# RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY

*Lauren D. Godfrey, Suzie Allen, Catherine Geisler, Joy Momin, Elisabeth Axberger, Pahoua Thao, Tara Kennedy, Lindsey Knapton, Ali Cabeza, Josh Hansen, Robert A. Stines, and Anna A. Gadberry*

I. U.S. and EU Statutory Developments ..... 175
A. United States and International Statutory Developments, by Lauren D. Godfrey, Suzie Allen, and Catherine Geisler ..... 175
1. United States State Developments ..... 175
2. Developments Outside the United States ..... 185
II. Developments in Artificial Intelligence ..... 197
A. Statutory Developments in Artificial Intelligence, by Pahoua Thao ..... 197

*Lauren D. Godfrey is a Partner in the Cybersecurity & Data Privacy Practice Group of Constangy, Brooks, Smith & Prophete, LLP. Suzie Allen is an Attorney in the Cybersecurity & Data Privacy Practice Group of Constangy, Brooks, Smith & Prophete, LLP. Catherine Geisler is an Attorney in the Cybersecurity & Data Privacy Practice Group of Constangy, Brooks, Smith & Prophete, LLP. Elisabeth Axberger is an Associate in the Cybersecurity & Data Privacy Practice Group of Wilson Elser Moskowitz Edelman & Dicker LLP. Pahoua Thao is an attorney at Stafford Rosenbaum LLP. Tara D. Kennedy is an attorney in Shook, Hardy & Bacon L.L.P.'s Chicago office. Alexandra N. Cabeza is an attorney in Shook, Hardy & Bacon L.L.P.'s Miami office. Lindsey Knapton is an attorney in Shook, Hardy & Bacon L.L.P.'s Denver office. Josh Hansen is an attorney in Shook, Hardy & Bacon L.L.P.'s Denver office. Robert A. Stines is a partner in Smith, Gambrell & Russell, LLP's Tampa office. Anna A. Gadberry is an attorney in Shook, Hardy & Bacon L.L.P.'s Kansas City office.*

III. Developments in Case Law ..... 206
A. Case Law Developments Related to Advertising Technology, by Tara D. Kennedy ..... 206
1. Case Law Narrowing "Subscriber" Status Under the Video Privacy Protection Act ..... 206
2. What Does the VPPA Cover? ..... 206
3. Cases Dismissing VPPA Claims Where Plaintiff Did Not Adequately Allege "Subscriber" Status ..... 207
B. Case Law Developments in Session Replay Litigation, by Alexandra N. Cabeza ..... 209
C. A Year in Review: Meta Pixel, by Lindsey Knapton ..... 211
1. *In re Meta Pixel*, Case No. 22-cv-03580-WHO (United States District Court for the Northern District of California) ..... 211
2. *Kurowski v. Rush System for Health*, No. 22 C 5380 (United States District Court for the Northern District of Illinois) ..... 213
3. *Cousin v. Sharp Healthcare*, Case No. 22-cv-2040-MMA (DDL) (United States District Court for the Southern District of California) ..... 213
4. *Hartley v. University of Chicago Medical Center* (United States District Court for the Northern District of Illinois) ..... 214
5. Developing Legal Trends ..... 215
IV. Notable Enforcement Actions ..... 216
A. Privacy Breaches, Settlements, and Regulator Activity: A Year (and Then Some) in Review, by Josh Hansen ..... 216
1. The FTC Revives Dormant Rule to Address Disclosures of Medical Data. ..... 216
2. Privacy and Security Liability Comes for Leadership ..... 218
3. OCR Takes Expansive Reading of HIPAA and Online Trackers ..... 219
4. Data Brokers Find Themselves in the FTC Crosshairs ..... 221
5. New York Enforces and Bolsters Its Cybersecurity Requirements ..... 222
6. Children's Privacy Becomes a Focal Point for the FTC ..... 224
V. Notable Settlements ..... 225
A. Advocate Aurora Health Pixel Litigation Settlement, by Robert A. Stines ..... 225

## I. U.S. AND EU STATUTORY DEVELOPMENTS

### A. *United States and International Statutory Developments, by Lauren D. Godfrey, Suzie Allen & Catherine Geisler*

State legislatures in the data breach notification and consumer privacy space have been very active during the survey period with amending existing data breach notification statutes, as well as more states enacting their own consumer privacy statutes. Outside of the United States, countries continue to enact laws to protect its residents' data. This section of the survey will focus on states that enacted new data breach and privacy legislation during the survey period, and developments outside the United States.

#### 1. United States State Developments

##### a. *California Privacy Rights Act*

On February 3, 2023, the Board of the California Privacy Protection Agency held a meeting focusing on the regulations that will interpret the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA).[1] The regulations were set to go into effect on July 1, 2023, but were delayed by a ruling of the Superior Court of California, County of Sacramento.[2] Additionally, Governor Gavin Newsom signed AB 947 and AB 1194 into law. AB 947 amends the definition of "sensitive personal information" to add a consumer's citizenship or immigration status.[3] AB 1194 provides that a business must comply with the privacy rights of consumers under the CCPA if the consumer's personal information contains information related to reproductive health.[4] It also amends the text of the law to provide that a consumer that accesses, procures, or searches for reproductive health services does not constitute a natural person at risk or danger of death or serious physical injury.[5]

##### b. *Colorado Privacy Act*

On July 7, 2021, Governor Polis signed Senate Bill 21-190: Protect Personal Data Privacy, otherwise known as the Colorado Privacy Act (CPA).[6]

1. Cal. Consumer Privacy Act of 2018 (amended), Cal. Civ. Code § 1798.100 *et seq*. (2020), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

2. *See* Cal. Chamber of Commerce v. Cal. Privacy Prot. Agency, No. 34-2023-80004106-CU-WM-GDS (Cal. Super. Ct. June 30, 2023), *available at* https://www.mwe.com/pdf/cal-chamber-of-commerce-v-cal-privacy-prot-agency.

3. Cal. Consumer Privacy Act of 2018, A.B. 947, 2023–2024 Reg. Sess. (Cal. 2023) (enacted) (sensitive personal information).

4. Cal. Privacy Rights Act of 2020, A.B. 1194, 2023–2024 Reg. Sess. (Cal. 2023) (enacted) (contraception services).

5. *Id.*

6. Act Concerning Additional Protection of Data Relating to Personal Privacy, S.B. 21-90, 2021 Reg. Sess. (Colo. 2021) (enacted), https://leg.colorado.gov/bills/sb21-190.

The CPA is part of the State of Colorado's Consumer Protection Act, and it went into effect on July 1, 2023. Additionally, the Colorado Secretary of State filed its final rules on March 15, 2023. The CPA provides consumers the right to access, correct, and delete personal data, along with the right to opt out of the sale, collection, and use of their personal data.[7] It imposes affirmative obligations upon companies to safeguard consumer personal data, provide clear, understandable, and transparent information to consumers about how their personal data are used, and strengthens compliance and accountability.[8] Finally, the CPA empowers the Colorado Attorney General and district attorneys to access and evaluate a company's data protection assessments, impose penalties where violations occur, and prevent future violations.[9]

c. *Connecticut*

On May 10, 2022, Governor Ted Lamont signed Senate Bill 6: An Act Concerning Personal Data Privacy and Online Monitoring (also known as The Connecticut Data Privacy Act) (CTDPA) into law.[10] The CTDPA went into effect on July 1, 2023.[11] The CTDPA gives Connecticut residents rights over their personal data and creates responsibilities and privacy protection standards for data controllers that process consumer's personal data.[12] It applies to people who conduct business in Connecticut or produce products or services targeted to Connecticut residents and who control or process the personal data of at least 100,000 Connecticut consumers or 25,000 or more consumers and derived more than twenty-five percent of gross revenue from the sale of personal data.[13] It also applies to service providers called "processors" that maintain or provide services involving personal data on behalf of covered business.[14]

d. *Delaware*

On September 11, 2023, Delaware became the thirteenth state to enact a consumer privacy law. The Delaware Personal Data Privacy Act (DPDPA)—to go into effect on January 1, 2025—provides residents the rights to access, opt out, correct, and request a deletion of their personal data by an entity or person.[15] The DPDPA applies to entities that control

7. *Id.*
8. *Id.*
9. *Id.*
10. An Act Concerning Personal Data Privacy and Online Monitoring, S.B. 6, Gen. Assemb. (Conn. 2022) (enacted), https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.*
15. Delaware Personal Data Privacy Act, H.B. 154, 152d Gen. Assemb. §12D-104(a)(1)–(6) (Del. 2023), https://legis.delaware.gov/BillDetail?LegislationId=140388.

or process personal data of 35,000 or more Delaware residents in a given year or organizations that control or process personal data of 10,000 or more Delaware residents and derive more than twenty percent of their gross revenue from the sale of personal data.[16] The DPDPA also applies to nonprofits that are dedicated exclusively to preventing an addressing insurance crimes. Enforcement will exclusively be left to the Department of Justice (DOJ), and the DPDPA does not provide for a private right of action.[17] Entities will receive a sixty-day notice to rectify violations. Failure to do so can result in an enforcement action by the DOJ.[18]

e. *Pennsylvania*

In November 2022, the Pennsylvania legislature amended Pennsylvania's Breach of Personal Information Notification Act (Pennsylvania Act).[19] The amendments to the Pennsylvania Act went into effect on May 3, 2023.[20] In amending the Pennsylvania Act, the state legislature took steps similar to other states' data breach notification statutes and expanded the definition of "personal information."[21] Among other things, the amendments expanded the reach of the Act to cover "State Agency Contractors," as well as hold state agencies (including public schools) and their contractors to stricter notification requirements, specific timelines, and requirements for notification by state agencies, state agency contractors, public schools, counties, and municipalities when a determination of breach has been made.[22] The amendments will allow entities to investigate and make a "determination" that a breach has occurred before their notification obligation takes effect;[23] they will be able to provide certain notifications by email;[24] and they may be exempt if they are in compliance with other specified regulatory obligations.[25]

f. *Florida*

On June 7, 2023, Governor Ron DeSantis signed into law the Florida Technology Transparency Bill (FTTB),[26] which will take effect on July 1,

16. *Id.* § 12D-103(a)(1)–(2).
17. *Id.* § 12D-111(a)–(d).
18. *Id* § 12D-111(b).
19. Breach of Personal Information Notification Act, Act of Dec. 22, 2005, P.L. 474, No. 94 (Penn. 2022), https://www.legis.state.pa.us/WU01/LI/LI/US/HTM/2005/0/0094..HTM.
20. Act of Nov. 3, 2022, Breach of Personal Information Notification Act, Act. Of Nov. 3, 2022, P.L. 2139, No. 151 (Penn. 2022), https://www.legis.state.pa.us/WU01/LI/LI/US/HTM/2022/0/0151..HTM?40.
21. 73 Pa. Cons. Stat. § 2302.
22. *See id.* § 2303(a.1), (a.2).
23. *Id.* § 2309.
24. *Id.* § 2303(a.3).
25. *Id.* §§ 2305.3, 2307(b)(2).
26. Technology Transparency, S.B. 262, 2023 Leg., Reg. Sess. (Fla. 2023) (enacted) (Fla. Stat. § 501.701 *et seq.* (2023)).

2024. The bill is split into three sections, (a) the Florida Digital Bill of Rights (FDBR); (b) the protection of minors in online spaces; and (c) the prohibition of government entities from using their positions to make certain requests to social medial platforms. FTTB applies to a person who conducts business in Florida or produces products or services targeted to Florida residents and that processes or engages in the sale of personal data.[27] FDBR provides consumers the rights to access, to correct, to delete, to portability, to opt out of profiling/targeted advertising purposes, to opt out of the sale of their personal information, to opt out of the collection or processing of personal data, and to opt out of the collection of personal data collected through voice recognition or facial recognition features.[28] FTTB prohibits online platforms that provide services predominantly accessed by minors from processing the minor's personal data if it has actual knowledge that such processing may result in substantial harm or privacy risk to minors.[29] FTTB further prohibits government entities from requesting social media platforms to remove content or accounts from the platform.[30] The bill also prohibits government entities from initiating or maintaining relationships with social media platforms for the purposes of content moderation.[31] FTTB does not create a private right of action.[32] The bill grants the Florida Department of Legal Affairs exclusive enforcement authority and may seek civil penalties of up to $50,000 per violation.[33]

g. *Iowa*

On March 28, 2023, Iowa Governor Kim Reynolds signed into law the Iowa Consumer Data Protection Act (Iowa CDPA),[34] which will take effect on January 1, 2025. Iowa CDPA applies to a person who conducts business in Iowa or produces products or services targeted to Iowa residents and that during a calendar year (a) controls or processes personal data of at least 100,000 consumers; or (b) controls or processes personal data of at least 25,000 consumers and derives over fifty percent of gross revenue from the sale of personal data.[35] Iowa CDPA grants consumers the rights to access, to delete, to portability, and to opt out of the sale of personal data.[36] The act also imposes certain obligations on controllers, such as providing a privacy notice that includes the categories of personal data processed by

27. *Id.* § 6 (Fla. Stat. § 501.705(2) (2023)).
28. *Id.* § 8 (Fla. Stat. § 501.705(2) (2023)).
29. *Id.* § 2 (Fla. Stat. § 501.1735(2) (2023)).
30. *Id.* § 1 (Fla. Stat. § 112.23(2) (2023)).
31. *Id.*
32. *Id.* § 2 (Fla. Stat. § 112.23(4)(f) (2023)).
33. *Id.* § 2 (Fla. Stat. § 501.1735(4)); *id.* § 23 (Fla. Stat. § 501.72(1) (2023)).
34. Iowa Consumer Data Protection Act, Iowa S.F. 262 (2023) (enacted) (Iowa Code § 715D.1 *et seq*. (2023)).
35. *Id.* § 2 (Iowa Code § 715D.2.1 (2023)).
36. *Id.* § 3 (Iowa Code § 715D.3.1 (2023)).

the controller and shared with third parties, the purpose for processing that data, and a description on how consumers may exercise their rights.[37] The act does not create a private right of action.[38] The act grants the Iowa Attorney General exclusive enforcement authority and may seek civil penalties of up to $7,500 per violation.[39]

h. *Indiana*

On May 1, 2023, Governor Eric Holcomb signed the Indiana Consumer Data Protection Act (Indiana CDPA),[40] which takes effect on January 1, 2026. Indiana CDPA applies to a person who conducts business in Indiana or produces products or services that are targeted to Indiana residents and that during a calendar year (a) controls or processes personal data of at least 100,000 Indiana consumers; or (b) controls or processes personal data of at least 25,000 Indiana consumers and derives over fifty percent of gross revenue from the sale of personal data.[41] Indiana CDPA grants consumers the rights to access, to correct, to portability, to delete, and to opt out of targeted advertising and sale of personal data.[42] The act also imposes certain obligations on controllers, such as providing a privacy notice that includes the categories of personal data processed by the controller and shared with third parties, the purpose for processing that data, and a description on how consumers may exercise their rights.[43] Indiana CDPA does not grant a private right of action.[44] The act grants the Indiana Attorney General exclusive enforcement authority and may seek civil penalties of up to $7,500 per violation.[45]

i. *Montana*

(1) Montana Consumer Data Privacy Act (MCDPA)

On May 19, 2023, Governor Greg Gianforte signed into law the Montana Consumer Data Privacy Act (MCDPA),[46] which will take effect on October 1, 2024. MCDPA applies to controllers that conduct business in Montana or produce products or services targeted to Montana residents and that (a) control or possess personal data of 50,000 or more consumers; or (b) personal data of 25,000 or more consumers, while deriving more than

