric information is any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier, used to identify an individual.[11]

Biometric identifiers include retina or iris scans, fingerprints, voiceprints, and scans of hands or face geometry.[12] Biometric data and identifiers are highly sensitive due to their biologically unique nature. Meaning, once they are compromised, an individual has a heightened risk for identify theft and cannot use biometric-facilitated actions without the risk of his or her identity being compromised.[13]

D. What is a Private Right of Action?

A private right of action is a right of a private party to seek judicial relief from injuries caused by another's violation of a legal requirement.[14] This allows a private plaintiff to bring an action based directly on a public statute, the Constitution, or federal common law.[15]

---

8 Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 33 (EU).

9 California Consumer Privacy Act, CAL. CIV. CODE § 1798.140 (West 2021).

10 *Biometrics*, U.S. DEP'T OF HOMELAND SEC. (June 9, 2021), https://www.dhs.gov/biometrics.

11 740 ILL. COMP. STAT. 14/10 (2008).

12 *Id.*

13 *Id.*

14 Cannon v. Univ. of Chi., 441 U.S. 677, 730 (1979) (Powell, J., dissenting).

15 Caroline Bermeo Newcombe, *Implied Private Rights of Action: Definition, and Factors to Determine Whether a Private Action Will Be Implied from a Federal Statute*, 49 LOY. U. CHI. L.J. 117, 120 (2020).

III. BACKGROUND INFORMATION ON CURRENT PRIVACY LAWS

A. Privacy Laws that Currently Exist in the United States: The Federal Level.

1. The Federal Trade Commission and the Federal Trade Commission Act

There is no comprehensive federal statute that regulates internet data privacy in the United States.[16] However, the United States currently has federal statutes in effect to address specific internet data privacy concerns including the Federal Trade Commission Act of 1914 ("FTCA"),[17] the Electronic Communications Privacy Act ("ECPA"),[18] the Computer Fraud and Abuse Act ("CFAA"),[19] the Children's Online Privacy Protection Act ("COPPA"),[20] the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"),[21] the Gramm-Leach Bliley Act ("GLBA"),[22] and the Fair and Accurate Credit Transactions Act ("FACTA").[23] The Health Insurance Portability and Accountability Act ("HIPAA"), is also a commonly-known federal data protection statute, however, it is not tailored to internet data privacy protections.[24]

Although these laws exist and address consumer data protection, they do so only to the extent of specific substantive fields. These areas include unfair or deceptive practices,[25] consumer financial information,[26] personal health information,[27] and children's data.[28] The most significant discrepancy between the current laws in the United States and other international privacy laws is that the United States lacks a comprehensive regulation which generally protects consumer data.[29] The most relevant privacy statutes belonging to the aforementioned specific substantive categories will be discussed in further detail below.

---

16 *Internet Privacy Laws Revealed—How Your Personal Information is Protected Online*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online (last visited Sept. 23, 2021).

17 15 U.S.C. §§ 41-58.

18 18 U.S.C. §§ 2510-23.

19 18 U.S.C. § 1030.

20 15 U.S.C. §§ 6501-05.

21 15 U.S.C. §§ 7701-13.

22 15 U.S.C. § 6801.

23 15 U.S.C. § 1681.

24 Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1938 (1996) (codified as amended at 29 U.S.C.A. §§ 1181-6039F).

25 THOMSON REUTERS, *supra* note 16.

26 15 U.S.C. §§ 41-58.

27 15 U.S.C. § 6801.

28 15 U.S.C. §§ 6501-05.

29 O'Connor, *supra* note 4.

In the United States, there is no single national authority—or agency—that governs data protection.[30] There are only a few designated agencies which govern data protection related to specific subjects.[31] For example, the Federal Trade Commission ("FTC") was created to have the authority to oversee data protection in relation to commercial practices targeted directly at American consumers.[32]

The most prominent FTC regulation is the Federal Trade Commission Act ("FTCA") which prohibits companies from engaging in unfair and deceptive practices.[33] Unfair and deceptive practices are defined as representations, omissions, or practices which mislead or are likely to mislead a consumer; a consumer's interpretation of the misleading representation, omission, or practice, which is considered reasonable under the circumstances; and the misleading representations, omissions, or practices are material.[34] Under the FTCA, the FTC is empowered to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[35] It is important to note that the FTCA does not allow a private right of action.[36] On behalf of the United States, the FTC has brought charges against Facebook under the FTCA and PayPal under the GLBA for breaches in data privacy.[37]

The primary claim by the United States in its action against Facebook was that Facebook was engaging in deceptive acts and practices by representing to its users that Facebook's privacy settings allowed them to restrict information they shared to limited audiences.[38] However, those settings did not prevent Facebook from sharing any user information with third-party developers of apps installed by the users' Friends (i.e., games and shopping).[39] Facebook was required to pay a penalty of five billion dollars in a settlement order for violating the FTCA.[40] Under the FTCA, Facebook

---

30 *Data Protection Laws of the World*, DLA PIPER (Jan. 28, 2021), https://www.dlapiperdataprotection.com/index.html?t=law&c=US.

31 STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW (2019).

32 *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Jan. 30, 2021).

33 15 U.S.C. §§ 41-58.

34 FEDERAL RESERVE, CONSUMER COMPLIANCE HANDBOOK (2016), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

35 15 U.S.C. §§ 41-58.

36 Stephanie L. Kroeze, *The FTC Won't Let Me Be: The Need for a Private Right of Action Under Section 5 of the FTC Act*, 50 VAL. U. L. REV. 227, 227-30 (2015).

37 *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

38 Complaint for Civil Penalties, Injunction, and Other Relief at 4, United States v. Facebook, Inc., 456 F. Supp. 3d. 105 (D.D.C. 2020) (No. 19-cv-2184).

39 *Id.*

40 FED. TRADE COMM'N, *supra* note 37.

users affected by its breach were not entitled to bring a private right of action.[41]

The United States charged PayPal under the GLBA.[42] The main purpose of the GLBA is to ensure that financial institutions are explaining their information-sharing practices to customers for products and services like loans, insurance, or general financial advice.[43] Currently, under the GLBA, there is no private right of action.[44] This note will not focus on the GLBA, but it is important to highlight that no federal regulations currently allow private parties to bring a private right of action.

2. The Video Privacy Protection Act

The Video Privacy Protection Act ("VPPA") was enacted in 1988.[45] The essence of the VPPA is to penalize any videotape service provider[46] "who knowingly discloses, to any person, personally identifiable information[47] concerning any consumer."[48] The VPPA specifically outlines the relief to be provided to an aggrieved person.[49] Relief under the VPPA includes "actual damages but not less than liquidated damages in an amount of [two thousand five hundred dollars]; damages; reasonable attorneys' fees and other litigation costs reasonably incurred; and such other preliminary and equitable relief as the court determines to be appropriate."[50]

The VPPA is rarely invoked today since the primary purpose behind enacting it was to protect consumer records of "prerecorded video cassette

---

41 *Id.*

42 *PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act*, FED. TRADE COMM'N (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

43 15 U.S.C. § 6801.

44 *The Gramm-Leach Bliley Act*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/glba (last visited Sep. 23, 2021).

45 18 U.S.C. § 2710.

46 A video tape service provider is defined as:

> [A]ny person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

18 U.S.C. § 2710(a)(4).

47 Personally identifiable information is "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

48 18 U.S.C. § 2710(b)(1).

