# Survey of Developments in Privacy Law

*By Steve Snyder* and Elizabeth Brusa***

## I. Introduction

This year's survey of privacy law focuses on some specific areas where legislators, agencies, enforcement officials, and courts were very active as the entire landscape of privacy law continued to rapidly develop. Section II discusses biometric privacy, addressing developments involving the leading regulation on the subject in the United States—the Illinois Biometric Information Privacy Act. Section III provides updates on regulations and case law relating to the Internet of Things. Some developments concerning surveillance and search-and-seizure law are covered in Section IV. And finally, the survey year includes the first full year of enforcement of the European Union's landmark privacy regulation—the General Data Protection Regulation ("GDPR"). Section V discusses enforcement and some of the guidance on issues surrounding the critical element of consent.

## II. Biometrics and the Illinois Biometric Information Privacy Act

In the past year, the Illinois Supreme Court considered whether a plaintiff established injury sufficient to bring a private right of action under the Illinois Biometric Information Privacy Act ("BIPA"). In addition, courts decided several cases analyzing Article III standing with regard to alleged violations of the BIPA. These cases are discussed in more detail below.

### A. BIPA Definition of "Aggrieved" Person—*Rosenbach v. Six Flags Entertainment Corp.*[1]

In *Rosenbach*, the Supreme Court of Illinois considered whether a plaintiff is an "aggrieved" person under the BIPA and therefore eligible to bring a private cause of action if the plaintiff alleges only a technical violation of the BIPA

* Steve Snyder is a board certified Privacy and Information Security Law specialist attorney practicing at Bradley Arant Boult Cummings on the Cybersecurity and Privacy Team.

** Elizabeth Brusa is a Certified Information Privacy Professional for the U.S. Private-Sector (CIPP/US) and an associate in the Banking and Financial Services Practice Group at Bradley Arant Boult Cummings.

1. No. 123186, 2019 WL 323902 (Ill. Jan. 25, 2019).

without allegations of actual injury or adverse effect.[2] The court answered this question in the affirmative.

The plaintiff was a fourteen-year-old boy, and his mother filed the action as next friend. Plaintiff sued the Six Flags theme park in Illinois state court for allegedly violating the BIPA. Six Flags collected, stored, and used fingerprints of customers that purchased season passes to quickly verify and admit those customers on subsequent visits to the park.[3] However, the plaintiff alleged that Six Flags failed to obtain his written consent prior to collecting his fingerprints and failed to disclose how his fingerprints would be used or how long the fingerprint information would be retained and failed to publicize its retention and destruction policy.[4]

After the trial court denied Six Flags' motion to dismiss, Six Flags brought an interlocutory appeal before the Illinois Court of Appeals, which held that the plaintiff was not an "aggrieved" person under the BIPA, absent allegations of injury or adverse effect as a result of violation of the BIPA.[5] The Illinois Supreme Court then granted review.

The Illinois Supreme Court first looked to the plain language of the BIPA and determined that it did not impose a requirement for actual injury.[6] The court also looked to other Illinois statutes in which the term "aggrieved" person is used to create a private right of action for violation of the statue and noted that, when the legislature intended actual injury to be a precondition to suit, it stated that requirement explicitly.[7] Additionally, the court considered the dictionary definition of "aggrieved," stating that it means "suffering from an infringement or denial of legal rights" and "having legal rights that are adversely affected."[8] The court held that:

> [W]hen a private entity fails to comply with one of [the BIPA's] requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach. . . . [S]uch a person . . . would clearly be "aggrieved" within the meaning of [the BIPA]. . . . No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action.[9]

2. *Id.* at *1 (interpreting 740 ILL. COMP. STAT. 14/20 (2018) ("Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party.")).

3. *Id.*

4. *Id.* at *2.

5. *Id.* at *3.

6. *Id.* at *5.

7. *Id.* at *5–6 (contrasting Illinois' Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. 505/10a(a) (2018) (requiring that a private cause of action allege actual damage), with Illinois' AIDS Confidentiality Act, 410 ILL. COMP. STAT. 305/13 (2018) (permitting "aggrieved" persons to pursue private causes of action based upon a violation of the statute)).

8. *Id.* at *6 (quoting, in the first instance, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 25 (11th ed. 2006) and, in the second instance, BLACK'S LAW DICTIONARY 77 (9th ed. 2009)).

9. *Id.*

The court also considered and rejected the appellate court's finding that Six Flags' violation was merely "technical" and did not give rise to relief under the BIPA, finding that such reasoning goes against the policy of the BIPA, which seeks to prevent and deter misuses of individuals' biometric information.[10]

## B. BIPA Article III Standing

During the survey period, several courts addressed Article III standing to bring an action under the BIPA. Two of these cases are outlined in the following sections.