37. *Id.* § 4 (Iowa Code § 715D.4.5 (2023)).
38. *Id.* § 8 (Iowa Code § 715D.8.4 (2023)).
39. *Id.* § 8 (Iowa Code § 715D.8.1 (2023)).
40. Consumer Data Protection, S.B. 5, 123d Gen. Assemb., Reg. Sess. (Ind. 2023) (enacted) (Ind. Code § 24-15 *et seq.* (2023)).
41. *Id.* ch. 1 (Ind. Code § 24-15.1.1(a)).
42. *Id.* ch. 3 (Ind. Code § 24-15.3.1(b)).
43. *Id.* ch. 4 (Ind. Code § 24-15.4.3(b)).
44. *Id.* ch. 10 (Ind. Code § 24-15.10.4).
45. *Id.* ch. 10 (Ind. Code § 24-15.10.1–2(a)).
46. Montana Consumer Data Privacy Act, S.B. 384, 68th Leg., Reg. Sess. (Mont. 2023).

twenty-five percent gross revenue from selling personal data.[47] MCDPA grants consumers the rights to access, to correct, to delete, to portability, and to opt out of targeted advertising, selling of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects on a consumer.[48] The act also imposes certain obligations on controllers, such as providing a privacy notice that includes the categories of personal data processed by the controller and shared with third parties, the purpose for processing that data, a description on how consumers may exercise their rights, and an active email address or other contact that consumers may use to contact the controller.[49] MCDPA does not grant a private right of action.[50] The act grants the Montana Attorney General exclusive enforcement authority.[51]

(2) Montana Genetic Information Privacy Act (MGIPA)

On June 7, 2023, Governor Greg Gianforte signed into law the Montana Genetic Information Privacy Act (MGIPA),[52] which went into effect on October 1, 2023. MGIPA requires entities to provide clear and complete information regarding its policies and procedures with respect to the collection, use, and disclosure of genetic data.[53] MGIPA requires entities to include a prominent and publicly available privacy notice that includes information regarding the entity's data collection, consent, use, access, disclosure, transfer, security, and retention and deletion practice for genetic data.[54] The entity must also obtain express consent from the consumer to collect, use, or disclose the consumer's genetic data.[55] Express consent is also required for the transfer or disclosure of genetic data to third parties for research purposes.[56] Finally, entities must obtain express consent for marketing to a consumer based on their genetic data, marketing by a third party to a consumer based on the consumer's purchase history of a genetic product or service, or sale of the consumer's genetic data.[57] The act grants the Montana Attorney General the exclusive authority to enforce MGIPA and may seek civil penalties of up to $2,500 per violation.[58]

47. *Id.* § 3.
48. *Id.* § 59.
49. *Id.* § 7(5).
50. *Id.* § 12(3).
51. *Id.* § 12(1).
52. Genetic Information Privacy Act, S.B. 351, 68th Legis., Reg. Sess. (Mont. 2023) (enacted).
53. *Id.* § 4(1)(a).
54. *Id.* § 4(1)(b).
55. *Id.* § 4(2).
56. *Id.* § 4(3)(b).
57. *Id.* § 4(3)(c).
58. *Id.* § 6.

j. *Nevada*

In May 2023, Nevada signed the Consumer Health Data Privacy Act (CHDPA) into law, providing additional protections for consumer health data collected and maintained by regulated entities.[59] The CHDPA will protect both residents and non-residents of Nevada whose consumer health data is being collected in Nevada.[60] The CHDPA provides consumers with several rights, including the right to access their data, to know with whom the regulated entity has shared or sold their data, to request deletion of their data, and to request the regulated entity cease processing their data.[61] Notably, the CHDPA will prohibit the use of geofencing—a type of location-based marketing and advertising—in and around healthcare facilities.[62] The CHDPA does not provide for a private right of action; however, a violation may constitute a deceptive trade practice for which the Attorney General may seek injunctive relief and/or civil penalties pursuant to Nevada Revised Statutes chapter 598.[63] The law will go into effect on March 31, 2024, with no delayed effective date for small businesses.[64]

k. *Oregon*

On July 18, 2023, Governor Tina Kotek signed into law the Oregon Consumer Privacy Act (OCPA), which will take effect on July 1, 2024.[65] OCPA applies to controllers that conduct business in Oregon or produce products or services targeted to Oregon residents and that during a calendar year (a) control or possess personal data of 100,000 or more consumers; or (b) personal data of 25,000 or more consumers, while deriving more than twenty-five percent gross revenue from selling personal data.[66] OCPA provides consumers the rights to access, to correct, to delete, to opt out of profiling/targeted advertising purposes, and to opt out of the sale of their personal information.[67] OCPA also imposes certain obligations on data controllers, such as providing a privacy policy that includes the categories of personal data processed by the controller and shared with third parties, the purpose for processing that data, and a description on how consumers may exercise their rights.[68] The act does not create a private

59. Consumer Health Data Privacy Act, S.B. 370, 83d Leg., Reg., Sess. (Nev. 2023) (enacted), https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text.

60. *Id.* § 7.

61. *Id.* § 24(1)–(2).

62. *Id.* § 31(1)(a)–(1)(c).

63. *Id.* § 34(1)–(2).

64. *Id.* § 36.

65. Oregon Consumer Privacy Act, S.B. 619, 82d Leg. Assemb., Reg. Sess. (Or. 2023) (enacted) (Or. Rev. Stat. § 180.095 *et seq*. (2023)).

66. *Id.* § 2.(1) (Or. Rev. Stat. § 180.095-2.(1) (2023)).

67. *Id.* § 3.(1) (Or. Rev. Stat. § 180.095-3.(1) (2023)).

68. *Id.* § 5 (2023) (Or. Rev. Stat. § 180.095-5.(4) (2023)).

right of action.[69] The act grants the Oregon Attorney General exclusive authority to enforce OCPA and may seek civil penalties of up to $7,500 per violation.[70]

l. *Tennessee*

On May 11, 2023, Governor Bill Lee signed into law the Tennessee Information Protection Act (TIPA),[71] which will take effect on July 1, 2025. TIPA applies to any person that conducts business in Tennessee or produces products or services targeted to Tennessee residents and that (a) exceeds $25 million in revenue and (b) controls or processes 25,000 consumers and derives more than fifty percent of gross revenue from the sale of personal information or controls or processes personal information of at least 175,000 consumers during a calendar year.[72] TIPA provides consumers the rights to access, to correct, to delete, to opt out of profiling/targeted advertising purposes, and to opt out of the sale of their personal information.[73] A unique feature of TIPA is that it will allow data controllers an affirmative defense if the data controller creates, maintains, and complies with its privacy policy that reasonably conforms to the National Institute of Standards and Technology privacy framework or other documented policies, standards, and procedures designed to safeguard consumer privacy.[74] The act does not provide a private right of action.[75] The Tennessee Attorney General has exclusive authority to enforce TIPA, and a court may impose civil penalties of up to $7,500 per violation.[76]

m. *Texas*

(1) Breach Reporting

Texas amended its breach notification law to shorten the amount of time that entities have to notify the Texas Attorney General of a data breach. Effective September 1, 2023, Texas requires entities that experience a data breach affecting 250 or more Texas residents to notify the Texas Attorney General as soon as practicable, but not later than thirty days from the determination of a breach.[77] Previously, businesses had up to sixty days to notify the Texas Attorney General.

69. *See id.* § 9 (Or. Rev. Stat. § 180.095-9 (2023)).
70. *Id.* § 9(4)(a) (Or. Rev. Stat. § 180.095-9(4)(a) (2023)).
71. Tennessee Information Protection Act, H.B. 1181, 112th Gen. Assemb., Reg. Sess. (Tenn. 2023) (enacted).
72. *Id.* § 2 (Tenn. Code Ann. § 47-18-3202 (2023)).
73. *Id.* § 2 (Tenn. Code Ann. § 47-18-3203(a) (2023)).
74. *Id.*
75. *Id.* § 2 (Tenn. Code Ann. § 47-18-3212(e) (2023)).
76. *Id.* § 2 (Tenn. Code Ann. § 47-18-3212 (a), (d) (2023)).
77. Tex. Bus. & Com. Code § 521.053(j) (2023).

(2) Texas Data Security & Privacy Act (TDSPA)

On June 18, 2023, Governor Greg Abbott signed into law the Texas Data Security & Privacy Act (TDSPA),[78] which will take effect on July 1, 2024. TDSPA applies to persons that conduct business in Texas or produce products or services for Texas residents, that process or engage in the sale of personal data, and that are not a "small business."[79] TDSPA is the first to adopt an exemption for small businesses as that term is defined by the U.S. Small Business Administration (SBA) and based on the SBA's industry size standards. TDSPA provides consumers the rights to access, to correct, to delete, to opt out of profiling/targeted advertising purposes, to opt out of sales, and to opt out of certain automated decision making.[80] TDSPA also imposes certain obligations on data controllers, such as providing a privacy policy that includes the categories of personal data processed by the controller and shared with third parties, the purpose for processing that data, and a description on how consumers may exercise their rights.[81] The act does not provide a private right of action.[82] The Texas Attorney General has exclusive authority to enforce the TDSPA and may seek civil penalties of up to $7,500 per violation.[83]

(3) Securing Children Online through Parental Empowerment (SCOPE) Act

On July 13, 2023, Governor Greg Abbott signed into law the Securing Children Online through Parental Empowerment (SCOPE) Act,[84] which will take effect on September 1, 2024. SCOPE applies to digital service providers that collect or process personal information of minors (under the age of eighteen) and either target minors or know or should know that the digital service appeals to minors.[85] Under SCOPE, digital service providers must obtain parental consent before allowing users under the age of eighteen to create an account on a provider's platform.[86] Digital service providers must develop and implement strategies to prevent minors from being exposed to harmful materials such as self-harm, suicide, eating disorders, and other similar behaviors.[87] SCOPE also requires digital service provid-

78. H.B. 4, 88th Leg., Reg. Sess. (Tex. 2023) (enacted) (Tex. Bus. & Com. Code § 541 *et seq*. (2023)).
79. *Id.* § 1 (Tex. Bus. & Com. Code § 541.003 (2023)).
80. *Id.* (Tex. Bus. & Com. Code § 541.051(b) (2023)).
81. *Id.* (Tex. Bus. & Com. Code § 541.102 (2023)).
82. *Id.* (Tex. Bus. & Com. Code § 541.155 (2023)).
83. *Id.* (Tex. Bus. & Com. Code § 541.154–155 (2023)).
84. Securing Children Online through Parental Empowerment Act, H.B. No. 18, 88th Leg., Reg. Sess. (Tex. 2023) (enacted) (Tex. Bus. & Com. Code § 509 *et seq*.).
85. *Id.* § 2 (Tex. Bus. & Com. Code § 509.002 (2023)).
86. *Id.* § 2 (Tex. Bus. & Com. Code § 509.052 (2023)).
87. *Id.* § 2 (Tex. Bus. & Com. Code § 509.051 (2023)).

ers to provide parents or guardians tools to allow them to supervise the minor's use of the digital service.[88] A minor's parent or guardian has a private right of action against a digital service provider for a violation under SCOPE and can seek injunctive relief, actual damages, punitive damages, reasonable attorney's fees, court costs, and any other relief that the court deems appropriate.[89] SCOPE also grants the Texas Attorney General authority to enforce the act.[90]

n. *Utah*

On March 24, 2022, Governor Spencer Cox signed into law the Utah Consumer Privacy Act (UCPA),[91] which went into effect on December 31, 2023. Utah will be the fourth state in the United States to enact a comprehensive consumer privacy law following California, Virginia, and Colorado. UCPA applies to any controller or processor that conducts business in Utah or produces products or services targeted to Utah residents, and that controls or process the personal data of at least (a) 100,000 consumers during a calendar year or (b) 25,000 consumers and derives over fifty percent of gross revenue from the sale of personal data.[92] UCPA provides consumers rights of access, deletion, data portability, and the right to opt-out of targeted advertising or sales of personal data.[93] Unlike its California, Virginia, and Colorado counterparts, UCPA does not include the right to correct. UCPA also requires controllers to provide a privacy policy that includes the categories of personal data processed by the controller and shared with third parties, the purpose for processing that data, and a description on how consumers may exercise their rights.[94] UCPA also requires controllers to provide clear and transparent information to consumers about how they can opt out of sales of their personal data or processing for targeted advertising and not discriminate against them for exercising their rights.[95] Moreover, controllers must establish, implement, and maintain reasonable administrative, technical, and physical data-security practices.[96] UCPA does not provide a private right of action.[97] The Utah Attorney General has exclusive authority to enforce UCPA and can seek civil penalties of up to $7,500 per violation.[98]

88. *Id.* § 2 (Tex. Bus. & Com. Code § § 509.053 (2023)).
89. *Id.* § 2 (Tex. Bus. & Com. Code § 509.152 (2023)).
90. *Id.* § 2 (Tex. Bus. & Com. Code § 509.151 (2023)).
91. Consumer Privacy Act, S.B. 227, 2022 Gen. Sess. (Utah 2022) (enacted) (Utah Code Ann. § 13-61-101 *et seq.* (2022)).
92. *Id.* § 3 (Utah Code § 13-61-102 (2022)).
93. *Id.* § 5 (Utah Code § 13-61-102 (2022)).
94. *Id.* § 9 (Utah Code § 13-61-102 (2022)).
95. *Id.*
96. *Id.*
97. *Id.* § 12 (Utah Code § 13-61-102 (2022)).
98. *Id.* § 14 (Utah Code § 13-61-102 (2022)).

o. *Virginia*

On March 2, 2021, Governor Ralph Northam signed into law the Virginia Consumer Data Protection Act (VCDPA),[99] which went into effect on January 1, 2023. VCDPA applies to any person that conducts business in Virginia, or produces products or services targeted to Virginia residents, in which that business controls or processes (a) personal data of at least 100,000 consumers during a calendar year; or (b) personal data of at least 25,000 consumers and derives over fifty percent of gross revenue from the sale of personal data.[100] The act grants consumers the rights to access, to correct, to delete, to portability, and to opt out of targeted advertising, selling of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects on a consumer.[101] The act also imposes certain obligations on controllers, such as providing a privacy notice that includes the categories of personal data processed by the controller and shared with third parties, the purpose for processing that data, and a description on how consumers may exercise their rights.[102] VCDPA does not grant a private right of action.[103] The act grants the Virginia Attorney General exclusive enforcement authority and may seek civil penalties of up to $7,500 per violation.[104]

2. Developments Outside the United States

a. *Swiss Data Protection Act*

The new Swiss Federal Act on Data Protection (nFADP) took effect on September 1, 2023. The goal of the law is to more closely align with the European Union's General Data Protection Regulation (GDPR) to protect the fundamental rights of persons when their data is processed. Notably, the nFADP applies only to natural persons—excluding legal "persons" such as corporations.[105] Another important objective of the nFADP is to continue allowing information to flow freely between EU and Swiss companies.[106] In part, the nFADP imposes new obligations on businesses processing data subject to the law. For example, implementing the principles of data protection by default,[107] keeping a register of processing activity,[108]

99. Va. Code Ann. § 59.1-576 *et seq*. (2023).
100. *Id.* § 59.1-576(A).
101. *Id.* § 59.1-577(A).
102. *Id.* § 59.1-578(C).
103. *Id.* § 59.1-584 (E).
104. *Id.* § 59.1-584 (A), (C).
105. Regulation 2020/7397, of the Federal Assembly of the Swiss Confederation, based on Articles 95, 122 and 173 paragraph 2 of the Federal Constitution, and having regard to the Federal Council Dispatch dated 23 March 1988 [hereinafter nFADP], Art. 2(1).
106. *Id.* Art.16 (1).
107. *Id.* Art. 7(1), (2).
108. *Id.* Art. 12, 15(1).