49 *Id.*

50 18 U.S.C. § 2710(c).

tapes or similar audio visual material."[51] However, the Plaintiffs in *In Re: TikTok, Inc., Consumer Privacy Litigation,* allege a breach under the Act. [52]

3. The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act ("COPPA") initially went into effect in 2000 and became effective a second time after several amendments in 2013.[53] The general focus of the COPPA is to imposes certain requirements on operators of websites or online services directed to children under thirteen years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under thirteen years of age.[54] In addition to these requirements, this rule imposes a duty to provide notice to parents and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under thirteen years of age.[55] The rule further requires that any data obtained about or regarding children must be stored securely.[56] In general, any data privacy breaches that occur, which involve children, immediately face higher penalties due to involving a minor.[57]

4. Possible Legislation? The Consumer Online Privacy Rights Act.

In 2019, Senator Maria Cantwell introduced a bill which addressed the need for a comprehensive federal digital privacy statute.[58] This proposed legislation, The Consumer Online Privacy Rights Act ("COPRA"), would focus on requiring companies to collect as little data about consumers as possible.[59] The bill also requires explicit consent from consumers when sharing their data with third parties, and holding companies responsible for correcting or deleting inaccurate data.[60] The purpose and requirements of this proposed bill reflect many aspects of the California Consumer Privacy Act

---

51 *Video Privacy Protection Act*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/vppa/ (last visited Dec. 14, 2021).

52 Consolidated Amended Class Action Complaint at 5, *In re* TikTok, Inc., Consumer Priv. Litig., No. 20-cv-4699, 2021 WL 4478403 (N.D. Ill. Sept. 30, 2021).

53 15 U.S.C. §§ 6501-08.

54 *Id.*

55 15 U.S.C. § 6502(b)(1)(B).

56 15 U.S.C. §§ 6501-08.

57 *Id.*

58 Allen St. John, *Consumer Online Privacy Rights Act Could Safeguard Data, but Tough Fight Lies Ahead*, CONSUMER REPS. (Nov. 26, 2019), https://www.consumerreports.org/privacy/consumer-online-privacy-rights-act-could-safeguard-data-but-tough-fight-lies-ahead/.

59 Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

60 *Id.*

("CCPA").[61] However, it goes beyond the CCPA.[62] Under the COPRA, consumers have the option to opt in or opt out for data sharing, unlike the CCPA which only provides Californians with different ways to opt out of data sharing.[63] Most importantly, the COPRA allows individuals to bring private actions against companies who breach their privacy rights.[64] This bill addresses the use of biometric data which is also a prevalent concern in the data privacy world today.[65] In addition to this bill's creation of a comprehensive digital privacy statute, it also calls for the formation of a new bureau under the Federal Trade Commission to oversee the regulation of all privacy activity in the United States.[66] Currently, this bill lacks bi-partisan support, making it more difficult to gather support to transform this bill into a law.[67]

B. Privacy Laws that Currently Exist in the United States: The State Level.

Biometric data has currently only been a concern of state law.[68] Illinois is, currently, the only state to have a comprehensive biometric privacy law. Other states do not have comprehensive biometric privacy laws but have included them as a part of other statutes. Texas,[69] Washington,[70] California,[71] New York,[72] and Arkansas[73] all regulate biometric data through statutes primarily aimed at regulating business activity concerning consumers.

Additionally, only three states in the United States have enacted comprehensive privacy laws.[74] These states are California,[75] Nevada

---

61 St. John, *supra* note 58.

62 *Id*.

63 *Id*.

64 S. 2968.

65 *Id*.

66 *Id*.

67 St. John, *supra* note 58.

68 Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, THE NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

69 TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017) (regulating biometric data in the business and commercial realm only).

70 WASH. REV. CODE ANN. § 19.375.020 (West 2017) (addressing biometric identifiers for the purpose of business compliance with what businesses do with consumer and employee information).

71 CAL CIV. CODE § 1798.100 (West 2018) (focusing on business regulation and protecting consumers).

72 Joseph J. Lazzarotti, *New York SHIELD Act FAQs*, THE NAT'L L. REV. (Mar. 11, 2020), https://www.natlawreview.com/article/new-york-shield-act-faqs.

73 ARK. CODE ANN. § 4-110-103(7) (West 2019).

74 Security.org Team, *47 States Have Weak or Nonexistent Consumer Data Privacy Laws*, SECURITY.ORG (Feb. 4, 2021), https://www.security.org/resources/digital-privacy-legislation-by-state/.

75 CIV. § 1798.100.

(effective October 1, 2021),[76] and Maine,[77] with California as the model state in enacting comprehensive data privacy laws.[78] The CCPA gives consumers the right to request disclosure of specific pieces of personal information that businesses have collected about them, along with the source of that information and the purpose for collecting it.[79] Nevada has a set of statutes concerning consumer data privacy online which has specific regulations for operators.[80] Like California and Nevada, Maine enacted an internet privacy statute which prohibits internet service providers from using, disclosing, selling, or permitting access to customer information through the use of internet service.[81]

1. The California Consumer Privacy Act.

Although Texas, Nevada, and Main have enacted some type of comprehensive data privacy law, the CCPA is the closest law to reflect the European Union's comprehensive data privacy law, the General Data Protection Regulation ("GDPR").[82]

The purpose of the CCPA is to give citizens of California more control over their personal information by granting them several rights under the act.[83] Specifically, the right to know about the personal information a business collects about individuals and how it is used and shared, the right to delete personal information collected from citizens, the right to opt out of the sale of personal information, and the right to non-discrimination for exercising rights under the CCPA.[84] Under the CCPA's definition of personal information, biometric information and internet, or other electronic network, activity information is also protected.[85]

Aside from the rights explicitly outlined regarding a Californian's personal information, the CCPA allows an individual to commence a private right of action, but only in limited situations.[86] A private right of action is allowed only when personal information "is subject to unauthorized access

---

76 NEV. REV. STAT. §§ 603A.010-.360 (2019).

77 ME. REV. STAT. ANN. tit. 35-A, § 9301 (West 2020).

78 CIV. § 1798.100.

79 *Id*.

80 Brian J. Pezzillo, *Privacy Rights and Data Breaches*, NEV. LAW., Apr. 2020, at 14.

81 Peter J. Guffin & Kyle M. Noonan, *Maine's New Internet Privacy Law: What You Need to Know*, THE NAT'L L. REV. (June 14, 2019), https://www.natlawreview.com/article/maine-s-new-internet-privacy-law-what-you-need-to-know.

82 Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Apr. 2, 2021), https://www.varonis.com/blog/us-privacy-laws/#comparison.

83 CIV. §§ 1798.100-.199.

84 *California Consumer Privacy Act (CCPA)*, OFF. OF THE ATT'Y GEN. CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa (last visited Sept. 22, 2021).

85 CIV. § 1798.140.

86 CIV. § 1798.150(a)(1).

and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information . . . ."[87] So, although the CCPA includes a private action, it is very narrow in comparison to the GDPR.[88] The statutory amount an injured plaintiff can recover under the CCPA is between one hundred and seven hundred and fifty dollars per consumer per incident, or actual damages, whichever is greater. The private right of action does not apply to violations of the CCPA itself (i.e., obligations of a business).[89] Instead, the private right of action only applies to violations of the California Customer Records Act, which requires that businesses ensure the protection of consumer information being held.[90] The CCPA also includes injunctive or declaratory relief and a catch-all for "any other relief the court deems proper."[91]

2. The Illinois Biometric Information Privacy Act.

The Illinois Biometric Information Privacy Act ("BIPA") is one of the strictest privacy laws in the United States.[92] The BIPA addresses five key areas.[93] First, the BIPA requires informed consent before collection of data.[94] Second, the BIPA requires a limited right to disclosure.[95] Third, the act mandates protection obligations and retention guidelines.[96] Fourth, the BIPA prohibits companies from profiting off of consumer biometric data.[97] Finally, and most importantly to this note, the BIPA allows harmed individuals to bring a private right of action.[98] The BIPA has been paramount to many privacy violations in Illinois.[99] Many class action lawsuits have been influential under this act, including four class actions against Facebook and one class action against Shutterfly.[100] Under the BIPA, private individuals

---

87 CIV. § 1798.150(a).

88 Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, IAPP, https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/ (last visited Dec. 19, 2021).