### 1. Rivera v. Google, Inc.[11]

In *Rivera*, the U.S. District Court for the Northern District of Illinois considered whether users of Google Photos, which applies a facial recognition software technology, alleged sufficient injury to establish Article III standing, finding that they did not.[12] Google Photos uses facial recognition software to identify and categorize users' photos, and the data Google Photos gathers is not used for purposes other than organizing photos within users' individual accounts.[13] However, Google does not obtain consent to collect, use, and retain users' face scans.[14]

Plaintiffs alleged that Google violated their privacy interests but did not allege any additional pecuniary, physical, or emotional injury.[15] Google moved for summary judgment on the basis that the plaintiffs lacked Article III standing.[16] The court reviewed the Supreme Court's decision in *Spokeo, Inc. v. Robins*,[17] stating that, although intangible injuries may support Article III standing, more than a procedural violation of a statute is necessary for concrete injury to establish standing.[18] The court granted Google's motion for summary judgment, finding that, "[w]ith neither a legislative judgment nor a common law analogue . . . to support a finding of concrete injury, . . . Plaintiffs have not demonstrated an injury-in-fact sufficient to confer Article III standing."[19]

### 2. Goings v. UGN, Inc.[20]

In *Goings v. UGN, Inc.*, the plaintiff worked for the defendants and was required to scan his fingerprints for timekeeping purposes.[21] The plaintiff brought a class action in state court, alleging that the defendants' collection and storage of

10. *Id.* at *6–7.
11. 366 F. Supp. 3d 998 (N.D. Ill. 2018), *appeal docketed*, No. 19-1182 (7th Cir. Jan. 28, 2019).
12. *Id.* at 1001–02.
13. *Id.*
14. *Id.* at 1002–03.
15. *Id.* at 1003.
16. *Id.*
17. 136 S. Ct. 1540 (2016).
18. *Rivera*, 366 F. Supp. 3d at 1003–05.
19. *Id.* at 1014.
20. No. 17-cv-9340, 2018 WL 2966970 (N.D. Ill. June 13, 2018).
21. *Id.* at *1.

employees' fingerprints violated the BIPA.[22] After removing the action to federal court, the defendants moved to dismiss for, among other things, plaintiff's lack of Article III standing.[23] The plaintiff moved to remand to state court and sought fees on the ground that defendants had improperly removed the case.[24] The court noted that cases examining this issue generally require more than a mere procedural violation of the BIPA to establish Article III standing under the criteria set out in *Spokeo*, and found that the plaintiff alleged only procedural violations.[25] The court distinguished a previous case that found the plaintiff had Article III standing to bring an action under BIPA on the ground that, unlike in that case, the defendants here did not disclose the plaintiff's information to third parties.[26] The court accordingly held that the plaintiff's allegations failed to establish that he suffered any concrete injury and concluded that the plaintiff lacked standing to bring the action. It therefore remanded the case to state court but denied the plaintiff's request for fees.[27]

## III. The Internet of Things

### A. State Laws

Recently, two states enacted statutes pertaining to Internet of Things ("IoT") devices. In California, the first state to enact a law regulating the IoT, manufacturers will be required to include reasonable security features for IoT devices that will protect against unauthorized access, usage, or data disclosures beginning on January 1, 2020.[28] Also beginning on that date, manufacturers in Oregon will be required to include reasonable security measures for IoT devices.[29] While Oregon's new law mainly tracks California's, Oregon defines "connected devices"

22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.* at *2 (collecting cases).
26. *Id.* at *3–4 (discussing Dixon v. Wash. & Jane Smith Cmty., No. 17 C 8033, 2018 WL 2445292 (N.D. Ill. May 31, 2018)).
27. *Id.* at *4.
28. S. 327, 2017–18 Reg. Sess., 2018 Cal. Legis. Serv. Ch. 886 (West) (to be codified at Cal. Civ. Code §§ 1798.91.04–.06). The statute defines "connected device" as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." *Id.* (to be codified at Cal. Civ. Code § 1798.91.05(b)). The statute also deems a "reasonable security feature," among other possibilities, a "preprogrammed password [that] is unique to each device manufactured" or "a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time." *Id.* (to be codified at Cal. Civ. Code § 1798.91.04(b)).
29. H.R. 2395, 80th Leg. Assemb., Reg. Sess., 2019 Or. Laws Ch. 193 (West) (amending Or. Rev. Stat. Ann. §§ 646.605, 646.607). The statute defines "connected device" as "a device or other physical object that: (A) Connects, directly or indirectly, to the Internet and is used primarily for personal, family or household purposes; and (B) Is assigned an Internet Protocol address or another address or number that identifies the connected device for the purpose of making a short-range wireless connection to another device." *Id.* (to be codified at Or. Rev. Stat. Ann. § 646.605). The statute also provides that a "reasonable security feature may consist of . . . [a] preprogrammed password that is unique for each connected device . . . or [a] requirement that a user generate a new means of authentication before gaining access to the connected device for the first time." *Id.* (to be codified at Or. Rev. Stat. Ann. § 646.605).

less broadly. With respect to connected devices that can be accessed remotely, both laws define a "reasonable security feature" as providing for unique pre-programmed passwords or requiring the user to generate a new password prior to gaining access for the first time.