and providing prompt notice to the Federal Data Protection and Information Commissioner in the event of a security breach.[109] Further, the nFADP provides individuals additional rights to information regarding the processing of their personal data[110] including access to their data[111] and ensuring its accuracy.[112]

b. *India*

India's President Droupadi Murmu signed The Digital Personal Data Protection Act (DPDPA) into law on August 12, 2023.[113] The Act provides for processing of digital personal data "in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes" and other related matters.[114] The DPDPA sets out the obligations of Data Fiduciaries,[115] which includes the appointment of a Data Protection Officer in India.[116] Data Fiduciaries are persons who alone or in conjunction with other persons determine the purposes and means of processing of personal data.[117] The DPDPA sets out the rights and duties of a Data Principal,[118] the individual to whom personal data relates, including parents of children and guardians of individuals with disabilities.[119] The DPDPA also includes special provisions that address the processing of personal data outside of India.[120] The DPDPA established a Data Protection Board of India.[121] The DPDPA requires that Data Fiduciaries notify the Board and each affected Data Principal when an "intimation" of a personal data breach has occurred in a "form and manner as may be prescribed."[122] In part, the Board may direct any urgent remedial or mitigation measures in the event of a personal data breach, inquire into the breach, and impose penalties.[123] The DPDPA authorizes penalties to be assessed against a person who breaches the provisions of the DPDPA.[124]

109. *Id.* Art. 24 (1).
110. *Id.* Art. 19 *et seq*.
111. *Id.* Art. 25(2).
112. *Id.* Art. 6 (5).
113. The Gazette of India Extraordinary, CG-DL-E-12082023-248045, New Delhi, Aug. 11, 2023/Sravana 20, 1945 (SAKA).
114. *Id.*
115. *Id.*, ch. II.
116. *Id.*, ch. II., (10)(2).
117. *Id.*, ch. I, (2)(i).
118. *Id.*, ch. III.
119. *Id.*, ch. I., (2)(j).
120. *Id.*, ch IV.
121. *Id.*, ch. V.
122. *Id.*, ch. II, (8)(6).
123. *Id.*, ch. VI, (27)(1)(a).
124. *Id.*, ch. VIII.

c. *Saudi Arabia*

On September 7, 2023, the Saudi Data and Artificial Intelligence Authority (SDAIA) released the Kingdom of Saudi Arabia Personal Data Protection Law (PDPL).[125] Additionally, Implementing Regulations and Regulations pertaining to Personal Data Transfer outside the Kingdom were enacted.[126] These Regulations clarify and add further requirements separate from the PDPL.[127] The PDPL will be enforced starting on September 14, 2024.[128] The law applies to processing of personal data related to individuals, which takes place in the Kingdom including by parties outside of the Kingdom.[129] This also includes deceased individuals if it would lead to them or a member of their family being specifically identified.[130] Article 4 of the DPDPA sets forth data subject rights including the right to be informed, to access, to obtain their Personal Data from the controller, and to request destruction of their personal data held by the Controller.[131] The PDPL requires that the purpose of the collection of personal data must be directly related to the Controller's purposes and limited to the minimum amount necessary to achieve the purpose of the data collection.[132] Personal data must be destroyed if it is no longer necessary for the purpose for which it was collected.[133] Controllers must have a privacy policy in place and available to data subjects prior to collecting personal data.[134]

The PDPL also contains restrictions on the disclosure of personal data.[135] The PDPL requires the Controller to notify the Competent Authority upon "knowing of any breach, damage, or illegal access to personal data," as well as the data subject.[136] Notification to the Competent Authority be made within seventy-two hours of becoming aware of an incident, if the incident potentially causes harm to the personal data, or to the data subject, or conflicts with their rights or interests.[137] If notification cannot be made within seventy-two hours, then it must be made as soon as possible

125. Personal Data Protection Law (PDPL), Royal Decree No. (M/19) 9/02/1443, https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf.
126. The Implementing Regulation of the PDPL.
127. *Id.*
128. PDPL, Art. 43.
129. *Id.*, Art. 2(1).
130. *Id.*
131. *Id.*, Art. 4 (1)–(5).
132. *Id.*, Art. 11(1)–(3).
133. *Id.*, Art. 11(4).
134. *Id.*, Art. 12.
135. *Id.*, Arts. 15–16.
136. *Id.*, Art. 20(1)–(2).
137. The Implementing Regulation of the PDPL, Art. 24.

along with justifications for the delay.[138] Prior consent of the data subject is required before sending advertising or awareness-raising materials, as well as an opt out mechanism.[139] Cross-border data transfer of personal data is permitted to achieve certain purposes set out by the PDPL.[140] The PDPL contains penalties including fines (up to three million riyals) and imprisonment for disclosing or publishing sensitive data with the intent to harm the data subject or achieve a personal benefit.[141] It also imposes fines on persons "with a special natural or legal capacity" who violate this law or this regulation.[142]

d. *UK-US Data Bridge*

The UK-US Data Bridge was announced in September 2023 in order to establish a means through which UK businesses and organizations can transfer personal data to those that are certified compliant in the United States. According to the UK's Department for Science, Innovation, and Technology, the Data Bridge will drive trans-Atlantic research and innovation through ensuring robust and reliable data flows.[143] As of October 12, 2023, UK businesses are able to transfer data to a U.S.-based service provider or company in a more efficient and cost-effective manner.[144] The EU-US Data Privacy Framework (DPF) is an opt-in certification system for U.S. businesses and organizations that provides a set of enforceable requirements that must be complied with in order to join the DPF.[145] Organizations in the United States that have been certified through the DPF can now opt in to receive data from the United Kingdom through the UK-US Data Bridge.[146]

e. *European-US Data Privacy Framework Adequacy Decisions 2023, by Joy Momin*

(1) Background on GDPR's Data Exportation Regulations

The General Data Protection Regulation (GDPR) is the central law governing data protection in the European Union. The central objective of the GDPR's data transfer provisions is to ensure that the level of protection of

138. *Id.*, Art. 24(2).
139. *Id.*, Art. 25(1)–(2).
140. *Id.*, Art. 29(1)–(4).
141. *Id.*, Art. 35(1).
142. *Id.*, Art. 36(1).
143. Press release: Department for Science, Innovation, & Technology, "UK and US reach commitment in principle over 'data bridge.'" (June 8, 2023).
144. "UK Extension to the EU-US Data Privacy Framework" (UK Extension) under Article 45 of the UK General Data Protection Regulation (GDPR)
145. Department for Science, Innovation, & Technology, "Notice UK-US data bridge: factsheet for UK organisations." (Sept. 21, 2023).
146. *Id.*

natural persons guaranteed by the GDPR is not undermined. Pursuant to Article 45(3) of the GDPR, the European Commission has the authority to determine whether a third country ensures an adequate level of protection for personal data.[147] An adequacy decision establishes that the level of protection for personal data in the third country is "essentially equivalent" to the level of protection in the European Union (EU).[148] The test of whether a foreign system delivers the required level of protection is whether—through the substance of privacy rights and their effective implementation, supervision, and enforcement—the system as a whole delivers the level of protection that is available under the GDPR.[149] Once an adequacy decision is in place, personal data can flow freely from the EU and European Economic Area (EEA) countries to the third country without the need for any additional safeguards.[150] The United Kingdom has its own version of the GDPR, similar to that of the EU.[151]

(2) History of the EU-US Data Privacy Framework

Two previous iterations of the EU-US Data Privacy Framework are worth mentioning: the Safe Harbor framework and the Privacy Shield framework. In 2000, the United States and the European Union signed the Safe Harbor Agreement in compliance with the 1995 European Data Directive.[152] The Safe Harbor Agreement was a self-certification framework that allowed U.S. companies to transfer personal data from the EU to the United States by affirming their adherence to certain privacy principles. In 2015, the CJEU invalidated the Safe Harbor Agreement in the case of *Schrems v. Data Protection Commissioner*, finding that the Safe Harbor

147. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (Dec. 19, 2019), https://curia.europa.eu/juris/document/document.jsf;jsessionid=0D2FE09B7D7A588F8B97358BEE3D6897?text=&docid=221826&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=14058780.

148. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1.8 [hereinafter Decision 2016/1250].

149. See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM (2017) 7 final, sec. 3.1, at 6–7 (Jan. 10, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007.

150. Case C-362/14, Maximilian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 73.

151. Data Protection Act 2018, c. 12 (UK).

152. Letter from Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (Feb. 29, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european.

Agreement did not adequately protect the personal data of EU citizens from access by U.S. intelligence agencies.[153]

In 2016, the United States and the European Union signed the Privacy Shield Agreement, which was designed to address the concerns raised by the CJEU in the *Schrems* case. The Privacy Shield Agreement included new safeguards, such as an ombudsperson mechanism to investigate complaints from EU citizens about the collection and use of their personal data by U.S. companies. However, in 2020, the CJEU invalidated the Privacy Shield Agreement in the case of *Schrems II v. Data Protection Commissioner*. The CJEU found that the Privacy Shield Agreement still did not adequately protect the personal data of EU citizens from access by U.S. intelligence agencies.[154]

(3) EU-U.S. Data Privacy Framework Adequacy Decision

Following an initial February 2023 Opinion[155] on the insufficiency of a proposed framework and after several rounds of negotiations, the European Parliament adopted a resolution opposing the adoption of an EU adequacy decision for the United States based on the EU-US Data Privacy Framework (DPF) on May 11, 2023. The resolution was passed after the European Parliament analyzed Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities (EO 14086), which was issued in the United States to implement the DPF.[156]

The European Parliament concluded that EO 14086 fails to provide sufficient safeguards for the transfer of personal data from the EU to the United States, highlighting that:

(1) U.S. signals intelligence practices are still considered too broad, allowing for the bulk collection of personal data, including the content of communications. EO 14086 includes safeguards for bulk data collection, but does not require independent prior authorization, which is necessary to limit U.S. intelligence activities. The European Parliament has expressed concern that U.S. authorities could use this loophole to access data they would otherwise be prohibited from accessing, as noted by the European Data Protection Board in its opinion on the DPF.

153. Case C-362/14, *supra* note 150.

154. Decision 2016/1250, *supra* note 148.

155. Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data Under the EU-US Data Privacy Framework (Feb. 28 2023), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en.

156. European Parliament Resolution of 11 May 2023 on the adequacy of the Protection Afforded by the EU-U.S. Data Privacy Framework (2023/2501(RSP)), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html.

(2) The European Parliament believes that European citizens do not have access to effective legal remedies under EO 14086. Although EO 14086 creates a redress mechanism for European citizens, the decision of the competent authority is not intended to be made public, which means that data subjects who file complaints lack the ability to both appeal a decision and claim damages.

The EU Parliament furthered its stance, stating:

(1) The United States still lacks a federal data protection law, and Executive Order 14086 can be amended or revoked by the U.S. President at any time, undermining any long-term guarantee of the protection of EU citizens' data.
(2) The European Commission is required to assess the adequacy of a third country based on both its laws and regulations, and how they are implemented in practice. The EU Parliament is concerned that the United States has not demonstrated that it has the necessary safeguards in place to protect EU citizens' data.
(3) The DFP principles issued by the U.S. Department of Commerce were not considered to have been sufficiently amended subsequent to the criticisms of the EU-US Privacy Shield, continuing to fail in providing an essentially equivalent level of data protection to that provided under the GDPR.

On July 10, 2023, the European Commission adopted its adequacy decision for the DPF, finding that the proffered revisions were sufficient to meet the "essentially equivalent" standard.[157] U.S. companies and organizations (as well as their European subsidiaries and other entities) may now transfer personal data to participating companies in the United States without having to either take extra steps to protect the data (such as signing standard contractual clauses) or risk breaking the GDPR. The relevant companies must first join the DPF by self-certifying that they follow a set of privacy rules issued by the U.S. Department of Commerce.

Under the DFP, companies that want to be certified must follow seven principles:

(1) Notice: Companies must tell people what data they collect and how they use it.
(2) Choice: People must have the right to choose whether or not to let companies collect and use their data.

157. European Commission Press Release, European Commission Adopts Adequacy Decision for EU-U.S. Data Privacy Framework (July 10, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

(3) Accountability for onward transfer: Companies must be accountable for how they share personal data with other companies.
(4) Security: Companies must protect personal data from unauthorized access, use, or disclosure.
(5) Data integrity and purpose limitation: Companies must collect and use personal data in a way that is accurate and consistent with the purpose for which it was collected.
(6) Access: People must have the right to access their personal data and have it corrected or deleted.
(7) Recourse, enforcement, and liability: People must have the right to file complaints about how companies handle their personal data, and companies must be held accountable for violating the DPF principles.

In addition to these seven principles, DPF-certified companies must follow sixteen "Supplemental Principles" and provide additional details about how companies must comply with the seven core principles.

(4) Swiss-US Data Privacy Framework

As Switzerland is not a member of the EU or the EEA, but rather of only the Schengen Area, the Swiss-US Data Privacy Framework was subsequently adopted, following the EU-US. Under the Swiss-US DPF, the Swiss Federal Data Protection and Information Commissioner (FDPIC) has the same authority as the European Union Data Protection Authorities (DPAs). However, the definition of "sensitive data" under the Choice Principle is modified slightly under the Swiss-US DPF to include ideological views or activities, information on social security measures, or administrative or criminal proceedings and sanctions that are not pending.[158]

(5) October 2023 UK-US Data Bridge Regulations

The United Kingdom government published the data protection regulations (the "UK-US Data Bridge Regulations"), which adopt an adequacy decision for the United States (the "UK-US Data Bridge") and came into force on October 12, 2023.[159]

The UK-US Data Bridge recognizes that the United States offers an adequate level of data protection where the transfer is to a U.S. organization that (1) is listed on the DPF, and (2) participates in the UK Extension to the DPF.[160] The Information Commissioner's Office (ICO) and EU pri-

158. Privacy Shield Framework, SWISS-U.S. PRIVACY SHIELD FAQS, https://www.privacyshield.gov/ps/swiss-us-privacy-shield-faqs (last visited Oct. 19, 2023).
159. Data Protection (Adequacy) (United States of America) Regulations 2023, SI 2023/1028 (UK), https://www.legislation.gov.uk/uksi/2023/1028/regulation/1/made.
160. *Id.* § 3.

vacy activists have commented on the UK-US Data Bridge and the DPF.[161] Prevalent concerns include:

(1) The UK-US Data Bridge differs from the United Kingdom's GDPR in (a) the right to be forgotten; (b) the right to withdraw consent; and (c) the right to obtain human review of automated decisions—potentially resulting in UK residents lacking equivalent control over personal data.
(2) "Sensitive information" under the UK-US Data Bridge does not specify the UK GDPR's categories of personal data, and rather provides for a broad concept providing that any data may be designated as sensitive by the transferring entity, meaning that UK-based entities must clearly label sensitive data as such when transferring information to a U.S.-based UK Extension certified entity to remain in compliance with the GDPR.
(3) The United States does not have regulations in place for employment following a completed conviction record, whereas, in the United Kingdom, a "spent" conviction is a conviction that is no longer considered relevant for the purposes of employment or other background checks, risking that spent conviction data may be used for a variety of purposes, such as employment, housing, and immigration decisions in the United States.

f. *THE OECD and the EU Issue Declaration on Government Access to Personal Data Held by Private Sector Entities, by Elisabeth Axberger*[162]

(1) Introduction

In today's digital economy, different data governance models have emerged. In contrast to the noninterventionist era that facilitated globalization, the increase in conflicting data protection regulations is fragmenting the international community. It is clear, however, that a frictionless flow of data is the source of great economic and societal potential. Yet, debates over international agreements—such as the EU-U.S. Data Privacy Framework—have repeatedly given rise to uncertainties for the future of cross-border

161. Information Commissioner's Office, The UK Government's Assessment of Adequacy for the UK Extension to the EU-US Data Privacy Framework for the General Processing of Personal Data (Sept. 21, 2023), https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions-on-adequacy/the-uk-government-s-assessment-of-adequacy-for-the-uk-extension-to-the-eu-us-data-privacy-framework.