89 *Id.*

90 *Id.*

91 CIV. § 1798.150(a)(1).

92 Law 360, *Biometric Privacy in 2020: The Current Legal Landscape*, BLANKROME (Feb. 3, 2020), https://www.blankrome.com/publications/biometric-privacy-2020-current-legal-landscape.

93 *Illinois Biometric Information Privacy Act FAQs*, JACKSON LEWIS, https://www.jacksonlewis.com/sites/default/files/docs/IllinoisBiometricsFAQs2017.pdf (last visited Dec. 19, 2021).

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.*

98 Law 360, *supra* note 92.

99 *Id.*

100 *Illinois Biometric Information Privacy Act FAQs*, *supra* note 93.

may recover anywhere from one thousand to five thousand dollars per violation.[101] The BIPA allows more opportunity for private individuals to obtain relief in comparison to the CCPA, which limits the situations in which a private action may be commenced.[102]

In regard to the protection of minors under the BIPA, there are key requirements that businesses must follow in order to ensure compliance.[103] The business must provide written notice to the parent or legal guardian of the minor that it is collecting and storing biometric information.[104] Next, the business must inform the parent or legal guardian of the duration of storing the biometric information and for the specific purposes it is being used.[105] Additionally, the business must receive a written release from that parent or legal guardian.[106] Furthermore, and most importantly, no business in possession of a biometric identifier or information may sell, lease, trade, or otherwise profit from an individual's biometric information or identifier.[107] Under the BIPA, businesses are required to develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric data.[108]

C. Privacy Laws on a Global Level: The European Union's General Data Protection Regulation.

The United States is falling behind in protecting its citizens data on the internet. Currently, the European Union is leading globally for comprehensive data protection laws.[109] The GDPR was enacted in 2018 in the European Union requiring all organizations—no matter where they are incorporated legally—to be compliant due to various user data breaches occurring on internet platforms such as Google and Facebook.[110] The GDPR focuses on regulating and restricting the usage of personal data in general, regardless of how the information is being processed.[111] As long as an organization is conducting business within the European Union, which exposes its citizens to their data being shared, it is subject to the GDPR's regulations.

---

101 740 ILL. COMP. STAT. 14/20 (2008).
102 CAL. CIV. CODE § 1798.150 (West 2018).
103 14/15(b).
104 *Id.*
105 *Id.*
106 *Id.*
107 14/15(c).
108 *See generally The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Jan. 31, 2021).
109 *Id.*
110 Council Regulation 2016/679, *supra* note 8.
111 *Id.* at 44.

One of the most important aspects of the GDPR is that its enforcement is not limited only to organizations who operate in the European Union.[112] The GDPR applies to organizations that are based in the European Union but have data stored or processed outside of the jurisdiction and organization not based in the European Union that (1) offers goods or services to people in the European Union or (2) monitors individuals who live in the European Unions' online tendencies.[113] The bottom line is that if an organization targets European Union citizens, then it must be compliant with the GDPR.[114]

The seriousness of this regulation is well-reflected in its monetary penalties for any violations.[115] Infringements of the regulation are subject to fines up to twenty-million euros or four percent of the firm's total worldwide annual revenue of the preceding financial year, whichever is higher.[116]

The GDPR provides the following rights to individuals: the right to be informed in a fair and transparent manner, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights in relation to automated decision making and profiling.[117]

The first right afforded to individuals under the GDPR is the right to be informed.[118] The data subject (i.e., users) must be informed in a fair and transparent manner.[119] If a data subject requests the disclosure of what data is collected and how it will be used, the data controller[120] must provide that information.[121] This includes purposes for processing data, how long that data will be held, and who it will be shared with.[122] If personal data is collected or transferred directly or indirectly from a data subject, the data subject has a right to be informed.[123] Additionally, the data subject has a right to the

---

112 *Id.* at 19.

113 *Id.*

114 *Id.* at 33.

115 *Id.* at 82.

116 Council Regulation 2016/679, *supra* note 8, at 82.

117 *Id.* at 39.

118 *Id.*

119 *Id.* at 41.

120 Data Controller is defined as:

> [A] legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it" whereas a Data Processor is defined as "a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of a data controller.

GDPR Data Controllers and Data Processors, GDPR, https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/ (last visited Dec. 19, 2021).

121 *The Right to Be Informed*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-dp/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/ (last visited Sept. 24, 2021).

122 *Id.*

123 An example of indirect data subject identification would be a license plate number or a credit card number. A third party can easily look up either one of these items and identify to whom they belong.

information collected by the data controller, the purpose for processing the data, the categories of personal data concerned, the recipients of the data, and if applicable where the data is intended to be transferred.[124]

Second, is the right of access.[125] Under the GDPR, a data subject has a right to obtain, from the data controller, whether or not personal data is being processed. They further have a right to know where that is occurring and access to the general information on data processing.[126] For example, an individual may request the data controller provide any information it has obtained on the individual and disclosure of its intended use of that data.[127]

Third, is the right to rectification.[128] In the event that information collected on the data subject is incorrect, the data subject has the right to rectify the inaccurate personal data concerning him or her.[129] The data subject can correct the inaccurate data or provide additional information to complete deficient data.[130]

Fourth, is the right to erasure—also known as the right to be forgotten.[131] The data subject has a right to have data collected about him or herself deleted when: (1) the data is no longer necessary, (2) the data subject withdraws consent, (3) the data subject objects to the processing, (4) the personal data have been unlawfully processed, (5) the data must be erased as a result of legal compliance, or (6) there is an obligation to erase the personal data.[132]

Fifth, is the right to restrict processing.[133] Data subjects have a right to restrict processing of personal data where (1) the accuracy of the personal data has been contested by the individual, (2) processing is unlawful, (3) the controller no longer needs the personal data for processing, or (4) the data subject has generally objected to processing.[134]

Sixth, data subjects have the right to data portability.[135] The personal data must be stored in an easily shareable format.[136] The data must also be

---

Richie Koch, *What is Considered Personal Data Under the EU GDPR?*, GDPR.EU, https://gdpr.eu/eu-gdpr-personal-data/ (last visited Dec. 19, 2021); *see also* Council Regulation 2016/679, *supra* note 8, at 44.

124 Council Regulation 2016/679, *supra* note 8, at 40.

125 *Id.* at 43.

126 *Id.*

127 *Right of Access*, DATAGUISE, https://www.dataguise.com/gdpr-knowledge-center/right-of-access/ (last visited Jan. 30, 2021).

128 Council Regulation 2016/679, *supra* note 8, at 43.

129 *Id.*

130 *Right to Rectification*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-dp/guide-to-the-uk-gdpr/individual-rights/right-to-rectification/ (last visited Sept. 4, 2021).

131 Council Regulation 2016/679, *supra* note 8, at 43.

132 *Id.* at 44.

133 *Id.*

134 *Id.*

135 *Id.* at 45.