162. Elisabeth Axberger is an LLM graduate and Data Privacy Research Fellow at the University of Texas at Austin Strauss Center for International Security and Law.

data flows, and governments continue to enact legislation that limits transfers to address issues of privacy and national security.[163]

Private sector entities process significant amounts of personal data. This information is valuable for governments for a variety of purposes, perhaps most notably, to enable national security and law enforcement efforts. The issue of government access to privately held data was at the core of the Court of Justice of the European Union's (CJE") review of the EU-U.S. adequacy agreement, and the recent reciprocity requirements in Executive Order 14086 has put EU member states' frameworks under similar scrutiny.[164] Moreover, a considerable number of law enforcement cases involve electronic evidence located in other countries, which has spurred an increase in national legislation to ensure cross-border access.[165] There is a fear that these developments could lead to mistrust in transnational data flows, which could prompt governments to invoke data localization requirements that could be detrimental to the global economy.

To advance the debate about international cooperation on these matters, the Organization for Economic Co-operation and Development (OECD) has worked to establish common privacy standards. In December 2022, the organization adopted the Declaration on Government Access to Personal Data Held by Private Sector Entities (Declaration).[166] The Declaration articulates commonalities between member countries to help restore trust in data flows between democratic nation states. It aims to create "a shared understanding among like-minded democracies of protections for privacy and other human rights and freedoms in place for law enforcement and national security."[167] The OECD stated the importance of emphasizing similarities to increase trust between nation states that, although their frameworks are not identical, share the same views on democracy and the rule of law.[168] While it is not binding, the Declaration marks the first time democracies have come together and publicly issued a common

163. World Economic Forum, Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows 3 (Jan. 2023), https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf.

164. Exec. Order No. 14086, 87 Fed. Reg. 62283; U.S. DOJ, Nat'l Sec. Div., Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086, https://www.justice.gov/d9/2023-07/Supporting%20Memorandum%20for%20the%20Attorney%20General%27s%20designation%20of%20EU-EEA.pdf.

165. For example, the Cloud Act and the coming EU e-Evidence Regulation. Theodore Christakis, Kenneth Propp, Peter Swire, *Towards OECD Principles for Government Access to Data*, Lawfare (Dec. 20, 2021), https://www.lawfaremedia.org/article/towards-oecd-principles-government-access-data.

166. OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities (Dec. 13, 2022), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 [hereinafter OECD Declaration].

167. *Id.*

168. *Id.*

approach on government access to personal data for national security and law enforcement purposes.[169]

(2) The Declaration

The Declaration is brief. It consists of opening recitals and seven privacy principles. The central theme is the member countries' commitment to "maintaining a global, open, accessible, interconnected, interoperable, reliable and secure internet."[170] While it is recognized that nation states across the globe have a commitment to their citizens to ensure national security, the means to this end must always be consistent with democratic values and the rule of law. Any approach that undermines such values will significantly impede data flows and could have detrimental effects on the global economy.[171]

The Declaration applies to governments when accessing personal data that is in the possession of, or controlled by, private sector entities. The scope was contested during the negotiations. There was an ongoing debate as to whether the principles should govern both indirect and direct access to data. The current text suggests that direct access is excluded, which, from a U.S. perspective, means that the Declaration applies to data collection under the Cloud Act, however, not to direct access pursuant to Executive Order 12333.[172]

To enhance a trust-based common understanding of privacy protections, the Declaration sets out seven principles for government access: (1) legal basis; (2) legitimate aims; (3) approvals; (4) data handling; (5) transparency; (6) oversight; and (7) redress. As these principles are derived from existing frameworks, the OECD is not imposing new concepts on members. While these principles may not seem novel, the agreed-upon language paves the way for more interoperable frameworks internationally.

For example, the first principle states that government access to information held by private sector entities is regulated under the national legal frameworks. Though it requires a legal basis, it does not mandate regulation through statutory law. Rather, the term can be construed more broadly to include executive measures such as intelligence collection pursuant to Executive Order 12333.[173] This option gives more room for governments to maintain existing frameworks, as long as they meet the substantive standards.

---

169. Kenneth Propp, *Gentlemen's Rules for Reading Each Other's Mail: The New OECD Principles on Government Access to Personal Data Held by Private Sector Entities*, Lawfare (Jan. 10, 2023), https://www.lawfaremedia.org/article/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held.

170. OECD Declaration, *supra* note 166.

171. *Id.*

172. Propp, *supra* note 169.

173. *Id.*

Principle II states that government "access supports the pursuit of specified and legitimate aims" and clarifies that legal standards such as necessity, proportionality, and reasonableness apply.[174] Historically, the United States has used reasonableness while the EU has preferred necessity and proportionality. This has been a point of contention for the CJEU. However, the Declaration strives to bridge this gap by stressing that these terms are functionally the same.[175]

The transparency principle emphasizes the importance of having a general legal framework that is accessible to the public such that individuals can evaluate the privacy impacts. It also considers the specific nature of surveillance by stating that all member countries have mechanisms in their national frameworks that balance the interest of "the public to be informed with the need to prevent the disclosure of information that would harm national security or law enforcement activities."[176]

According to Principle VII, member countries also provide effective oversight and redress. The Declaration widens the perspective on redress by acknowledging that both judicial and non-judicial measures can identify and remedy violations effectively. To increase flexibility regarding oversight, the OECD used the terms "effective" and "impartial," rather than "independent," which is used in EU-jurisprudence.[177]

In essence, the Declaration highlights that substance must prevail over form and, by articulating the commonalities, it simultaneously delineates how OECD member countries are distinguished from nation states that allow unconstrained, arbitrary, and disproportionate access. This delineation is designed to increase trust between nation states that, although their frameworks are not identical, share the same values.

(3) Implications for Cross-Border Data Flows

Though some argue that the divergence between the largest economies will never allow compatible surveillance frameworks to enable multilateral agreements and frictionless flow of data, recent efforts such as the OECD Declaration and the new EU-U.S. Data Privacy Framework suggest otherwise.[178] As Cameron Kerry wrote for *Lawfare*, highlighting and

174. OECD Declaration, *supra* note 166.

175. *The OECD Breaks New Ground with Historic Declaration on Government Access to Private Sector Data*, Allen and Overy LLP (Jan. 2023), https://www.allenovery.com/en-gb/global/blogs/data-hub/the-oecd-breaks-new-ground-with-historic-declaration-on-government-access-to-private-sector-data; Propp, *supra* note 169.

176. OECD Declaration, *supra* note 166.

177. *Id.*; Regulation (EU) 2016/679 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) art. 45 [hereinafter GDPR].

178. U.S. DOJ, Nat'l Sec. Div., Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order

comparing surveillance frameworks of different democracies should not be interpreted as "a matter of 'everybody does it,' finger pointing, or a lowest common denominator . . . [but provides] some understanding of what is necessary in a democratic society."[179] Though the Declaration is not binding, it is still an important step in leveraging greater trust in cross-border data flows, and it represents a constructive way to work towards interoperable standards.

For transatlantic data transfers, the Declaration signifies a step in the right direction. While the European Commission has issued a new U.S. adequacy decision, the new agreement has yet to be evaluated by the CJEU, and the court could (at least in theory) consider the Declaration as proof of the United States' commitment to privacy standards.[180] Beyond the EU-U.S. controversy, the new Declaration will likely be a positive contribution to other countries' adequacy determinations and, it is hoped, provide more foreseeability for adequacy agreements as well as convergence in future legislation.

## II. DEVELOPMENTS IN ARTIFICIAL INTELLIGENCE

### A. *Statutory Developments in Artificial Intelligence, by Pahoua Thao*

Prior to 2022, artificial intelligence (AI) was not considered mainstream technology. However, in the past year, the publicity surrounding generative AI websites has caused legislators and courts to focus their attention on AI. In general, all laws governing data privacy can bear upon AI use; however, the recent rise in the potential use of AI has prompted numerous privacy laws or proposals that specifically address AI and consumer rights.

The term "artificial intelligence" is a catchall term used to describe computers and technology that have the capability to imitate human intelligence. AI comprises four main elements: machine processing, machine learning, machine perception, and machine control—where "machine" refers to the AI system conducting data analysis, which can be a code or a network of connected hardware, and "processing," "learning," "perception," and "control" are functions that the machine performs.

14086 (July 10, 2023), https://www.justice.gov/d9/2023-07/Supporting%20Memorandum%20for%20the%20Attorney%20General%27s%20designation%20of%20EU-EEA.pdf.

179. Cameron Kerry, *Will the New EU-U.S. Data Privacy Framework Pass CJEU Scrutiny?*, Lawfare (Aug. 10, 2023), https://www.lawfaremedia.org/article/will-the-new-eu-u.s.-data-privacy-framework-pass-cjeu-scrutiny.

180. GDPR art. 45(2)(c); *see also The OECD Breaks New Ground with Historic Declaration on Government Access to Private Sector Data*, Allen and Overy LLP (Jan. 2023), https://www.allenovery.com/en-gb/global/blogs/data-hub/the-oecd-breaks-new-ground-with-historic-declaration-on-government-access-to-private-sector-data (EU-leaders indicating that the Declaration has been favorably received, but also stressed that the "essentially equivalent" standard will ultimately be measured against EU law).

At the time of this survey, no comprehensive privacy law exists in the United States that bears upon the use of data in AI. At the federal level, a few bills of note have been proposed that specifically address AI:

- The Artificial Intelligence Accountability Act[181] requires the National Telecommunications and Information Administration (NTIA) to study and report on accountability measures for artificial intelligence systems. The NTIA must study, solicit stakeholder feedback about, and report to Congress concerning mechanisms (*e.g.*, audits, certifications, and assessments) to provide assurances that an AI system is trustworthy.
- In June 2023, a bill was introduced to amend 47 U.S.C. § 230.[182] This bill proposes to add a provision to waive immunity under section 230 of the Communications Act of 1934 for claims and charges related to generative AI.
- The Preventing Deep Fake Scams Act[183] proposes to establish the Task Force on Artificial Intelligence in the Financial Services Sector. The Task Force is to report to Congress on issues related to AI in the financial services sector.

With the rise in the use of AI in commercial operations, the potential that AI could be used for discriminatory purposes has become a concern for federal agencies. In response to the potential discriminatory effects of AI, four federal agencies issued a joint statement on AI. On April 25, 2023, the Consumer Financial Protection Bureau, the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission, and the Federal Trade Commission issued a Joint Statement on Enforcement Efforts against Discrimination and Bias in Automated Systems.[184] The agencies jointly pledged to uphold the principles of fairness, equality, and justice as automated systems become increasingly common and may impact civil rights, fair competition, consumer protection, and equal opportunity.[185]

181. The Artificial Intelligence Accountability Act, H.R. 3369, 118th Cong. (1st Sess. 2023).

182. A bill to waive immunity under section 230 of the Communications Act of 1934 for claims and charges related to generative artificial intelligence, S. 1933, 118th Cong. (1st Sess. 2023).

183. The Preventing Deep Fake Scams Act, H.R. 5808, 118th Cong. (1st Sess. 2023).

184. Fed. Trade Comm'n Press Release, FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI (Apr. 25, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-chair-khan-officials-doj-cfpb-eeoc-release-joint-statement-ai.

185. Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems, FTC ET AL. (Apr. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

Five consumer privacy laws went or will go into effect by December 31, 2023. On January 1, 2023, the California Privacy Rights Act (CPRA)[186] and the Virginia Consumer Data Protection Act (VCDPA)[187] went into effect. On July, 1, 2023, the Colorado Privacy Act (CPA)[188] and the Connecticut Data Privacy Act (CTDPA)[189] went into effect. At the end of the year, the Utah Consumer Privacy Act (UCPA)[190] went into effect on December 31, 2023. Numerous states have followed suit and have proposed or enacted privacy bills which would also regulate AI. Many of the proposed privacy bills use the same or similar language that can be found in the privacy laws that went into effect this year.

In 2024, four new privacy laws will go into effect. Those new privacy laws and other notable proposed bills for AI are highlighted below.

- **Delaware:** The Delaware Personal Data Privacy Act[191] provides individuals with the right to opt out of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. This Act is effective on January 1, 2025.
- **District of Columbia:** The proposed Stop Discrimination by Algorithms Act of 2023 (SDAA)[192] would prohibit both for-profit and nonprofit organizations from using algorithms that make decisions based on protected personal traits such as race, color, religion, national origin, sex, gender identity or expression, sexual orientation, familial status, source of income, or disability.
- **Illinois:** H.B. 3563 amended the Department of Innovation and Technology Act[193] to allow the Department of Innovation and Technology to establish the Generative AI and Natural Language Processing Task Force to investigate and report on generative artificial intelligence software and natural language processing software. This statute was effective on August 4, 2023.

186. Cal. Civ. Code §§ 1798.99.28–1798.99.40 (West 2023).
187. Va. Code Ann. §§ 59.1-575 to -585 (West 2023).
188. Colo. Rev. Stat. §§ 6-1-1301 to -1313 (West 2023).
189. Conn. Gen. Stat. Ann. §§ 42-515 to 42-530 (West 2023).
190. Consumer Privacy Act, 2022 Utah Laws 462 (codified at Utah Code Ann. §§ 13-61-101 to -404 (West 2023)).
191. The Delaware Personal Data Privacy Act, H.B. 154, 152d Gen. Assemb., Reg. Sess. (Del. 2023) (codified at Del. Code Ann. tit. 6, §§ 12D-101 to 12D-111 (West 2023)) [effective Jan. 1, 2025].
192. The Stop Discrimination by Algorithms Act of 2023, B25-0114, (D.C. 2023), https://lims.dccouncil.gov/downloads/LIMS/52282/Introduction/B25-0114-Introduction.pdf.
193. The Department of Innovation and Technology Act, H.B. 3563, 103d Gen. Assemb., Reg. Sess. (Ill. 2023) (codified at 20 Ill. Comp. Stat. Ann. 1370/1-80 (West 2023)).

- **Indiana:** Indiana created a consumer privacy law[194] regulating the collection and processing of personal information. The article sets out rules for profiling and automated decision-making and allows individuals to opt out of profiling. The Act is effective January 1, 2026.
- **Maine:** The proposed Data Privacy and Protection Act[195] is a comprehensive bill aimed at protecting consumer data. Section 9615 specifically governs the use of algorithms. The Act provides that covered entities that use algorithms to collect, process, or transfer data in a manner that poses a consequential risk of harm must complete an assessment of the algorithm and provide the assessment to the Attorney General's office. The bill includes a private right of action and allows for the recovery of punitive damages.
- **Massachusetts:**
  - The proposed Massachusetts Data Privacy Protection Act (MDPPA)[196] would require companies to conduct an impact assessment if they use a "covered algorithm" such as machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques, in a way that poses a consequential risk of harm to individuals.
  - An Act Regulating the Use of Artificial Intelligence in Providing Mental Health Services[197] proposes to regulate the use of AI in providing mental health services. The bill provides that the use of AI by any licensed mental health professional in the provision of mental health services must satisfy certain conditions.
  - The proposed Massachusetts Information Privacy and Security Act (MIPSA)[198] creates various rights for individuals regarding the processing of their personal information. Large data holders are required to perform risk assessments where the processing is based in whole or in part on an algorithmic computational process.
  - An Act Preventing a Dystopian Work Environment[199] proposes to require employers to provide employees and independent

194. S.B. 5, 123d Gen. Assemb., 1st Reg. Sess. (Ind. 2023) (codified at Ind. Code Ann. §§ 24-15-1-1 to 24-15-11-2 (West 2023)) [effective Jan. 1, 2026].

195. The Data Privacy and Protection Act, H.P. 1270, 131st Leg., 1st Spec. Sess. (Me. 2023).

196. The Massachusetts Data Privacy Protection Act, S.25, 193d Gen. Ct., Reg. Sess. (Mass. 2023).

197. An Act Regulating the Use of Artificial Intelligence in Providing Mental Health Services, H.B.1974, 193d Gen. Ct., Reg. Sess. (Mass. 2023).