136 *Id.*

stored in a way that is easily understood by other processors or third parties.[137]

Seventh, is the right to object.[138] At any time, the data subject has a right to object to the processing of personal data concerning him or her and the controller must halt processing of data.[139] However, there is one exception to this right available to the data controller.[140] The data controller must show legitimate grounds for the processing of the data to override the rights and freedoms of the data subject.[141]

Finally, are the rights in relation to automated decision making and profiling.[142] The data subject has the right not to be exposed to a decision based solely on automated processing with the impact of having legal effects on him or her.[143] The GDPR offers three exceptions to this, if the data is (1) necessary for entering into a contract, (2) is authorized by the Union or Member State law, or (3) is based on data subject's explicit consent.[144]

In addition to the explicit rights stated in the regulation, the GDPR contains an express provision that holds the entire regulation applicable to controllers or processors' means of processing personal data for household and personal activities.[145] This includes, but is not limited to, social networking or online activity.[146] Though this statement is brief, the umbrella effect of the GDPR is fully applicable to all internet user activity taking place in the European Union.[147]

Children are subject to specific and enhanced protection under the GDPR.[148] Any information being directed to a child must be delivered in a clear and plain manner that can be easily understood.[149] The GDPR defines children as individuals under the age of eighteen.[150] Although children are defined as individuals under the age of eighteen, the age of consent for processing of personal data is sixteen.[151] If the child is below the age of

---

137 Council Regulation 2016/679, *supra* note 8, at 45.
138 *Id.*
139 *Id.*
140 *Id.*
141 *Id.*
142 *Id.* at 46.
143 Council Regulation 2016/679, *supra* note 8, at 46.
144 *Id.*
145 *Id.* at 3-4.
146 *Id.*
147 *Id.* at 4.
148 *Id.* at 11.
149 Council Regulation 2016/679, *supra* note 8, at 11.
150 *Children and the UK GDPR*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/ (last visited Sept. 14, 2021).
151 Council Regulation 2016/679, *supra* note 8, at 37.

sixteen, then data processing is only lawful when parents or guardians have given consent.[152]

The GDPR considers biometric data a special category of personal data.[153] Under the GDPR, biometric data means "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images."[154] Biometric data can be categorized in two groups: bodily characteristics and behavioral information.[155] Bodily characteristics are physical or physiological traits.[156] Behavioral characteristics are more broad and can potentially include any personal actions of an individual.[157]

Under the GDPR, Biometric data cannot be processed for the purpose of identifying a natural person's health.[158] Furthermore, the GDPR explicitly states that biometric data may not be used unless the data subject has given clear consent.[159] Merely having a legal basis to process biometric data is not sufficient.[160] The GDPR requires a privacy impact assessment to be performed by data controllers before conducting any type of processing for biometric data.[161] This is because biometric data is highly sensitive and a high risk subject in privacy law.[162]

Additionally, by using the GDPR as a broad guideline for biometric data standards, member states within the European Union have the discretion to create further restrictions on use of genetic data, biometric data, or data concerning health in the European Union.[163]

Since the GDPR is broad in scope and applies to all types of companies, it allows data subjects[164] to bring private rights of action under a broad

---

152 *Id.*

153 *Id.* at 38-39.

154 *Id.* at 34.

155 Danny Ross, *Processing Biometric Data? Be Careful,* [sic] *Under the GDPR*, IAPP (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/.

156 *Id.*

157 *Id.*

158 Council Regulation 2016/679, *supra* note 8, at 38.

159 Jeremy Dunn, *Managing Biometric Data: The GDPR's Requirements*, IRON MOUNTAIN (Oct. 16, 2018), https://www.ironmountain.com/blogs/2018/managing-biometric-data-the-gdprs-requirements.

160 Ross, *supra* note 155.

161 *Id.*

162 *Id.*

163 Council Regulation 2016/679, *supra* note 8, at 39.

164 A data subject is:

> [A]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

category of circumstances.[165] In any event where there is a failure to comply with the GDPR, a private action may be commenced, and the relief received will be limited to compensation for the damages that are suffered by the data subject.[166] This includes material, or non-material, damage as a result of the infringement.[167]

D. The Invasion of Privacy Torts: Publicity Given to Private Life and Intrusion Upon Seclusion

As mentioned in the introduction, this note will focus on various private actions against social media platforms. The main claim plaintiffs bring in these actions is the tort claim of invasion of privacy.[168] Specifically, publicity given to private life and intrusion upon seclusion.[169] When proving publicity given to private life, a plaintiff must show that "one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[170]

To prove intrusion upon seclusion, a plaintiff must show that: "(1) the defendant intentionally invaded the private affairs of the plaintiff, without authorization; (2) the invasion would be offensive to a reasonable person; (3) the matter the defendant intruded upon involved a private matter; and (4) the intrusion caused mental suffering to the plaintiff."[171] The case that is the focus of this note is *In Re: TikTok, Inc., Consumer Privacy Litigation* ("*In Re: TikTok*").[172] This case involved a consolidated class action for a private right of action for online privacy in relation to the popular social media platform and app, TikTok.[173] *In Re: TikTok* also addressed how the inclusion

---

Regulation 2016/679, art. 4, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119 27.04.2016), 1.

165 *Id.* at 81 (applying to both privately held and publicly held companies, rendering any activity that may reach an audience in the European Union or business activities relating to any ties with the European Union subject to this regulation).

166 Christian M. Auty, *GDPR Privacy FAQs: Is There a Private Right of Action for Failing to Comply with European Cookie Laws?*, BRYAN CAVE LEIGHTON PAISNER (Aug. 9, 2019), https://www.bclplaw.com/en-US/insights/gdpr-privacy-faqs-is-there-a-private-right-of-action-for-failing.html.

167 Council Regulation 2016/679, *supra* note 8, at 81.

168 Class Action Complaint at 2-3, Tellone v. TikTok, Inc., No. 20-cv-03771 (N.D. Ill. filed June 26, 2020).

169 *Id.*

170 RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1975).

171 *Id.*

172 Consolidated Amended Class Action Complaint, *supra* note 52.

173 *Id.*

of minors in the suit increases the severity of such a cause of action.[174] Plaintiffs brought this action under the Illinois Biometric Information Privacy Act.[175]

IV. ANALYSIS

A. What is TikTok?

In August 2018, ByteDance launched the now popular social media platform and app, TikTok (formerly known as Musical.ly) in the United States.[176] The app's popularity increased rapidly in 2019 and reached its first peak number of over eight hundred million users worldwide amid the COVID-19 pandemic in 2020.[177] As of late September 2021, TikTok has one billion active users globally[178] and one hundred and thirty million monthly active users in the United States.[179] Of the one hundred and thirty billion users in the United States, twenty-five percent are between the ages of ten and nineteen.[180] The social media's primary function is to create up to sixty-second videos which range from home improvement tips, quick and easy recipes, lip-syncing, dance videos and much more.[181] Users are able to create these videos and potentially "go viral" through the app's embedded artificial intelligence ("AI") tools and public video sharing feature.[182] Users have the option to share TikTok Videos ("TikToks") both within the app and outside of it, such as through text message or Snapchat.[183]

B. TikTok's Privacy Policies

TikTok's privacy policies vary depending on which country users are located in. Different privacy policies apply to the United States, the European

---

174 *Id.*

175 *Id.* at 4.

176 Rebecca Fannin, *The Strategy Behind TikTok's Global Rise*, HARV. BUS. REV. (Sept. 13, 2019), https://hbr.org/2019/09/the-strategy-behind-tiktoks-global-rise.

177 Consolidated Amended Class Action Complaint, *supra* note 52, at 1.

178 Jessica Bursztynsky, *TikTok Says 1 Billion People Use the App Each Month*, CNBC (Sept. 27, 2021, 11:49 AM EDT), https://www.cnbc.com.

179 Brandon Doyle, *TikTok Statistics—Updated Sep* [sic] *2021*, WALLAROO (Sept. 27, 2021), https://wallaroomedia.com/blog/social-media/tiktokstatistics/#:~:text=Monthly%20Active%20Users%20in%20the,and%2028.8%20million%20in%20March.

180 *Distribution of TikTok Users in the United States as of March 2021, by Age Group*, STATISTA, https://www.statista.com/statistics/1095186/tiktok-us-users-age/ (last visited Dec. 14, 2021).

181 Consolidated Amended Class Action Complaint, *supra* note 52, at 1.

182 *Id.* at 2-3.

183 *Sharing*, TIKTOK, https://support.tiktok.com/en/using-tiktok/exploring-videos/sharing (last visited Dec. 14, 2021).

Economic Area ("EEA"),[184] the United Kingdom ("UK"),[185] and Switzerland.[186] If a user does not reside in any of the above listed countries, then a completely different privacy policy applies which will be discussed in detail.[187] Every TikTok privacy policy mentions that any legal action that is commenced against the social media platform, must be solved through arbitration.[188] However, there are exceptions.[189] The arbitration clause does not apply when minors are involved and are at the center of privacy violations.[190]

C. TikTok Privacy Policies in the United States

Under TikTok's privacy policy in the United States, there are two main categories of information collected: information users choose to provide and information that is collected automatically.[191] For users who are over the age of thirteen, TikTok gathers information (1) provided by users when first creating an account, (2) data shared from third-party social networks, and (3) technical and behavioral information about a user's activity on the platform.[192] The user must grant TikTok the right to obtain this information.[193] TikTok also collects information contained in messages sent by users and information from users' phones which the user has granted TikTok access.[194] The social media platform also has access to user generated content which includes comments, photographs, videos, and content that is uploaded or broadcasted on the platform.[195] In addition to user information and content, TikTok also has access to third-party payment information and users' personal contacts.[196] It is important to note that the aforementioned categories of information are granted by users themselves, just by utilizing the platform.[197]

---

184 The European Economic Area includes the European Union, Iceland, Liechtenstein, and Norway. *Countries in the EU and EEA*, GOV.UK, https://www.gov.uk/eu-eea (last visited Dec. 14, 2021).

185 *Privacy Policy*, TIKTOK (June 2, 2021), https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-us.

186 *Id.*

187 *Id.*

188 *Id.*

189 Bobby Allyn, *Class-Action Lawsuit Claims TikTok Steals Kids' Data and Sends it to China*, NPR (Aug. 4, 2020, 1:39 PM ET), https://www.npr.org/2020/08/04/898836158/class-action-lawsuit-claims-tiktok-steals-kids-data-and-sends-it-to-china.

190 *Id.*

191 *Privacy Policy*, *supra* note 185.

192 *Id.*

193 *Id.*

194 *Id.* (including a user's photos, videos, and phone contacts).

195 *Id.*

196 *Id.*

197 *Privacy Policy*, *supra* note 185.

The second category of data collected is information that is obtained automatically by the social media platform.[198] This includes internet activity, the user's IP address, geolocation-related data, as well as, browsing and search history.[199] This information is transmitted to website servers almost immediately.[200] However, there are regulations in place requiring users to consent to cookies by accepting them or rejecting them.[201]

Overall, TikTok's privacy policies state that the purpose for collecting user data is to improve the users' experiences.[202] This includes general functionalities of the app, showing suggestions, promoting the platform, and customizing the ad experience; however, it seems that the collecting of user data is more favorable to TikTok than its users. Although this includes the general functionalities of the app—showing suggestions, promoting the platform, and customizing the ad experience—the real reason behind the collection of user data seems to be more favorable to the platform and not its users.[203]

D. TikTok's Privacy Policies in the United States as Applied to Minors

TikTok has an additional privacy policy for users under the age of thirteen.[204] The primary purpose of this separate privacy policy is to limit the extent of general data collection on minors.[205] The content children choose

---

198 *Id.*

199 Unfortunately, these are not the only pieces of information collected by TikTok. *Id.* The platform collects information on cookies as well as unique identifiers for the device being used. *TikTok Platform Cookies Policy*, TIKTOK (Nov. 5, 2020), https://www.tiktok.com/legal/cookie-policy?lang=en. The Federal Trade Commission simply defines a cookie as information saved by your web browser. *Internet Cookies*, FED. TRADE COMM'N (May 2021), https://www.ftc.gov/site-information/privacy-policy/internet-cookies.When a user visits a website, the site may place cookies on a user's web browser so it can recognize the device in the future. *Id.* Many, if not all, websites require permission to accept cookies. *Id.* Cookies transmit information, including pages viewed and activities on a website, back to a website's server. *Id.* Additionally, the site recognizes its users, customizes the browsing experience, and delivers targeted ads through cookies. *Id.*

200 *Privacy Policy*, *supra* note 185.

201 *Id.*

202 *Id.*

203 TikTok's approach in justifying collection of data for "user experience" is interesting. The policies make it seem like data is being collected for the benefit of its users and not the platform. *Id.* However, the platform lists reasons under its privacy policies which all seem to benefit the platform. *Id.* These reasons include platform functionality, support, and internal operations which include troubleshooting, data analysis, testing, research, and others. *Id.* Furthermore, one of the main reasons for using user data is to send promotional materials and targeted ads. *Id.* The list goes on to describe advertising and marketing purposes in other words, as well as to generally "inform algorithms" and vaguely mention the use of use of data for "any other purposes" that are disclosed to individuals using the platform at the time data is collected or pursuant to user consent. *Id.*

204 *Id.*

205 *Privacy Policy for Younger Users*, TIKTOK (Jan. 2020), https://www.tiktok.com/legal/privacy-policy-for-younger-users?lang=en (allowing younger users to view videos and content from other creators while still having the option to create their own videos).

to create may be saved to their devices, but the videos will not be saved or viewable by TikTok or other users.[206] In addition to this, users cannot exchange messages with or view the profiles of users' under the age of thirteen.[207] The information collected on minor users includes their username, password, and birthday as well as network activity information (i.e., the device ID, IP address, web browser type and version, country-level location, and certain app activity data).[208]

There are many similarities between data collection on users over the age of thirteen to the data collection on users under the age of thirteen. The only difference in type of data collected by TikTok is that behavioral and technical user activity is absent from data collection for users under the age of thirteen.

TikTok's purpose for collecting minor users' data is not much different than its purpose for collecting data of users over the age of thirteen. TikTok's privacy policies explicitly state that the information collected on users under thirteen is to "provide personalized content, targeted advertising, perform analytics and troubleshoot, and protect the security or integrity and ensure legal or regulatory compliance."[209] When protecting user data for users under the age of thirteen, TikTok does not guarantee complete security of data that is transmitted through the internet.[210] But, the platform does ensure that it does not sell the information of users under the age of thirteen to third parties.[211]

E. TikTok's Privacy Policies in the European Economic Area, United Kingdom, and Switzerland

Similar to the policy for users in the United States, TikTok's privacy policy for European territories includes the information collected when a user creates an account as well as technical and behavioral information.[212] TikTolk also collects and processes messages, which includes the scanning and analysis of that information where local laws allow it to do so.[213] TikTok automatically processes and shares third-party information from users' accounts.[214] For purposes of data collection, TikTok provides the same

---

206 *Id.*

207 *Id.*

208 This differs from the information collected on users above the age of thirteen which also includes behavioral and technical information pertaining to user activity. *Id.* Furthermore, the category of "app activity data" includes video watches, time in the app, and vague general usage data. *Id.*

209 *Id.*

210 *Id.*

211 *Privacy Policy for Younger Users*, *supra* note 205.