198. The Massachusetts Information Privacy and Security Act, S.227, 193d Gen. Ct., Reg. Sess. (Mass. 2023).

199. An Act Preventing a Dystopian Work Environment, H.1873, 193d Gen. Ct., Reg. Sess. (Mass. 2023).

contractors with a particularized notice prior to the use of an Automated Decision System (ADS) and the right to request information, including whether their data is being used as an input for the ADS, and what ADS output is generated based on that data. The bill also prohibits the use of ADSs in certain circumstances and requires the performance of algorithmic impact assessments.

  - An Act drafted with the help of ChatGPT to Regulate Generative Artificial Intelligence Models Like ChatGPT[200] proposes to regulate generative AI models like ChatGPT. This Act would require any company operating a large-scale generative AI model to adhere to certain operating standards such as reasonable security measures to protect the data of individuals used to train the model, informed consent from individuals before collecting, using, or disclosing their data, and performance of regular risk assessments. The bill further requires any company operating a large-scale generative AI model to register with the Attorney General and provide certain enumerated information regarding the model.

- **Montana:** The Consumer Data Privacy Act[201] creates an omnibus consumer privacy law that regulates data uses, the collection and processing of personal information and profiling and automated decision-making. The Act regulates profiling by automated processes performed on personal data related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. The Act is effective on October 1, 2024.
- **New Hampshire:** An Act Relative to the Expectation of Privacy[202] was proposed. The bill sets out rules for profiling and automated decision-making. The bill enables individuals to opt out of solely automated decisions that produce legal or similarly significant effects concerning the consumer. Profiling is defined as "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[203]

200. An Act Drafted with the Help of ChatGPT to Regulate Generative Artificial Intelligence Models Like ChatGPT, S.31, 193rd Gen. Ct., Reg. Sess. (Mass. 2023).

201. An Act Establishing the Consumer Data Privacy Act, S.B. 384, 68th Leg., Reg. Sess. (Mont. 2023) (codified at Mont. Code Ann. §§ 30-14-2801 to 30-14-2817 (West 2023)) [effective Oct. 1, 2024].

202. An Act Relative to the Expectation of Privacy, S.B. 225, 2023 Sess. (N.H. 2023).

203. *Id.*

- **New Jersey:** A bill was proposed to regulate the use of automated tools in hiring decisions to minimize discrimination in employment.[204] This bill would require that candidates be notified that an automated employment decision tool was used in connection with the application for employment within thirty days of the use of the tool.
- **New York:** The proposed New York Privacy Act[205] would be the state's first comprehensive privacy law. The law would require companies to disclose their use of automated decision-making that could have a "materially detrimental effect" on consumers, such as a denial of financial services, housing, public accommodation, health care services, insurance, or access to basic necessities; or could produce legal or similarly significant effects.
- **Oregon:** The Oregon Consumer Privacy Act[206] creates an omnibus consumer privacy law and sets out rules for profiling and automated decision-making. The Act enables individuals to opt out of processing for the purpose "profiling the consumer to support the decisions that produce legal effects or effects of similar significant significance."[207] Profiling is defined as "an automated processing of personal data for the purpose of evaluating, analyzing or predicting an identified or identifiable consumer's economic circumstances, health, personal preferences, interests, reliability, behavior, location or movements." This Act is effective on January 1, 2024.
- **Pennsylvania:** The proposed amendment to the Administrative Code of April 9, 1929,[208] would direct the Department of State to establish a registry of business operating AI systems in the State. The proposed Consumer Data Protection Act[209] would establish an omnibus consumer privacy law that allows consumers the right to opt out of the processing of their personal data for certain purposes. Profiling is defined as a "form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location

204. An Act Concerning the Use of Automated Tools to Assist with Hiring Decisions and Supplementing Title 34 of the Revised Statutes, A. 49093, 220th Leg., Sess., 2022–2023 (N.J. 2022).

205. New York Privacy Act, S.B. 365, Reg. Sess., 2023–2024 (N.Y. 2023).

206. S.B. 619, 82d Legis. Assemb., Reg. Sess. (Or. 2023) (amending Or. Rev. Stat. Ann. § 180.095 (West 2023)) [effective Jan. 1, 2024].

207. *Id.*

208. Administrative Code of 1929, H.B. 49, Gen. Assemb., Reg. Sess., 2023–2024 (Pa. 2023).

209. Consumer Data Protection Act, H.B. 708, Gen. Assemb., Reg. Sess., 2023–2024 (Pa. 2023).

or movements."[210] The bill also mandates the performance of data protection assessments in connection with "profiling" where the profiling presents a reasonably foreseeable risk for certain impacts on consumers.

- **Rhode Island:** The proposed Rhode Island Data Transparency and Privacy Protection Act[211] would establish an omnibus consumer privacy law that provides consumers the right to opt out of the processing of their personal data for purposes of profiling in furtherance of solely automated decisions. Profiling is defined as "any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[212] The bill also mandates the performance of data protection assessments in connection with "profiling" where the profiling presents a reasonably foreseeable risk for certain impacts on consumers.
- **South Carolina:** Proposed S.B. 404[213] would prohibit any operator of a website, an online service, or an online or mobile application to utilize an automated decision system for content placement for a user under the age of eighteen. The bill includes a private right of action.
- **Tennessee:** The Tennessee Information Protection Act[214] establishes an omnibus consumer privacy law that mandates the performance of data protection assessments in connection with "profiling" where the profiling presents a reasonably foreseeable risk of certain types of impacts on consumers. This Act is effective on July 1, 2025.
- **Texas:** The Texas Data Privacy and Security Act[215] creates requirements enabling individuals to opt out of "profiling" that produces a legal or similarly significant effect concerning the individual. "Profiling" means any form of solely automated processing performed on personal data related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. This Act is effective on July 1, 2024.

---

210. *Id.*

211. Rhode Island Data Transparency and Privacy Protection Act, H.B. 6236, Gen. Assemb., Jan. Sess., 2023 (R.I. 2023).

212. *Id.*

213. S.B. 404, Gen. Assemb., 125th Sess., 2023-2024 (S.C. 2023).

214. Tennessee Information Protection Act, H.B. 1181, Gen. Assemb., Reg. Sess. (Tenn. 2023) (codified at Tenn. Code Ann. §§ 47-18-3301 to 47-18-3315 (West 2023)) [effective July 1, 2025].

215. Texas Data Privacy and Security Act, H.B. 4, 88th Leg. Sess., (Tex. 2023) (codified at Tex. Bus & Com Code Ann. §§ 541.001–541.005 (West 2023)) [effective July 1, 2024].

- **Vermont:** Proposed Bill H. 114[216] would restrict the use of electronic monitoring of employees and the use of automated decision systems (ADSs) for employment-related decisions. ADSs must meet a number of requirements including corroboration of system outputs by human oversight of the employee and creation of a written impact assessment prior to using the ADS.

The easy access to generative AI has caused courts across the United States to address the use of AI in the courtroom. In 2023, fourteen courts issued standing orders addressing the use of generative AI. Below is a summary of notable developments for courts.

In May 2023, Judge Brantley Starr from the Northern District of Texas issued a standing order on the use of AI requiring that all attorneys and pro se litigants appearing in court file on the docket a certificate attesting that either no portion of any filing will be drafted by generative AI or that any language drafted by generative AI will be checked for accuracy, using print reporters or traditional legal databases by a human being.[217] Judge Starr specifically noted that generative AI in its current state, although being incredibly powerful, is prone to hallucinations and bias.

Senior Judge Michael J. Baylson from the Eastern District of Pennsylvania issued a standing order[218] on June 6, 2023. The standing order requires disclosure of the use of AI in the preparation of the filing, and the party must certify that every citation to the law or record in the filing has been verified as accurate.

On June 8, 2023, Magistrate Judge Gabriel A. Fuentes from the Northern District of Illinois issued a standing order[219] for civil cases. The standing order requires that any party using any generative AI tool to conduct legal research or to draft documents for filing with the court must disclose in the filing that AI was used. The party must specifically identify the AI tool that was used and the way in which it was used. The court reminded parties of the applicability of Federal Rule of Civil Procedure 11.

216. H. 114, 2023–2024 Sess. (Vt. 2023).

217. Judge Brantley Starr, *Mandatory Certification Regarding Generative Artificial Intelligence*, N.D. Tex. (Dec. 1, 2023), https://www.txnd.uscourts.gov/judge/judge-brantley-starr.

218. Judge Michael M. Baylson, *Standing Order re: Artificial Intelligence ("AI") in Cases Assigned to Judge Baylson*, E.D. Pa. (June 6, 2023), https://www.paed.uscourts.gov/sites/paed/files/documents/procedures/Standing%20Order%20Re%20Artificial%20Intelligence%206.6.pdf.

219. Magistrate Judge Gabrial A. Fuentes, *Standing Order for Civil Cases Before Magistrate Judge Fuentes*, N.D. Ill. (Dec. 1, 2023), https://www.ilnd.uscourts.gov/_assets/_documents/_forms/_judges/Fuentes/Standing%20Order%20For%20Civil%20Cases%20Before%20Judge%20Fuentes%20rev%27d%205-31-23%20(002).pdf.

Magistrate Judge Jeffrey Cole from the Northern District of Illinois also issued a standing order[220] on the use of AI. Judge Cole's standing order requires the disclosure of what AI tool was used to conduct legal research and/or used in the preparation of any document. The court reminded parties that Federal Rule of Civil Procedure Rule 11 would apply and that certification on a filing will be deemed as a representation by the filer that they have read and analyzed all cited authorities to ensure that such authorities exist.

On July 14, 2023, District Judge Michael J. Newman issued a standing order[221] on the use of AI. The court's order prohibits the use of AI in the preparation of any filing submitted to the court. The order warns that a party in violation of the order may face sanctions or contempt. The order specifically excludes legal search engines and Internet search engines from the AI ban. The order also imposes a duty on all parties to immediately inform the court if they discover the use of AI in any document filed in their case.

As outlined by the courts in the Northern District of Illinois, the improper use of generative AI has severe consequences for attorneys in the form of sanctions.[222] While not every improper use of generative AI will result in sanctions, federal courts are aware of generative AI's shortcomings.[223] Courts have made it clear that attorneys are ultimately responsible for court filings regardless of the tools employed.

AI is a powerful tool when used properly, but, as Judge Starr's standing order notes, generative AI in its current state may be full of hallucinations. The failure to understand how to use AI properly—whether in court or for consumer data collection—may cause more harm than good. Users of AI should understand the laws and rules that they must abide by before using AI tools.

---

220. Magistrate Judge Jeffrey Cole, *The Use of "Artificial Intelligence" in the Preparation of Documents Filed Before this Court*, N.D. Ill. (Dec. 1, 2023), https://www.ilnd.uscourts.gov/_assets/_documents/_forms/_judges/Cole/Artificial%20Intelligence%20standing%20order.pdf.

221. Judge Michael J. Newman, *Standing Order Governing Civil Cases*, S.D. Ohio (Dec. 1, 2023), https://www.ohsd.uscourts.gov/sites/ohsd/files/MJN%20Standing%20Civil%20Order%207.14.23%20Final.pdf.

222. *See* Mata v. Avianca, Inc., 2023 WL 4114965, *1 (S.D.N.Y. 2023) (the court sanctioning attorneys for their use fake quotes and citations created by ChatGPT and for refusing to admit to the use of AI until the court issued an order to show cause).

223. *See* Frier v. Hingiss, 2023 WL 6046840, at *3 n.1 (E.D. Wis. 2023) (reminding counsel that to the extent AI was used, counsel is responsible for any briefing filed regardless of the tools employed).

## III. DEVELOPMENTS IN CASE LAW

### A. *Case Law Developments Related to Advertising Technology, by Tara D. Kennedy*

#### 1. Case Law Narrowing "Subscriber" Status Under the Video Privacy Protection Act

The last year has seen an exponential increase in the number of lawsuits alleging violations of the Video Protection Privacy Act[224] (VPPA). The VPPA was enacted in 1988, after a newspaper published a profile of then-Supreme Court nominee Judge Robert H. Bork, "which contained the titles of 146 films he and his family had rented from a local video store."[225] Despite the fact that brick and mortar video rental stores are now nearly extinct, between October 1, 2022, and September 30, 2023, more than 150 cases were filed raising VPAA claims. Many of these new cases focus on websites that offer video content of any kind (for example, WebMD, sports websites, and even General Mills) and their use of pixel technology to transmit information about videos watched on the website to third parties such as Facebook.

Given the pervasiveness of pixel tracking technology—it would be difficult if not impossible to browse the Internet without encountering websites that utilize pixels—the potential for filing this type of VPPA claim appears nearly limitless. Motions to dismiss such suits have resulted in a mixed bag of decisions, but over the last year some defenses have emerged where courts are beginning to limit the expanding scope of the VPPA. One such area is in the definition of a "subscriber" under the statute. Specifically, several courts have held that the VPPA does not extend to any website visitor, and not even to any person that signs up for an electronic newsletter; instead, to qualify as a "subscriber," a plaintiff must at least allege some relationship between their subscription and access to video content.

#### 2. What Does the VPPA Cover?

The VPPA prohibits "video tape service providers" from "knowingly" disclosing personally identifiable information about a "consumer" of that provider, subject to a few narrow exceptions.[226] The VPPA defines "video tape service provider" in relevant part, as "any 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[.]"[227] Notably, courts have construed "similar audio visual materials" broadly,

224. 18 U.S.C. § 2710.
225. Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1252–53 (11th Cir. 2015).
226. 18 U.S.C. § 2710(b)(1).
227. *Id.* § 2710(a)(4).

"finding that streaming video delivered electronically falls within that definition" with an exception for live broadcasts.[228] A "consumer" is a "renter, purchaser, or *subscriber* of goods or services from a video tape service provider."[229]

The statute creates a private right of action for any consumer whose PII is disclosed in violation of the Act with statutory damages of $2,500, and the potential for punitive damages and reasonable attorney's fees and costs.[230] The private right of action, statutory damages, and widespread use of prerecorded videos on the Internet have made the VPPA an attractive tool for the plaintiff's class action bar, especially given the ubiquitous use of pixel technology on websites containing video content.

3. Cases Dismissing VPPA Claims Where Plaintiff Did Not Adequately Allege "Subscriber" Status

As noted above, one defense increasingly successful at the motion to dismiss stage is the argument that the plaintiff is not a "consumer" under the VPPA because they do not qualify as a "subscriber of goods or services."[231] Courts had previously established that the VPPA does not provide coverage for every visitor to a website that happens to include free video content. Rather, to qualify as a consumer where they have not rented or purchased video content, a plaintiff must be a "subscriber," which requires some relationship such as account registration, subscription to a newsletter or content, or access to restricted content.[232] Over the past year, courts have narrowed this further, finding that just any "subscription" is not enough. Specifically, plaintiffs bringing VPPA claims based on enrollment in electronic newsletters must allege some relationship between their subscription and access to video content. Links to video content on the public website will not suffice; the subscription must contain special or tailored video content for subscribers.

For example, in *Carter v. Scripps Networks, LLC*,[233] the court dismissed a VPPA claim where plaintiffs alleged they were "subscribers" under the

228. *See Stark v. Patreon, Inc.*, 635 F. Supp. 3d 841, 851 (N.D. Cal. 2022) (collecting cases regarding "broad" interpretation covering streaming).

229. 18 U.S.C. § 2710(a)(1) (emphasis added).

230. *Id.* § 2710 (c)(1), (c)(2).

231. *Id.* § 2710(a)(1).