212 *Id.*

213 *Id.*

214 *Id.*

reasons as it does in the policy used in the United States to access and process users' data and activity.[215] TikTok only shares personal data with third parties when the user chooses to register for the app with another social network site or if the user grants that permission.[216] However, unlike United States users, TikTok provides EEA users with explicit rights such as access to data, deletion of data, changing or correcting data, portability of data, objection or restriction of data, and withdrawal of consent.[217] These rights are clearly mentioned under the privacy policy to ensure compliance with this region's privacy laws.[218]

F. Consumer Privacy Litigation

1. In Re: TikTok.

The main case discussed in this note is *In Re: TikTok, Inc., Consumer Privacy Litigation* ("*In Re: TikTok*").[219] This case originates from over twenty separate actions—consolidated into this single class action—commenced in 2020 based on an alleged biometric privacy breaches.[220] The majority of the plaintiffs in this action are minors represented by their guardians.[221] As with all social media platforms, such as Facebook and Instagram, there are many costs and benefits associated with giving individuals the power to express themselves and share information through creative means on TikTok. *In Re: TikTok* is another example of what the costs associated with social media are.[222] Specifically, the collection and utilization of "highly sensitive and immutable biometric identifiers and information."[223]

This action was brought under the Illinois Biometric Privacy Act ("BIPA").[224] The premise of the plaintiffs' complaint is that TikTok is collecting, using, and storing user's facial geometry through certain visual features and effects.[225] The complaint alleges that TikTok is doing so without

---

215 *Id.* The purposes of data collection include user support, troubleshooting, personalizing content, enabling interaction with other users, communicating with users, promoting popular topics, provide advertising and promotion of products. *Id.*

216 *Id.*

217 *Privacy Policy for Younger Users*, *supra* note 205.

218 *Id.*

219 *In re* TikTok, Inc., Consumer Priv. Litig., No. 20-cv-4699, 2021 WL 4478403 (N.D. Ill. Sept. 30, 2021).

220 *Id.*

221 Consolidated Amended Class Action Complaint, *supra* note 52, at 5-19.

222 *See generally* Lauraann Wood, *$92M TikTok Privacy Deal Gets Ill. Jude's Early OK*, LAW360 (Oct. 1, 2021, 9:13 PM EDT), https://www.law360.com/articles/1427169.

223 Consolidated Amended Class Action Complaint, *supra* note 52, at 4.

224 *Id.* at 3.

225 *Id.*

disclosure or the parental consent of minor users.[226] The complaint further alleged that TikTok is sending this data to ByteDance in China, which is a direct violation of the BIPA.[227] The plaintiffs allege that TikTok further failed to disclose why they collect, use, and store this biometric data; who has access to the data; and how long the data will be held in possession—all of which are required by the BIPA.[228] Plaintiffs seek (1) injunctive and equitable relief as is necessary to protect the interests of the Plaintiffs and the members of the class action by requiring Defendants to comply with the BIPA; (2) statutory damages of five thousand dollars for each intentional and reckless violation of the BIPA or alternatively statutory damages of one thousand dollars for each negligent violation; and (3) reasonable attorneys' fees and costs and other litigation expenses.[229] The goal of this suit is to prohibit TikTok from continuing to engage in these unlawful acts, omissions, and practices.[230]

A significant factor to this action is that none of the minor plaintiffs, nor their guardians, recall seeing or reviewing the terms of service, privacy policy, or privacy policy for younger users upon creating their TikTok accounts.[231] Moreover, the Plaintiffs allege this "Privacy Policy for Younger Users" is ineffective at times since the reported ages and birthdates used to create accounts by users can be falsified and are not verified by the platform.[232]

One of the main factual allegations in this case is that TikTok collects and stores geo-location-related data.[233] This is noted in the U.S. privacy policies, but the seriousness of this data collection is not addressed as location data is one of the most sensitive personal pieces of information that a user can share with a company.[234] The average smartphone used by Americans tracks more than the street address at which the user is located—it is able to identify which floor in the building the user can be found.[235]

---

226 *Id.* at 83.

227 *See id.* at 51 (citing David Carroll, *Is TikTok a Chinese Cambridge Analytica Data Bomb Waiting to Explode*?, QUARTZ (Aug. 5, 2019), https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/); Jack Nicas et al., *TikTok Said to be Under National Security Review*, N.Y. TIMES (Aug. 7, 2020), https:www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

228 Consolidated Amended Class Action Complaint, *supra* note 52, at 111-12.

229 *Id.* at 114.

230 Class Action Complaint, *supra* note 168, at 29-30.

231 *Id.* at 2-3; *see also* Consolidated Amended Class Action Complaint, *supra* note 52, at 5-19.

232 Class Action Complaint, *supra* note 168, at 11.

233 *Id.* at 8-9.

234 *Id.* at 10 (citing Letter from Christophe Coons, U.S. Sen., and Josh Hawley, U.S. Sen., to Mark Zuckerberg, Chief Exec. Officer of Facebook, Inc. (Nov. 19, 2019) (on file at https://www.coons.senate.gov/imo/media/doc/11.19.19%20FB%20Letter%20FINAL%20(signed).pdf)).

235 *Id.*

The biometric data that has been collected and stored by TikTok without consent or disclosure and it is important to note that this collection is automatic.[236] The technology of the platform allows instant capturing of biometric data which is then used to engage in facial recognition for filters and even allowing users to select an individual's face in a video to identify other videos in which that user appears in.[237] Although these practices are direct violations of the BIPA, the platform collects facial geometry for its algorithms while indicating a failure to comply with the BIPA.[238] The algorithms create targeted content, features, and effects which become addictive for users, resulting in prolonged hours on the platform in comparison to other social media apps such as Facebook, Twitter, Instagram, and Snapchat, where users eventually run out of content to view.[239]

A primary feature that uses biometric identifiers are face filters.[240] To use face filters, the app will scan and map the user's face through the smartphone or tablet's camera then apply the desired filter.[241] These filters include categories like "trending," "funny," and "animals."[242] It was reported that a feature existed that allowed users to superimpose other users facial features on top of their own and record videos with it as a face filter.[243] Clearly, this specific feature, known as "deepfake," can pose serious security issues since it is using two individuals' biometric face scans and is manipulating both identifiers to share it with the entire platform's users.[244] In additions to TikTok's facial recognition capabilities, it is alleged that the platform also has voice recognition tools that can be used to identify certain users and manipulate their words on the app.[245] The algorithm used to collect and use such information was developed and patented by ByteDance in China.[246]

It is important to remember that this case involves minors whose biometric identifiers and information were collected, stored, and used by TikTok.[247] Minors make up a large percentage of the TikTok's user

---

236 Consolidated Amended Class Action Complaint, *supra* note 52, at 38-39.

237 *Id.*

238 *Id.* at 14.

239 *Id.*

240 *Id.* at 14-15 (citing *How Camera Face Filters Brought TikTok Millions of Users*, BANUBA (Sept. 3, 2019), https://medium.com/@banuba/how-camera-face-filters-brought-tiktok-millions-of-users-4081f885f81c).

241 *Id.* at 15.

242 Class Action Complaint, *supra* note 168, at 15 (citing Peter Suciu, *TikTok's Deepfakes Just the Latest Security Issue for the Video Sharing App*, FORBES (Jan. 7, 2020, 3:22 PM EST), https://www.forbes.com/sites/petersuciu/2020/01/07/tiktoks-deepfakes-just-the-latest-security-issue-for-the-video-sharing-app/?sh=fd6b0a370a21).

243 *Id.*

244 *Id.*

245 *Id.* at 16.

246 *Id.*

247 *Id.*

demographic.[248] As of September 2020, TikTok classified more than one third of its forty-nine million users in the United States as being fourteen years old or younger.[249] The COPPA, as discussed earlier,[250] requires internet platforms to obtain parental consent before collecting personal information on children under the age of thirteen.[251]

In 2019, the FTC commenced an action against TikTok under the COPPA.[252] The settlement resulted in TikTok paying $5.7 million in restitution damages for the company illegally collecting personal information from children.[253] TikTok's primary violation was failing to seek parental consent before collecting names, email addresses, and other personal information from children under the age of thirteen, and failing to delete children's information at the request of parents and legal guardians.[254] As a result of this litigation, TikTok was required to comply with the COPPA and to take down all videos made by children under the age of thirteen.[255]

Journalists' investigations revealed that sexual predators have used TikTok as an ideal means to connect with children.[256] These reports revealed that sexually explicit comments were left on teenagers' videos.[257] As a result, a High Court of India and India's Ministry banned the app from its country.[258] In May 2020, subsequent the $5.7 million settlement in the United States and TikTok being banned in India, a group of twenty advocacy groups filed a complaint alleging that TikTok continued to violate the COPPA.[259] Specifically, that all user data for individuals under the age of thirteen was not deleted.[260] The complaint by the advocacy groups further alleged that

---

248 Class Action Complaint, *supra* note 168, at 16.

249 Raymond Zhong & Sheera Frenkel, *A Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions*, N.Y. TIMES (Sept. 17, 2020), https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html.

250 *See supra* Section III.A.3.

251 *See supra* Section III.A.3.

252 Press Release, Fed. Trade Comm'n, FTC Obtains Largest Monetary Settlement in a COPPA Case (Feb. 27, 2019) (on file at https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc).

253 *Id.*

254 *Id.*

255 *Id.*

256 Class Action Complaint, *supra* note 168, at 19 (citing Marco Silva, *Video App TikTok Fails to Remove Online Predators*, BBC: BBC TRENDING (Apr. 5, 2019), https://www.bbc.com/news/blogs-trending-47813350?mod=article).

257 *Id.*

258 *Id.* (citing Rishi Iyengar, *India's Two-Week Ban Cost TikTok 15 Million Users*, CNN BUSINESS (May 2, 2019), https://www.cnn.com/2019/05/02/tech/tiktok-ban-india-users/index.html (discussing a court's reversal of its order after TikTok appealed the decision, arguing that it had removed the inappropriate content)).

259 CAMPAIGN FOR A COMMERICAL-FREE CHILDHOOD ET AL., COMPLAINT AND REQUEST FOR INVESTIGATION OF TIKTOK FOR VIOLATION OF THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT AND IMPLEMENTING RULE 1-2 (2020), https://commercialfreechildhood.org/wp-content/uploads/2020/05/tik_tok_complaint.pdf.

260 *Id.*

TikTok unnecessarily collects information beyond its scope of operations and shares it with third parties.[261]

Defendants responded to the heart of the allegations stating that the app does not capture biometric identifiers and information and users' data is not sent to China.[262] This appears to be inconsistent with the information discovered during the investigation of this case.[263] TikTok also asserts that even if they wanted to capture biometric information and send that data to China, they have the right to do so.[264] Based on the numerous actions commenced resulting in this class action, this may not be true.[265] Final judgment in this matter has not been entered; there is a Fairness Hearing on Plaintiffs' anticipated Motion for Final Approval of Class Action Settlement set for May 18, 2022.[266]

2. Lawsuits Filed Against Other Social Media and Internet Platforms

TikTok is not the only social media platform to be sued for alleged violations of the BIPA.[267] In 2018, three separate actions were brought by Illinois residents alleging that Facebook unlawfully collected and stored biometric data derived from users' faces.[268] Facebook has long allowed users to "tag" others in the photos that they upload.[269] In 2010, Facebook introduced a new feature called "Tag Suggestions."[270] If enabled, this feature will use facial-recognition technology to determine if the user's Facebook friends are in a photo and if so, Facebook will suggest tagging that friend.[271] The technology works by comparing various geometric data points (i.e., the distance between facial features) from the faces in uploaded photos and compares that to Facebook's database of "user face templates."[272] Facebook

---

261 This information includes videos, usage history, content of the messages sent between users on the platform, and geolocation, all of which were obtained without consent and all were categories of information that were not needed to run the operations of the app. *Id.*

262 Allyn, s*upra* note 189.

263 *Id.*

264 *Id.*

265 *See generally In re* TikTok, Inc., Consumer Priv. Litig., No. 20-cv-4699, 2021 WL 4478403 (N.D. Ill. Sept. 30, 2021).

266 *Upcoming Court Proceedings*, *MDL 2948: In Re TikTok, Inc., Consumer Priv. Litig.*, U.S. DIST. CT. N. DIST. ILL., https://www.ilnd.uscourts.gov/mdl-details.aspx?i3mxb9gEBxL2sL90OMEQ2A== (last visited Dec. 20, 2021).

267 Butler Snow LLP & Melonie Wright, *"Face It"—Snapchat, Facebook, and Google Deal with Suits Over Facial Recognition Technology*, JDSUPRA, https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=e9adbd67-9e33-490b-ba09-ea8871f7e4ec#:~:text=Snapchat%2C%20Facebook%2C%20and%20Google%20have,740%20ILCS%2014%2F10 (last visited Dec. 19, 2021).

268 Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

269 *Id.* at 1267.

270 *Id.* at 1268.

271 *Id.*

272 *Id.*

will create a face template for a user if that user "(1) has been tagged in at least one photo; (2) has not opted out of Tag Suggestions; and (3) satisfied other privacy-based and regulatory criteria."[273]

The plaintiffs alleged that Facebook "collecting using, and storing biometric identifiers" from users' photos without users' knowledge or consent, was a violation of the BIPA and in turn a violation of Illinois residents' privacy rights.[274]

This lawsuit was eventually classified as a class action suit which allowed Facebook users to join the action and seek recovery of damages for the alleged invasion of their privacy rights.[275] Facebook argued that the BIPA was being used outside of its established territory as users who were not residents of Illinois were allowed to seek recovery under the class action.[276] The court rejected this argument stating that as long as the plaintiffs used Facebook while in the state of Illinois and the activities occurred primarily and substantially in the state, then the application of the BIPA, in this case, is nationwide.[277] This broad application makes it easier to protect the data and interests of American consumers.[278] In January 2020, Facebook was ordered to pay Illinois users five hundred and fifty million dollars for violating their privacy rights under the BIPA through the facial tagging feature.[279]

Social media platforms are not the only internet entities notorious for violating privacy laws. In 2010, Google notified the public of using its Street View feature as a means to collect user passwords, e-mails, and other personal information.[280] Street View is an extension of Google maps which allows users to search for a location and have a picture of the location appear in the results.[281] In response to this discovery being brought to light, Google stated that the collection was an accident.[282] As a result, Street View was banned from the Czech Republic and Germany allowed its citizens the option of opting out of this feature.[283] After nearly a decade of litigation,[284] Google

---

273 *Id.*

274 Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

275 Ally Marotti, *Facebook Could be Forced to Pay Billions of Dollars Over Alleged Violations of Illinois Biometrics Law*, CHI. TRIB. (Apr. 17, 2018, 4:20 PM), https://www.chicagotribune.com/business/ct-biz-facebook-tagging-privacy-lawsuit-20180417-story.html.

276 Patel v. Facebook, Inc., 932 F.3d 1264.

277 *Id.*

278 *Id.*

279 *Id.*

280 Doug Gross, *What Google's Street View Breach Means for Your Privacy*, CNN (Oct. 26, 2010, 4:28 PM EDT), https://www.cnn.com/2010/TECH/web/10/26/google.street.view/index.html.

281 *Id.*

282 *Id.*

283 *Id.*

284 Consolidated Class Action Complaint, *In Re* Google, Inc. Street View Electronic Communications Litigation, 794 F. Supp. 2d 1067 (N.D. Cal. 2011) (No. C 10–MD–02184).

was ordered to pay a thirteen million dollar settlement to the original twenty-two plaintiffs and were ordered to delete the data obtained from Street View.[285]

VI. PROPOSED SOLUTION

Based on *In Re: TikTok*, the United States' federal government should consider enacting a comprehensive data security statute while allowing states to impose their own broader restrictions. This section will offer a proposal, for a potential federal statute, that will use the key provisions of the GDPR[286] and the Consumer Online Privacy Rights Act ("COPRA"), proposed by Senator Maria Cantwell, as a model. This solution will outline the essential components necessary for comprehensive privacy legislation. If the United States had a federal privacy law as strict as the GDPR could the entire class action suit against TikTok have been avoided? The answer is more likely than not.