232. *See* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1256 (11th Cir. 2015) (holding that "merely downloading [the provider's] app for free and watching videos at no cost does not make [plaintiff] a subscriber"); Austin-Spearman v. AMC Network Ent. LLC, 98 F. Supp. 3d 662, 669 (S.D.N.Y. 2015) (finding no subscriber relationship where plaintiff merely visited website to watch videos and "did not pay [the provider] for the content on its free website, nor did [plaintiff] 'sign up,' register for an account, establish a user ID or profile, download an app or program, or take any action to associate herself with [the provider]").

233. Carter v. Scripps Networks, LLC, 2023 WL 3061858 (S.D.N.Y. Apr. 24, 2023).

VPPA because they subscribed to HGTV's electronic newsletter and independently watched videos on the HGTV website.[234] The court disagreed, finding that, under the VPPA, "the scope of a 'consumer' is cabined by the definition of 'videotape service provider,' with its focus on the rental, sale, or delivery of audiovisual materials, not a broader category of consumers."[235] As a result, the court found that the plaintiffs' "subscription" to defendant's newsletter was not enough to qualify them as subscribers under the VPPA because their "status as a newsletter subscriber was not a condition to accessing videos on defendant's website," nor did it "enhance or in any way affect the viewing experience."[236] Simply put, the plaintiffs "were subscribers to *newsletters*, not subscribers to *audio visual materials*."[237] That the newsletter contained links directing subscribers back to the website, where they were free to watch—or not watch—videos without any type of obligation, did not create subscriber status, because plaintiffs were no different from any visitor to the website.[238]

Similarly, in *Jefferson v. Healthline Media, Inc.*,[239] the Northern District of California held that "while the VPPA broadly protects paid and unpaid subscribers, not everything that might be labeled a 'subscription' automatically triggers the statute's protections."[240] There, the plaintiff subscribed to the defendant's e-mail list using her name and e-mail address.[241] But the court held that a "subscriber [under the VPPA] is not just someone who provides [their] name and address to a website for some undisclosed purpose or benefit," and dismissed plaintiff's VPPA claim.[242]

In another recent decision, *Gardener v. MeTV*,[243] the Northern District of Illinois reached a similar conclusion. The plaintiffs in *Gardener* alleged they were "subscribers" under the VPPA because they provided their names and e-mail addresses to MeTV when they opened an account. The court held that opening an account with MeTV did not qualify plaintiffs as subscribers under the VPPA, because viewing videos on the website was "separate and apart from" their accounts.[244] The plaintiffs did not receive special access to video content and were "free to watch or not watch [MeTV's] videos without any type of obligation, no different than any of the other

234. *Id.* at *1.
235. *Id.* at *11.
236. *Id.* at *12–13.
237. *Id.* at *12 (emphasis added).
238. *Id.*
239. Jefferson v. Healthline Media, Inc., 2023 WL 3668522 (N.D. Cal. May 24, 2023).
240. *Id.* at *3.
241. *Id.*
242. *Id.*
243. Gardener v. MeTC, NLP, 2023 WL 4365901 (N.D. Ill. July 6, 2023).
244. *Id.* at *4.

[] monthly visitors to the site."[245] Ultimately, the court held the plaintiffs were "subscribers to a *website*, not subscribers to audio visual materials" and therefore dismissed their VPPA claims.[246]

Plaintiffs are testing these decisions, however, in an appeal in *Salazar v. National Basketball Association*.[247] In *Salazar*, the district court agreed with the *Carter* court and held that the plaintiff was not a subscriber under the VPPA because the plaintiff did "not allege that his newsletter subscription allowed him access to the videos on the NBA.com site that any member of the public would not otherwise have, Plaintiff has alleged that he was a "subscriber[ ] to newsletters, not [a] subscriber[ ] to audio visual materials."[248] On appeal, the plaintiff has asked the court to decide whether a subscription to any good or service, not only audio visual materials, is sufficient to qualify as a subscriber under the VPPA, and whether a newsletter containing links to otherwise generally available videos is enough to create a subscriber relationship. The appeal is in the briefing phase, but will provide guidance on the strength of the subscriber defense moving forward.

### B. *Case Law Developments in Session Replay Litigation, by Alexandra N. Cabeza*

Session replay software allows a website operator to monitor and record a website visitor's interactions with the website, namely mouse movements, clicks, keystrokes, search terms, and pages viewed. This software allows a website operator to "replay" the visitor's experience on their website, focusing on how users interact with the website. Companies use this software to understand and enhance a visitor's online experience.

This technology has created a wave of litigation challenging the use of session replay code. Courts in numerous jurisdictions have been inundated with lawsuits related to session replay software involving state and federal wiretap laws and claimed violations of privacy rights. The core of plaintiffs' claims is that by using the software provided by third-party vendors, website operators permit and participate in the interception, use, and/or disclosure of plaintiffs' communications with the website without their consent.

Most cases are in their earliest stages, where defendants are seeking dismissal on several grounds, including a lack of standing, the party exemption rule, and a failure to state a claim under relevant wiretap acts. Arguments

245. *Id.* (citing *Carter*, 2023 WL 3061858, *6).

246. *Id.* (quotation marks omitted and emphasis supplied).

247. Salazar v. Nat'l Basketball Ass'n, 2023 WL 5016968 (S.D.N.Y. Aug. 7, 2023), appeal pending in No. 23-1147 (2d Cir.).

248. *Id.* at *9. The court further noted the complaint "does not allege that the newsletters contained videos" or that "a user must log in to watch the video [content on NBA.com]," or that "the video content he accessed was exclusive to a subscribership." *Id.*

raising a lack of jurisdiction—both personal[249] and subject matter—have been the most successful. Some courts have even considered the issue *sua sponte*.[250] Specifically, courts are finding that plaintiffs are unable to allege a concrete harm necessary to establish an injury in fact, and therefore lack Article III standing to bring these lawsuits.[251] Essential to a claim is plaintiffs' burden of demonstrating the following: (1) an injury in fact, (2) that is fairly traceable to the challenged conduct, and (3) that is likely to be redressed by judicial decision.[252] The harm alleged across these lawsuits is the violation of wiretapping statutes themselves, which bears a close relationship to traditional harms for invasion of privacy torts. But this argument runs contrary to established Supreme Court precedent "as it would mean *any* alleged violation of a wiretap statute necessarily constitutes an injury in fact even without allegations of actual harm."[253]

The lack of standing argument fares noticeably better in session replay cases than other trending data privacy litigation—like pixel healthcare and VPPA lawsuits—because the nature of the data allegedly intercepted, used and/or disclosed does not implicate a protectable privacy interest. Like the court in *Adams* noted, "[T]he plaintiff's alleged harm was not closely related to the harm upon which the tort of intrusion of seclusion is based—or any invasion of privacy tort for that matter—because plaintiff had not alleged the [website operator] had intercepted private communications or personal information."[254] Courts across numerous districts are concluding that the use of session replay code, without more, is insufficient to establish a concrete injury and are dismissing cases at the motion to dismiss stage.[255]

249. Numerous district courts across the country have found a lack of specific jurisdiction over session-replay code claims. *See*, *e.g.*, Rosenthal v. Bloomingdale's, Inc., No. CV 22-11944-NMG, 2023 WL 5179506 (D. Mass. Aug. 11, 2023); Hasson v. Fullstory, Inc., No. 2:22-cv-1246, 2023 WL 4745961 (W.D. Pa/ July 25, 2023); Alves v. Goodyear Tire & Rubber Co., No. CV 22-11820-WGY, 2023 WL 4706585 (D. Mass. July 24, 2023); Licea v. Caraway Home Inc., No. EDCV 22-1791-JGB, 2023 WL 1999496 (C.D. Cal. Feb. 9, 2023); Sacco v. Mouseflow, Inc., No. 2:20-cv-233-TLN-KJN, 2022 WL 4663361 (E.D. Cal. Sept. 30, 2023); Massie v. Gen. Motors Co., No. 1:20-cv-1560-JLT, 2021 WL 2142728 (E.D. Cal. May 26, 2021); Mikulsky v. Noom, Inc., No. 3:23-cv-285-H-MSB, 2023 WL 4567096 (S.D. Cal. July 17, 2023); Schnur v. Papa John's Int'l, No. 2:22-cv-1620-NL, 2023 WL 5529775 (W.D. Pa. Aug. 28, 2023); Mikulsky v. Bloomingdale's, LLC, No. 23-cv-425-L- WVG, 2023 WL 6538380 (S.D. Cal. Oct. 6, 2023).

250. *See* Jones v. Bloomingdales.com LLC, No. 4:22-cv-01095 (E.D. Mo. Sept. 18, 2023).

251. Adams v. PSP Grp., LLC, No. 4:22-CV-1210 RLW (E.D. Mo. Sept. 13, 2023).

252. Spokeo, Inc. v. Robins, 578 U.S. 330, 136 S. Ct. 1540 (2016) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992)).

253. *Adams*, No. 4:22-CV-1210 RLW (E.D. Mo. Sept. 13, 2023) (emphasis added).

254. *Id.*

255. A number of district courts across the country have addressed Article III standing in cases involving session replay code. These courts have all held that where personal or sensitive information has not been shared on the website in question, the plaintiff has not alleged a concrete harm to support standing. *See* Straubmuller v. Jetblue Airways Corp., No. CV DKC 23-384, 2023 WL 5671615, at *4 (D. Md. Sept. 1, 2023) (finding plaintiff lacked Article III

C. *A Year in Review: Meta Pixel, by Lindsey Knapton*

Over the last year, there has been a surge in litigation related to Meta's pixel technology. These lawsuits target businesses that allegedly share protected information with Meta. In particular, cases involving hospitals exploded after the Markup shed light on the common use of the Meta Pixel on hospital websites, followed by the Office of Civil Rights and the U.S. Department of Health and Human Services (HHS) publication of a bulletin on the use of online tracking technologies.[256] But hospitals are not the only target of pixel litigation. Plaintiffs' attorneys across the country have filed suits against entities that collect protected information, which includes other health-related, firearm, tax, and driver's license information.

The Meta Pixel, as it is known, is a snippet of JavaScript code that is placed on a website. This code enables businesses to learn how visitors interact with their websites and to better direct their products and services to potential customers. The pixel works by sharing information about a visitor's actions on a third-party website with Meta. In addition, the pixel also directs the visitor's browser to share information stored in their Facebook cookies with Meta. As a result, both businesses and website visitors can control how much information Meta receives. As case law emerges, these basic notions about how the pixel works have formed the foundation for many court orders.

1. *In re Meta Pixel*, Case No. 22-cv-03580-WHO (United States District Court for the Northern District of California)

Over the last year, numerous cases against Meta were consolidated in the Northern District of California for Meta's role in hospitals' use of the pixel. These cases are now before Judge William H. Orrick. The claims against the original named plaintiffs' healthcare providers—MedStar Health System, Rush University System for Health, and UK Healthcare—have

standing because allegations in the complaint that Session Replay Code on the defendant's website captioned the plaintiff's keystrokes and clicks were insufficient to allege a concrete harm that bears a close relationship to the substantive right of privacy); Cook v. GameStop, Inc., No. 2:22-CV-1292, 2023 WL 5529772, at *2 (W.D. Pa. Aug. 28, 2023) (same); Mikulsky v. Noom, Inc., No. 3:23-CV-00285-H-MSB, 2023 WL 4567096, at *5 (S.D. Cal. July 17, 2023) (same); Lightoller v. Jetblue Airways Corp., No. 23-CV-00361-H-KSC, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (same); Massie v. Gen. Motors, No. 21-cv-787-RGA, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) ("'Eavesdropping' on communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury.").

256. Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, Markup (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites; *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

proceeded separately. In the meantime, hundreds of other cases have been filed against other hospitals, some also naming Meta as a defendant.

Through the course of this litigation, the *In re Meta Pixel* court has issued two significant orders this year that will continue to shape pixel litigation moving forward. In December, the court denied Plaintiffs' Motion for Preliminary Injunction and, then in September, the court denied in part and granted in part Meta's motion to dismiss.[257]

When it denied the preliminary injunction, the court was clear that it did so because of Meta's mitigation efforts, not because plaintiffs had failed to state a plausible claim. In particular, the court pointed to Meta's filtering mechanisms, which it "designed and implemented" as the "'most effective and feasible methods' to address the receipt of sensitive information."[258] The court noted that discovery would also be necessary to clarify both the scope of the problems and the potential solutions.[259] For these reasons, the court denied the preliminary injunction.

Again, in its motion to dismiss, Meta leaned into its mitigation efforts to defend the collection of any protected information. Consistent with its preliminary analysis of the claims, the court refused to dismiss the case against Meta in its entirety. Although the court initially indicated that it was inclined to dismiss some claims without leave to amend, plaintiffs convinced the court that they could amend their complaint to state a claim. The court ultimately dismissed with leave to amend the following claims: the common-law privacy, violation of California's Comprehensive Computer Data Access and Fraud Act (CDAFA), negligence per se, trespass, larceny, violation of California's Unfair Competition Law (UCL), and violation of California's Consumer Legal Remedies Act (CLRA). But the court refused to dismiss claims for violations of the federal wiretap law, Electronic Communications Privacy Act of 1986 (ECPA); violation of the state wiretap law, the California Invasion of Privacy Act; breach of contract; and unjust enrichment.[260] In large part, the court found many of Meta's arguments were evidence-bound and thus not ripe for resolution at the motion to dismiss stage. As this case proceeds towards class certification and summary judgment, it will likely continue to influence the broader ecosystem of pixel litigation.

257. *In re* Meta Pixel Healthcare Litig., 647 F. Supp. 3d 778 (N.D. Cal. 2022) (order denying preliminary injunction); Doe v. Meta Platforms, Inc., No. 22-CV-03580-WHO, 2023 WL 5837443 (N.D. Cal. Sept. 7, 2023) (order on motion to dismiss)

258. *In re* Meta Pixel Healthcare Litig., 647 F. Supp. 3d at 805.

259. *Id.* at 790.

260. *Meta Platforms, Inc.*, 2023 WL 5837443, at *17.

2. *Kurowski v. Rush System for Health*, No. 22 C 5380 (United States District Court for the Northern District of Illinois)

The *Rush Health* case has also become influential in *Meta Pixel* litigation. This early adtech case is before Judge Matthew F. Kennelly in the Northern District of Illinois. In it, plaintiffs allege that Rush deployed adtech, including the Meta Pixel and Google Analytics, on its public-facing website and within its patient portal. Even so, in two separate orders, the court largely granted the hospital's motions to dismiss claims related to its use of the Meta Pixel.[261]

This case has paved the way for how other courts have addressed violations of the federal Wiretap Act. The Wiretap Act has a "party exception," which essentially permits a party to the communication to "intercept" the communication. Here, there was no question that the hospital was a party to plaintiff's communications on the hospital's website. The only issue was whether the criminal or tortious rule barred the application of the Wiretap Act's party exception. In its second order, the *Rush Health* court took great efforts to close the door on such an argument. Not only did the court find that the plaintiffs failed to allege "any particular health or treatment information" was disclosed to Meta, but the court explained that the Department of Health and Human Services' guidance on website tracking technologies is not entitled to deference.[262] In addition, the court noted that the plaintiffs had failed to identify any independent criminal or tortious purpose from the alleged interception.[263]

Similarly, the analysis of the intrusion upon seclusion claim in *Rush Health* is widely cited in *Meta Pixel* litigation. Specifically, the court rejected the plaintiffs' argument that Rush "bugs" its own web properties by placing third-party cookies on them that are disguised as belonging to Rush. But even with plaintiff's new theory, the *Rush Health* court found that the hospital could not have intruded on plaintiffs' communications as it was the intended recipient.[264] Courts continue to cite the *Rush Health* orders in recent decisions and will likely continue to do so.