First, the statute should state its purpose. Following the GDPR, the purpose of this statute is to protect individuals in relation to the processing of personal data.[287] The application of this statute would extend to data processors and businesses in the United States and to actors located internationally.[288] Ideally, the statute would recognize protection of personal data as a vital piece in American lives and violations of citizens' privacy would be subject to severe penalties, such as heavy fines. In addition to administrative fines, the proposed legislation, ideally, would give individuals the right to commence a private action.[289]

Next, the proposed statute should delegate an agency under an already existing federal agency to overlook the new comprehensive privacy law, perhaps under the FTC based on its previous enforcements of other federal privacy acts. Ideally, the proposed statute would create an agency under the FTC since privacy law covers many areas. The creation this agency would ensure effectiveness and quickness in creating and implementing regulations since the FTC is familiar with privacy to a certain extent. Currently, the FTC is responsible for overseeing data protection matters.[290] However, the FTC's

---

285 *Google Agrees to Pay $13 Million In Street View Privacy Case*, CBS SF BAYAREA (July 22, 2019, 2:00 PM), https://sanfrancisco.cbslocal.com/2019/07/22/google-street-view-privacy-lawsuit-settlement; *see also* Alaina Lancaster, *Judge Approves $13M Google Street View Privacy Settlement with No Payout to Class*, LAW.COM: THERECORDER (Mar. 19, 2020, 7:02 PM), https://www.law.com/therecorder/2020/03/19/judge-approves-13m-google-street-view-privacy-settlement-with-no-payout-to-class/.

286 Council Regulation 2016/679, *supra* note 8.

287 *Id.*

288 *Id.* at 22.

289 *Id.* at 81.

290 *Id.*

primary purpose is to investigate and prevent unfair methods of competition and unfair or deceptive practices affecting commerce.[291] It is fair to say that data protection does not necessarily fall into the FTC's duties based on its primary purpose.[292] Therefore, the new agency within the FTC would be able to focus specifically on regulating data protection.[293]

The internet is used in nearly every aspect of U.S. citizens' lives including education, banking, healthcare, media, and socializing—there is a platform for every activity in people's lives. Generation Z and Generation Alpha are the generations who are the most active on social media.[294] Due to this strong presence in households, especially with the increase in minor users, the new legislation should have a special provision pertaining to children. Children are the most vulnerable individuals subject to breach in data protection and privacy.[295] They are particularly vulnerable to the social media platforms and internet sites they visit.[296] Children may be less aware of privacy risks and not able to comprehend privacy policies and user data as well as adults. So, there must be a consent provision in the proposed bill that requires parents to consent on behalf of their children. The proposed bill should also contain an opt out provision for any type of data collection. There should also be transparent language on the website or social media platform so that the information is easily understandable.[297] Additionally, there should be increased penalties for violating this statute when children are involved. It would also be beneficial to include a section on how this new statute would interact with the COPPA, specifically regarding penalties.[298]

In addition to the specific sections for addressing children's data protection, the legislation should also include a section on biometric data. Biometric data is present across all social media platforms.[299] The proposed federal statute should use both the GDPR's approach to biometric data and the BIPA as its model. The unlawful processing of biometric data should also

---

291 *About the FTC*, *supra* note 32.

292 *Id.*

293 Data protection would include oversight of this new legislation as well as other federal substantive privacy acts discussed earlier in this Note such as HIPAA, GLBA, and COPPA.

294 Generation Z consists of individuals born in 1997 to early 2010 and Generation Alpha consists of individuals born in 2010 and onwards. *See Gen Z and Gen Alpha Infographic Update*, MCCRINDLE, https://mccrindle.com.au/insights/blogarchive/gen-z-and-gen-alpha-infographic-update/ (last visited Dec. 19, 2021); *Distribution of TikTok Users in the United States as of March 2021, by Age Group*, *supra* note 180.

295 *General Questions About the COPPA Rule*, *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

296 *Id.*

297 Council Regulation 2016/679, *supra* note 8, at 11.

298 15 U.S.C. §§ 6501-08.

299 IDmission Team, *The Importance of Biometric Authentication Across Social Media Channels*, IDMISSION (Feb. 19, 2021, 8:22:36 AM), https://www.idmission.com/en/blog/the-importance-of-biometric-authentication-across-social-media-channels.

be subject to higher penalties, due to its highly sensitive and confidential nature.[300] This would allow biometric data to be recognized as a special category of personal data under federal law. Individual states would have the discretion to impose further limitations and penalties concerning biometric data.[301]

On top of businesses being subject to strict regulation concerning data collection, social media platforms should have privacy policies in place that comply with this new comprehensive privacy statute. Just as TikTok's privacy policies in Europe express individuals' rights to access to data, deletion of data, changing or correcting data, portability of data, objection or restriction of data, and withdrawal of consent, the United States should have the same policy in place. This new federal statute would have the ability to increase and ensure protection of users on all social media platforms. As analyzed earlier in this note, TikTok users' rights are well protected under the GDPR and a similar legislative approach should be taken by the United States federal government.

Until there is a comprehensive federal statue in place, states should begin to introduce privacy statutes for their own citizens. Currently, the CCPA is the most refined comprehensive privacy statute in effect in the United States.[302] Although the BIPA has serious consequences for privacy violations through its strict enforcement, it does not cover all aspects of privacy law.[303] More states adopting comprehensive privacy statutes will bring more awareness of the need for a federal statute to be enacted.

Finally, people should be able to recover damages for the harm they have suffered from privacy violations. A private right of action should be included in both federal and state privacy laws. This would serve as a way to compensate the victims, as well as deter future privacy violations. There may be pushback from those who oppose the legislation due to its strict nature in regulating businesses. However, this statute would be a significant step in protecting individuals' personal and immutable information which outweighs the burdens imposed on businesses.

While the proposed solution offers citizens more protection as to personal data and the ability to bring a private action in the right

---

300 The BIPA is one of the strictest biometric privacy laws in the United States, providing the utmost protection and recovery for citizens. 740 ILL. COMP. STAT. 14/20 (2008); *see also* Bilzin Sumberg et al., *As Florida Mulls New Privacy Protections, Facebook Takes Hit in Illinois for Biometric Data Collection*, JDSUPRA (Mar. 5, 2021), https://www.jdsupra.com/legalnews/as-florida-mulls-new-privacy-1027799/#:~:text=BIPA%20is%20among%20the%20strictest,class%20action%20lawsuits%20in%20Illinois.

301 Council Regulation 2016/679, *supra* note 8, at 39.

302 *See* Lock Lord LLP & Theodore Augustinos, *Privacy Laws Begin to Ripple Across the States Following the California Consumer Privacy Act*, JDSUPRA (Mar. 12, 2021), https://www.jdsupra.com/legalnews/privacy-laws-begin-to-ripple-across-the-1707016/.

303 740 ILL. COMP. STAT. 14/1-99 (2008).

circumstances, there are also implications involved. The most significant implication may be that consumers will begin to commence frivolous suits once they find out that collection and utilization of personal and biometric may be compromised. How could this be prevented or mitigated? Under the new comprehensive privacy law, a provision should be included which gives states the power to cap the amount recovered per person on an annual basis. Without a limitation of some kind, businesses—particularly small businesses—will face potential hardships due to lack of financial means to remediate such breaches if they were to occur.

VI. CONCLUSION

In light of the numerous class action suits against social media platforms and the advancement of privacy laws around the world, there is a great need for a comprehensive privacy statute in the United States. If the United States had a federal privacy law as strict and comprehensive as the European Union's, it appears that it is more likely than not that the class action lawsuit against TikTok could have been avoided. Implementing a comprehensive privacy statute will help ensure further protection of personal information, compliance with regulations already in place, and emphasize the value of personal information that should remain private. The United States should follow the lead of the Europe Union, in enacting the GDPR, to maintain pace with the advancement in technology and the growing use of social media.