3. *Cousin v. Sharp Healthcare*, Case No. 22-cv-2040-MMA (DDL) (United States District Court for the Southern District of California)

One such order that cites *Rush Health* is the July order in *Cousin v. Sharp Healthcare* before Judge Michael Anello in the Southern District of

261. Kurowski v. Rush Sys. for Health, No. 22 C 5380, 2023 WL 4707184 (N.D. Ill. July 24, 2023); Kurowski v. Rush Sys. for Health, No. 22 C 5380, 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023).

262. *Kurowski*, 2023 WL 4707184, at *6–8.

263. *Id.* at *9.

264. *Id.* at *17–18.

California. In this order, the court dismissed five claims against Sharp Healthcare for its use of the Meta Pixel: (1) breach of fiduciary duty; (2) violation of common law invasion of privacy—intrusion upon seclusion; (3) invasion of privacy under the California Constitution; (4) violation of the California Confidentiality of Medical Information Act; and (5) violation of the California Invasion of Privacy Act. Unlike other pixel cases, Sharp Healthcare did not use the pixel in its user authenticated patient portal. But even before reaching the merits of Sharp's claims, the court dismissed Plaintiffs' allegations as factually deficient because the plaintiffs never explained how they used Sharp's website.[265]

Although the court found that most claims should be dismissed, it did not accept all of Sharp Healthcare's arguments. First, it found that the disclosure of health information from the hospital's appointment scheduling page may constitute a "highly offensive" intrusion sufficient to withstand dismissal.[266] Second, the court decided that the question of whether Meta or the hospital intruded is best left for summary judgment.[267] Last, the court found whether the communication was intercepted in transit and whether the hospital had either aided, agreed, employed, or conspired with Meta sufficient to survive a motion to dismiss. Even so, before the court will consider these claims again, plaintiffs must add specificity to the complaint.

4. *Hartley v. University of Chicago Medical Center* (United States District Court for the Northern District of Illinois)

In yet an even more recent *Meta Pixel* order, the court again cited the *Rush Health* case. In the case before Judge Harry D. Leinenweber against the University of Chicago Medical Center (UCMC), the court dismissed claims for violation of the federal Wiretap Act, breach of implied duty of confidentiality, and intrusion upon seclusion. Like in *Rush Health*, the *UCMC* court agreed that the hospital is a necessary party to any communication between a patient and the hospital. And again, like *Rush Health*, the court found plaintiffs' "similar generalizations as to what UCMC was communicating with Facebook" insufficient to plausibly violate HIPAA, and thus preclude the application of the party exception.[268] The court also found that, absent specificity, plaintiff failed to allege a breach of any duty of confidentiality. And like in *Rush Health*, the court found no intrusion

265. Cousin v. Sharp Healthcare, Case No.: 22-cv-2040-MMA (DDL), 2023 WL 4484441, at *5–7 (S.D. Cal. July 12, 2023).

266. *Id.* at *12.

267. *Id.*

268. Hartley v. Univ. of Chi. Med. Ctr., No. 22 C 5891, 2023 WL 7386060, at *4 (N.D. Ill. Nov. 8, 2023).

upon seclusion claim where plaintiff initiated the publication of her information to Meta.

5. Developing Legal Trends

Because most cases involving the Meta Pixel were filed only within the last year, few courts have reached the merits of plaintiffs' common-law and statutory claims. These claims frequently include violations of state and federal wiretap laws, intrusion upon seclusion, negligence, unjust enrichment, breach of fiduciary duty, and breach of contract. To the extent that courts have addressed those claims in motions to dismiss, several trends are beginning to emerge, suggesting how courts may address pixel-related claims moving forward.

First, claims related to the Meta Pixel must include specific allegations about how a plaintiff used a website. This is because a URL or button click alone is not protected information. Without such details, it is unclear that protected information has been disclosed. As the *Sharp Healthcare* court found, plaintiffs must provide "meaningful factual support as to what activities each Plaintiff engaged in on [the hospital's] website and what information each Plaintiff provided. *Sharp Healthcare*, 2023 WL 4484441, at *3. In another case, the court found plaintiff's allegations sufficient where she alleged that she entered data relating to her heart issues and high blood pressure in MyChart and then later received advertisements on Facebook for high blood pressure medication.[269] Following this order, courts have found such allegations to be the bare minimum required by plaintiffs in Meta Pixel cases. This would include details about the plaintiff's use of the hospital's website and the nature of the information disclosed. Courts generally dismiss similar claims in the absence of these core details.[270]

Second, website owners do not intrude by using the pixel on their own websites. Instead of an intrusion, courts largely agree that a hospital's use of the pixel amounts to a disclosure or publication as the hospital was the intended recipient of the information.[271]

Third, courts—and even some plaintiffs' counsel—largely now agree that hospitals are a party to a website visitor's communications on the hospital's website.[272] Some plaintiffs are now choosing to litigate whether a

269. Doe v. Regents of Univ. of Cal., Case No. 23-cv-00598-WHO, 2023 WL 3316766, at *4 (N.D. Cal. May 8, 2023).

270. *See, e.g.*, *Hartley*, 2023 WL 7386060; Murphy v. Thos. Jefferson Health, Civ. Action No. 22-4674, 2023 WL 7017734 (E.D. Pa. Oct. 10, 2023).

271. *Kurowski*, 2023 WL 4707184, at *8 ("The harm caused by Rush, if any, continues to be its alleged disclosure of the Kurowski's private health information."); *Hartley*, 2023 WL 7386060, at *3 ("Since Plaintiff is complaining about what she thinks UCMC told Facebook, her complaints are with the publication, and not any intrusion, which she probably initiated.").

272. *Hartley*, 2023 WL 7386060 (finding the hospital a necessary party to the communication); *Kurowski*, 2023 WL 4707184, at *2 (observing the parties do not dispute that the hospital was the intended recipient of the allegedly intercepted communications).

hospital's use of the Meta Pixel is a criminal or tortious act. To date, courts have rejected such arguments.[273] However, at least one court has left open the door open to reconsider with more specific allegations.[274]

Last, class certification is likely to present challenges for plaintiffs' counsel if they proceed past the motion to dismiss phase. In this last year, we have seen at least one court deny class certification for claims related to the Meta Pixel because plaintiffs failed to show that common issues of law and fact predominate over individual issues and that class certification is a superior method for adjudicating the claims.[275] Specifically, the court found that the "highly offensive" standard for an intrusion upon seclusion claim is a high standard that will require consideration of the exact type of information the hospital shared with Meta.[276] But unlike the *MedStar* case, the pixel case against Virginia Mason Medical Center has slowly lurched forward after an unsuccessful appeal of the trial court's adoption of plaintiffs' proposed order granting class certification in late 2021.[277]

The next year will undoubtedly be filled with new Meta Pixel decisions and new legal arguments as plaintiffs continue to file novel cases and claims and courts are steadily issuing orders.

## IV. NOTABLE ENFORCEMENT ACTIONS

### A. *Privacy Breaches, Settlements, and Regulator Activity: A Year (and Then Some) in Review, by Josh Hansen*

The last year (and then some) has brought significant changes to the status quo when it comes to regulator privacy/security enforcement. Regulators have shown an increased willingness to revive "dead" laws, hold executives accountable, embrace expansive readings of their authority, impose more prescriptive requirements, target data brokers, and protect children. Join me on this journey as we walk through some of the more notable decisions in those areas.

#### 1. The FTC Revives Dormant Rule to Address Disclosures of Medical Data.

In early 2023, the FTC reached separate settlements with two companies—GoodRX and BetterHelp—for alleged violations of the Health

273. *Kurowski*, 2023 WL 4707184, at *2–4 (rejecting plaintiff's allegations that by violating HIPAA, the hospital acted with a criminal or tortious purpose); *see also Murphy*, 2023 WL 7017734.

274. *Kurowski*, 2023 WL 4707184, at *2–4.

275. Doe v. MedStar Health, Inc., Case No. 24-C-20-000591, 2023 WL 4931348, at *10 (Md. Cir. Ct. Mar. 10, 2023).

276. *Id.* at *17.

277. *See* Doe v. Virginia Mason Med. Ctr., Case No. 19-2-26674-1 SEA (King Cnty. Super. Ct.).

Breach Notification Rule.[278] That rule requires companies not governed by HIPAA to notify the FTC and any impacted individuals when there is "breach"—unauthorized processing—of a person's identifiable health information.[279] Although the FTC issued the rule in 2009, it had never brought an enforcement action—until 2023.

The FTC revived the rule in their lawsuit against GoodRX and a month later in a complaint against BetterHelp.[280] Both cases were premised on the companies disclosing health records to advertisers via third-party trackers (such as the Meta Pixel) and other third parties, despite stating they did not do so in their privacy policies. The FTC asserted those disclosures violated the Health Breach Notification Rule. Specifically, the FTC alleged the disclosures, which occurred without the user's authorization, constituted a security breach requiring notice—which the companies did not provide. And the FTC added an FTC Act Section 5 claim on the grounds that the misrepresentation about disclosures constituted an unfair/deceptive practice. Both GoodRX and BetterHelp settled with the FTC; they agreed to, among other conditions, refrain from sharing health information with advertisers (except in limited situations) and obtain consent before disclosing information to other parties.[281]

These cases, along with a similar complaint that the FTC filed in May 2023, reflect a renewed focus on health information beyond the confines of HIPAA.[282] The FTC has breathed new life into its authority in the space, and its recent proposed rulemaking on the Health Breach Notification Rule suggests this will be an area of continued focus.[283] Some practical takeaways:

---

278. Stipulated Order for Permanent Injunction, Civil Penalty, and Other Relief, United States v. GoodRx Holdings, Inc., No. 3:23-cv-460 (N.D. Cal. Feb. 17, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf; Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 14, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf.

279. *Complying with FTC's Health Breach Notification Rule*, Fed. Trade Comm'n (Jan. 2022), https://web.archive.org/web/20230921095737/https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0; *see also* 16 C.F.R. § 318 (2023).

280. *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising*, Fed. Trade Comm'n (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising#:~:text=The%20Federal%20Trade,and%20other%20companies; United States v. GoodRx Holdings, Inc., Case No. 3:23-cv-00460-DMR (N.D. Cal.); *In re* Betterhelp, Inc., FTC Complaint.

281. *See* Stipulated Order, *supra* note 278 (GoodRX); Decision and Order, *supra* note 278 (BetterHelp).

282. *See* Complaint, United States v. Easy Healthcare Corp., Case No. 1:23-cv-03107 (N.D. Ill.), https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf.

283. *FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule*, Fed. Trade Comm'n (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule.

- **Key Takeaway #1.** There are restrictions on the use of health information even for companies not regulated by HIPAA.
- **Key Takeaway #2.** A privacy policy must accurately reflect disclosures of personal information.

2. Privacy and Security Liability Comes for Leadership.

The FTC, SEC, and DOJ have sought (and secured) civil or criminal penalties against senior executives—CEOs, Chief Information Security Officers (CISOs), etc. We will walk through a few of these cases.

- **Uber's Security Officer.** A jury convicted Uber's former security officer, Joseph Sullivan, of two federal crimes (obstruction and concealment of a felony) for his role in covering up a data breach at Uber. Upon learning of the breach, he tried to keep the breach hidden. He tried to conceal it from the FTC—who was investigating Uber's security practices due to an earlier breach—by signing off on documents that he knew were misleading. He also paid the threat actors a bug bounty that was ten times the maximum allowed under the program and had them sign nondisclosure agreements attesting that no data was exfiltrated, even though he knew this was false. [Another Uber executive would later state this payment was akin to extortion].[284]
- **Drizly's CEO.** Drizly's CEO, James Rellas, entered into a settlement agreement with the FTC that imposes conditions on him that persist even after he leaves the company. The FTC alleged Drizly and Mr. Rellas learned of various security failures—missing or deficient MFA, policies, access controls, and threat monitoring. And, despite making public proclamations about maintaining robust security, the company and Mr. Rellas failed to address those shortcomings or even hire a senior executive responsibility for security. After the FTC filed a complaint against Drizly and the CEO, they both settled. Mr. Rellas agreed to implement an information security program at any company he works at as an executive within the next ten years that collects personal data on more than 25,000 people, while Drizly agreed to various remedial measures (*e.g.*, destroying data, limiting collection, and obtaining independent assessments).[285]
- **Solar Winds' CEO.** The SEC charged Solar Winds' CISO with fraud in connection with misleading investors about the company's

284. *See* Press Release, U.S. Atty's Office, N.D. Cal., Former Chief Security Officer of Uber Convicted of Federal Charges for Covering up Data Breach Involving Millions of Uber User Record (Oct. 5, 2022)), https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach.

285. Decision and Order, *In re* Drizly, LLC, FTC (Jan. 10, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023185-drizly-llc-matter.

> security posture. [You may recall Solar Winds for its supply-chain hack: a threat actor compromised SolarWinds' security tool, and the company unknowingly pushed out that compromised code (and the resulting vulnerability) to its customers who used the tool.] The company claimed in public filings that it had a robust security posture and adhered to NIST frameworks. But the SEC alleges those were lies. Allegedly, the CISO acknowledged during an internal presentation that the "current state of security leaves us in a very vulnerable state for our critical assets," while the company lacked policies for most of the NIST they claimed to follow, and executives were told of widespread noncompliance with key policies. The SEC summed up the case by stating: "We allege that, for years, SolarWinds and [the CISO] ignored repeated red flags about SolarWinds' cyber risks, which were well known throughout the company and led one of [the CISO's] subordinates to conclude: 'We're so far from being a security minded company.'"[286]

These cases are a warning sign to executives: take privacy and security seriously because the stakes are now personal. But these cases are not signals that executives are at risk due to regular/routine shortcomings. Instead, consider the following takeaways:

- **Key Takeaway # 1.** Executives are likely not at risk for routine activities; regulators brought charges where there egregious, intentional, and irregular behavior.
- **Key Takeaway # 2.** The FTC will impose sanctions on executives that stay with them and affect how their future job opportunities.
- **Key Takeaway # 3.** Ransom payments remain legal, but companies cannot extract knowingly false statements or use them to conceal a breach.

3. OCR Takes Expansive Reading of HIPAA and Online Trackers.

The United States Department of Health and Human Services Office for Civil Rights (OCR)—the regulator who enforces HIPAA—issued subregulatory guidance stating OCR's position that the use of online trackers can constitute a HIPAA violation.[287] Specifically, OCR states that using these tracking tools—such as pixels, cookies, and session-replay tools—can cause

286. Press Release, U.S. SEC, SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures (Oct. 30, 2023) https://www.sec.gov/news/press-release/2023-227.

287. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dep't of Health & Hum. Servs. (Dec. 1, 2022), https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html.

an unauthorized disclosure of protected health information (PHI). A few months after issuing the guidance, OCR signaled this is an area of focus by sending a joint letter—cosigned by the FTC—to approximately 130 hospitals and telehealth providers in which the regulators highlighted OCR's guidance and the FTC's enforcement of the Breach Notification Rule (discussed above).[288]

To understand OCR's guidance, one needs a basic grasp of the technology underlying these tracking tools. These tools are third-party code that a company embeds into its website to track user activity and direct the user's browser to send that information to a third party.[289] The shared information includes details such as the user's IP address as well as details on the user's activity: webpages visited, actions taken (such as links clicked), and, in limited situations, text entered.

In its guidance on those tools, OCR starts by stating that regulated entities using online trackers are disclosing information (even though it is the user's browser that shares the data with the third party) and that a user's IP address "generally is PHI" (even without identifying details such as name or email address). The premise is that tracked information is PHI because it concerns a user's care or payment for care and "connects the individual to the regulated entity."[290] But then, OCR reveals the analysis is more nuanced: one must consider whether the tracking occurred on an authenticated page (which requires a user login before accessing) or unauthenticated page (which does not require a login).

- **Authenticated Pages.** OCR states that tracking tools on authenticated pages generally have access to PHI, and so a regulated entity must ensure that their use of the tools complies with the HIPAA Privacy Rule. [Basically, turn them off or execute a business associate agreement.]
- **Unauthenticated Pages.** Unlike authenticated pages, OCR explains that tracking tools on unauthenticated pages generally do not have access to PHI. But OCR states that the tools receive PHI if they collect an IP address when a user visits a website to search for available appointments, and they may access PHI if they monitor information on pages addressing specific symptoms.

288. *HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies*, U.S. Dep't of Health & Hum. Servs. (July 20, 2023), https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html.

289. Again, worth repeating: the website is not actually sharing the information with the third party—the user shares their information with the third party.

290. *Office for Civil Rights*, *supra* note 288.

In short, OCR takes the position that the use of tracking tools can involve a disclosure of PHI, even when the only potentially identifying characteristic is an IP address.

Suffice to say, the guidance is causing a ripple effect through the industry and has drawn some fierce criticism. One district court recently held that the guidance—which the court ruled was not entitled to deference—was not persuasive because its interpretation of what constitutes PHI "goes well beyond the meaning of what the statute can bear."[291] And trade groups have also gotten in on the action. In a letter to OCR, the American Hospital Association (AHA) urged OCR to suspend its "rule" (more on that terminology later) because it erred by treating an IP address as PHI.[292] The AHA argued that an IP address should not be treated as PHI for a few reasons, including that the user may be searching for general medical information or seeking nonmedical details (such as hours). The AHA reiterated their concerns in a letter to Congress and added that the guidance would have negative policy implications, such as limiting the use of analytic tools that help hospitals tailor guidance.[293] When none of those gained sufficient traction, the AHA sued OCR alleging that the guidance reflects improper rulemaking.[294] That lawsuit is pending.

4. Data Brokers Find Themselves in the FTC Crosshairs.

The FTC filed a lawsuit against Kochava alleging the company engaged in unfair practices by selling precise location data.[295] [Kochava tried to stop this lawsuit by preemptively suing the FTC. But that did not pan out: the court dismissed that complaint without leave to amend.][296] The crux of the FTC's complaint was that Kochava substantially harmed consumers because, by selling data that could identify them and reveal their movements to/from sensitive locations, the company put consumers at substantial risk of harm from third parties.[297] The FTC pressed two theories why

291. Kurowski v. Rush Sys. for Health, 683 F. Supp. 3d 836, 844 (N.D. Ill. 2023).

292. Melinda Reid Hatton, AHA Letter to OCR on HIPAA Privacy Rule, Online Tracking Guidance, Am. Hosp. Ass'n (May 22, 2023), https://www.aha.org/lettercomment/2023-05-22-aha-letter-ocr-hipaa-privacy-rule-online-tracking-guidance.

293. Stacey Hughes, *AHA Responds to Senate RFI on Health Data Privacy*, Am. Hosp. Ass'n (Sept. 28, 2023), https://www.aha.org/lettercomment/2023-09-28-aha-responds-senate-rfi-health-data-privacy.

294. Complaint, Am. Hosp. Ass'n v. Rainier, No. 4:23-cv-01110-P (N.D. Tex. Nov. 2, 2023), https://www.aha.org/legal-documents/2023-11-02-case-complaint-aha-tha-thr-united-health-care-system-v-rainer.

295. Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2023), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

296. Kochava Inc. v. FTC, No. 2:22-cv-00349-BLW, 2023 WL 3250496 (D. Idaho May 3, 2023).

297. Complaint, FTC v. Kochava Inc., Case No. 2:22-cv-00377-DCN (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.

consumers suffered a substantial injury (an element of an unfair practice claim). First, the FTC alleged Kochava's sale of location data constituted a direct harm because the disclosure of sensitive data is an invasion of privacy. Second, the FTC alleged Kochava's practices created an increased risk of secondary harms because a company using the data could draw inferences (*e.g.*, someone has a specific medical condition) and use that information to inflict harm. Kochava moved to dismiss on a variety of grounds.

In granting Kochava's motion to dismiss, the court explained that it did not buy the FTC's position on either theory of how Kochava substantially harmed consumers.[298] The court rejected the direct-harm contention because the FTC had not shown a sufficiently severe invasion of privacy. The court highlighted that (1) the potential harm comes from inferences—which are often unreliable; (2) the data is available through other means; and (3) the FTC did not allege how many users were impacted. Next, the court rejected the secondary harm theory because the FTC failed to alleged that Kochava's practices were likely to create an increased risk of injury—the FTC merely claimed the sales *could* lead to such harm.

The FTC filed an amended complaint. Kochava responded by urging the court to not make the new complaint public because it is "rife with false statements" as well as "false and inflammatory allegations clearly aimed at misleading this court and the public."[299] But the court ruled against Kochava, and the complaint is now publicly available.[300]

5. New York Enforces and Bolsters Its Cybersecurity Requirements.

The New York Department of Financial Services (NYDFS)—the state's regulator for the insurance, financial, and banking industry—has been active on the enforcement and rulemaking front when it comes to the department's rigorous cybersecurity requirements. Those requirements, which are called "New York's Cybersecurity Requirements for Financial Services Companies," apply to anyone operating under or required to operate under authorization from the state's laws on banking, insurance, or financial services.[301]

In May 2023, NYDFS reached a settlement with OneMain Financial Group for violations of NYDFS's cybersecurity rules.[302] NYDFS alleged

298. FTC v. Kochava Inc., 671 F. Supp. 3d 1161, 1174–75 (D. Idaho 2023).

299. Wendy Davis, *Mobile Data Broker Kochava Wants FTC's 'Scandalous' Complaint Kept Under Wraps*, Media Post (June 14, 2023), https://www.mediapost.com/publications/article/386332/mobile-data-broker-kochava-wants-ftcs-scandalous.html.

300. *See id.*

301. N.Y. Comp. Code R. & Regs. tit. 23 § 500.1(e).

302. Consent Decree with OneMain Financial Group, N.Y. Dep't Fin. Servs. (May 24, 2023), https://www.dfs.ny.gov/system/files/documents/2023/05/ea20230524_co_onemain.pdf; *see also Superintendent Adrienne A. Harris Announces $4.25 Million Cybersecurity Settlement with*

OneMain left itself (and its customers) at a significant risk of a cybersecurity incident because it failed to effectively manage third-party service provider risk, manage access privileges, and maintain a formal application security development methodology. In particular, NYDFS flagged a variety of issues, such as OneMain:

- Neglecting to follow its policies on vendor due diligence;
- Allowing administrators to keep default passwords;
- Using shared administrator accounts;
- Failing to address shortcomings identified by internal audit team;
- Storing passwords in a folder called "PASSWORDS" (which was accessible and editable by people across the company);
- Disregarding its obligation to properly train employees or track their training.

Based on those issues, NYDFS and OneMain entered into a consent decree. OneMain has agreed to pay $4.25 million and take various remedial measures within 180 days (including updating policies, implementing training procedures, and adopting a plan to review access privileges).

In early November, NYDFS issued amendments to the cybersecurity rules.[303] [Spoiler: They only got more prescriptive.] The changes add a variety of obligations covering topics such as accountability, incident reporting, and compliance certification. Some of the most notable changes:

- **Compliance Certifications** [500.17(b)]. Submit certifications from the CISO and highest executive attesting to material compliance or submit a written acknowledgment discussing the lack of such compliance.
- **Incident Reporting** [500.17(c)]. Notify NYDFS of cyber-extortion payments within twenty-four hours and explain within thirty days why the payment was necessary.
- **Asset Inventories** [500.13(a)]. Create and maintain a complete, accurate asset inventory.
- **Policy Review** [500.12(a–b)]. Obtain approval for policies each year from senior officer or senior governing body (board of directors or equivalent).
- **Training** [500.14(a)]. Conduct annual (or more frequent) cybersecurity training that includes social engineering for all personnel.

*OneMain Financial Group LLC*, N.Y. Dep't Fin. Servs. (May 25, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202305251.

303. *Second Amendment to 23 NYCRR 500*, N.Y. Dep't Fin. Servs. (Oct. 16, 2023), https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf.

The amendments impose even more onerous obligations on large companies ($20 million in gross revenue + other criteria)—which NYDFS calls "Class A Companies." Those companies must, for example deploy an Endpoint Detection and Response solution, implement a solution for centralized logging and security alerts, and conduct independent audits at a frequency determined by their risk assessment.

6. Children's Privacy Becomes a Focal Point for the FTC.

In 2023, the Federal Trade Commission (FTC) reached settlements with three companies over alleged violations of the Children's Online Privacy Protection Act (COPPA). A few critical points about COPPA before turning to each of the cases. The law, which protects minors under thirteen, generally empowers parents to control how their child's data is used (and when it is deleted), requires and prevents a company from keeping data after it is no longer necessary for its intended purpose. The three FTC settlements all honed in on various aspect of those rules.

- **Amazon.** Amazon agreed to pay a $25 million fine and implement remediation measures following allegations that it improperly retained voice recordings of minors who used Alexa. The FTC alleged that Amazon targeted children and collected recordings of their voice without deleting the data when it was no longer necessary. In some cases, Amazon even kept transcripts after the parent requested the company delete the data.[304]
- **Microsoft.** Microsoft agreed to pay $20 million and adopt various remediation measures to resolve a lawsuit alleging it failed to properly process minors' data or empower parents in connection with the company's online gaming service. Specifically, the FTC faulted Microsoft for (1) collecting information on known minors without first telling the parents about the company's privacy practices; (2) providing parents with incomplete disclosures about what it collected about their child; and (3) retaining information indefinitely on minors whose parents did not consent.[305]
- **Epic Games.** Epic Games, a video game developer, entered a settlement for alleged COPPA violations in connection with its popular game—Fortnite. The company agreed to pay $275 million and adopt a variety of remediation measures (including, a first-of-its-kind term:

304. *Amazon Agrees to Injunctive Relief and $25 Million Civil Penalty for Alleged Violations of Children's Privacy Law Relating to Alexa*, U.S. Dep't of Justice (July 19, 2023), https://www.justice.gov/opa/pr/amazon-agrees-injunctive-relief-and-25-million-civil-penalty-alleged-violations-childrens.

305. *Microsoft Agrees to Pay $20 Million Civil Penalty for Alleged Violations of Children's Privacy Laws*, U.S. Dep't of Justice (June 12, 2023), https://www.justice.gov/opa/pr/microsoft-agrees-pay-20-million-civil-penalty-alleged-violations-children-s-privacy-laws.

a requirement to adopt strong privacy defaults for minors). The settlement came after the FTC filed a lawsuit alleging various COPPA violations, including that Epic Games ignored evidence of children playing the game, failed to obtain parental consent to collect data from minors, and imposed unreasonable barriers for parents requesting deletion of their child's data (and sometimes the company never responded).[306]

## V. NOTABLE SETTLEMENTS

### A. *Advocate Aurora Health Pixel Litigation Settlement, by Robert A. Stines*

In October 2022, a group of plaintiffs initiated a class action against Advocate Aurora Health, Inc. for the alleged failure to properly secure and safeguard personally identifiable information and personal health information, including names, email addresses, phone numbers, computer IP addresses, emergency contact information, appointment information, medical provider information, and medical histories. The initial class complaint was filed in the United States District Court of the Eastern District of Wisconsin.[307] According to the complaint, Advocate configured and implemented a tracking pixel to collect and transmit information from its website to third parties, including information communicated in sensitive and presumptively confidential patient portals and mobile apps like its MyChart portal and LiveWell app.

Before the lawsuit was filed, on October 30, 2022, Advocate posted a Breach Notification on its website in which it disclosed that it used Internet tracking technologies, such as Google and Meta. Advocate learned that pixels or similar technologies installed on their MyChart and LiveWell patient portals, as well as on some of their scheduling widgets, transmitted certain patient information to third-party vendors. In the Breach Notification, Advocate disclosed that the information transmitted to third parties included IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; provider information; appointment or procedure type; and communications between patients and others through MyChart. Advocate made it clear that no social security number, financial account, credit card, or debit card information was involved in the incident.

306. *Epic Games Inc., Developer of Fortnite Video Game, Agrees to $275 Million Penalty and Injunction for Alleged Violations of Children's Privacy Law*, U.S. Dep't of Justice (Dec. 19, 2022), https://www.justice.gov/opa/pr/epic-games-inc-developer-fortnite-video-game-agrees-275-million-penalty-and-injunction.

307. *In re* Advocate Aurora Health Pixel Litig., Case No. 22-CV-1253-JPS, 2023 WL 2787985 (E.D. Wis. Apr. 5, 2023).

After Advocate made the breach disclosure, individuals filed class action lawsuits in various jurisdictions. The plaintiffs alleged that they never consented, agreed, authorized, or otherwise permitted Advocate to disclose their private information to third parties. The plaintiffs also alleged that Advocate never provided written notice about the disclosure of patient protected health information to third parties. The complaints alleged various claims for (1) Invasion of Privacy, (2) Breach of Contract (3) Breach of Fiduciary Duty, and (4) Violations of Confidentiality of Patient Health Care Records (Wis. Stat. § 146.81 *et seq*.). The various class actions were consolidated.[308]

On June 5, 2023, the parties notified the court that they had reached a settlement. On August 11, 2023, Plaintiffs filed an unopposed motion for preliminary approval of their class action settlement with Advocate, which would conclude the litigation. The parties agreed to the certification, for settlement purposes, of a class of approximately 2,500,000 individuals who

> resid[e] in the United States whose Personal Information or health information was or may have been disclosed to a third party without authorization or consent through any Tracking Pixel on Defendant's websites, LiveWell App, or MyChart patient portal between October 24, 2017 and October 22, 2022. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, and directors, as well as the judges presiding over this matter and the clerks of said judges. This exclusion does not apply to those employees of Defendant and its Related Parties who received Defendant's October 22, 2022 notification regarding its usage of Tracking Pixels.

The parties' settlement agreement provides that Advocate will establish a non-reversionary common settlement fund of $12,225,000.00, out of which payments to class members, service payments to named plaintiffs, settlement administration costs, and attorneys' fees and costs will be paid. Specifically, payments will be capped at $50.00 per class member; named Plaintiffs will receive service awards of $3,500.00 each; and class counsel will be permitted to seek an award of attorney's fees in an amount up to thirty-five percent of the common fund, or $4,278,750.00, plus up to $30,000.00 in costs.[309]

The court granted Plaintiffs' motion for preliminary approval of the class settlement. The court agreed that there were no barriers to conditional certification of the proposed class and preliminary approval of the class settlement. The court found that the class appears to satisfy the numerosity, commonality, typicality, adequacy, and predominance and superiority

308. *Id.*

309. *See* Advocate Aurora Pixel Litig., Case No. 2:22-cv-1253 (E.D. Wis.), https://www.advocateaurorasettlement.com.

requirements of Federal Rule of Civil Procedure 23(a) and (b)(3). The proposed settlement appeared fair, reasonable, and adequate, and it was within the range of approval. The court noted that the agreement was negotiated with the assistance of a mediator (Hon. David E. Jones) and did not appear to be a "product of collusion."[310] Finally, the settlement agreement provided for direct notice to class members in a manner that is practicable under the circumstances.

There will be a final approval hearing in 2024 where the court will consider whether (a) the settlement is fair, reasonable, and adequate; (b) the Settlement Class should be finally certified; (c) the preliminary appointment of Class Counsel should be made final; (d) the preliminary appointment of the Class Representatives should be made final; (e) Class Counsel's motion for attorneys' fees and Litigation Expenses should be granted; (f) the Service Awards sought for Class Representatives should be granted; and (g) a final judgment should be entered.

310. Order, Advocate Aurora Pixel Litig., Case No. 2:22-cv-1253 (E.D. Wis. Aug. 21, 2023), https://www.advocateaurorasettlement.com/home/7675/DocumentHandler?docPath=/Documents/_0036_ORDER_signed_by_Judge_J_P_Stadtmueller_on.pdf.