### B. S.D. v. Hytto Ltd.[30]

The U.S. District Court for the Northern District of California granted in part and denied in part a motion to dismiss filed by Chinese sex toy marketer and seller, Hytto Ltd., d/b/a Lovense ("Hytto"). Hytto sells its products over the Internet to mostly U.S. customers. Certain of Hytto's products may be linked to the Internet through user profiles and controlled via smartphone apps over long distances. Through such use, Hytto purportedly collects user information, including email addresses, dates and times of device usage, and device usage settings. The plaintiff, a user of one of Hytto's devices, filed a complaint against Hytto, alleging violation of the Wiretap Act, intrusion upon seclusion, and unjust enrichment. Hytto moved to dismiss for lack of personal jurisdiction and failure to state a claim.[31]

The court first denied Hytto's motion to dismiss for lack of personal jurisdiction, finding Hytto had sufficient contacts with the United States to meet the requirements of Federal Rule of Civil Procedure 4(k)(2).[32] The court next found that, because Hytto's alleged interceptions occurred while the data was being transmitted via the Internet, rather than during local transmission via Bluetooth, they fell within the purview of the Wiretap Act as "interceptions" of "electronic communications." Additionally, the court held that, although the date and time of device usage did not constitute "content" as contemplated under the Wiretap Act, the data pertaining to the device usage settings did. As such, the court granted the motion to dismiss the Wiretap Act claim as to interceptions of date and time information but denied the motion as to interceptions of device usage settings data.[33] Further, the court found that Hytto was not a party to the communications, and therefore Hytto's data collection was an "interception" under the Wiretap Act.[34] It also found that Hytto's defense based on the statute's "ordinary course of business" exception was premature.[35]

Additionally, based on the plaintiff's expectation of privacy created by Hytto's data usage policy, the court denied Hytto's motion to dismiss the intrusion upon seclusion claim. Finally, the court granted Hytto's motion to dismiss the unjust enrichment claim based on the plaintiff's failure to identify a particular state's laws in his complaint.[36]

30. Order Granting in Part & Denying in Part Defendant's Motion to Dismiss, No. 18-cv-00688-JSW (N.D. Cal. May 14, 2019).
31. *Id.* at 1–2.
32. *Id.* at 4–8 (applying Fed. R. Civ. P. 4(k)).
33. *Id.* at 8–12 (interpreting Wiretap Act, 18 U.S.C. § 2510(4), (8), (12) (2018) (defining "intercept," "contents," and "electronic communication")).
34. *Id.* at 12–13 (interpreting Wiretap Act, 18 U.S.C. §§ 2510, 2511 (2018)).
35. *Id.* at 13–15 (interpreting Wiretap Act, 18 U.S.C. § 2510(5)(a)).
36. *Id.* at 15–16.

## IV. Surveillance, Search, and Seizure

### A. *Carpenter v. United States*[37]

In June 2018, the Supreme Court addressed whether a person has a reasonable expectation of privacy in his movements as tracked by cell-site location information ("CSLI") collected by wireless carriers and, if so, whether acquisition of that information was a search requiring probable cause. In the case, the FBI accessed Carpenter's location information using a cell-phone-records request pursuant to the Stored Communications Act. The location information totaled 12,898 location points over 127 days.[38] Carpenter argued that the acquisition was an unreasonable search and seizure violating the Fourth Amendment.

The Supreme Court held that Carpenter had a reasonable expectation of privacy in his CSLI.[39] In so doing, it rejected the government's argument that Carpenter's claim was defeated by the third-party doctrine, according to which a person has no expectation of privacy in information he knowingly shares with another.[40] The acquisition of the location information was therefore a Fourth Amendment search.[41] The Court then concluded that the standard for a request under the Stored Communications Act—that the government show there are "reasonable grounds" to believe the records were "relevant and material" to an investigation—fell short of probable cause for a warrant.[42] The Court also noted broadly that "the Government will generally need a warrant to access CSLI," but recognized that there might be "case-specific exceptions."[43]

### B. *Naperville Smart Meter Awareness v. City of Naperville*[44]

In *Naperville*, the Seventh Circuit considered whether the city's collection of residents' electricity consumption and retention of such data violates the U.S. Constitution's Fourth Amendment and Article I, Section 6, of the Illinois Constitution.

Naperville owns and operates a public utility that supplies electricity to city residents.[45] Naperville used federal funds to update its electric grid and replace analog energy meters with digital "smart meters," which collect data over thousands of intervals each month and show when and how much energy is used in a particular home.[46] Such data can be used to derive information regarding activities occurring within a home. Notably, Naperville residents were not given an option to not use smart meters.[47]

37. 138 S. Ct. 2206 (2018).
38. *Id.* at 2212.
39. *Id.* at 2219.
40. *Id.* at 2219–20.
41. *Id.* at 2220.
42. *Id.* at 2221 (quoting Stored Communications Act, 18 U.S.C. § 2703(d) (2018)).
43. *Id.* at 2222.
44. 900 F.3d 521 (7th Cir. 2018).
45. *Id.* at 523.
46. *Id.* at 524.
47. *Id.*

The plaintiff, a non-profit citizens' group, sued Naperville for allegedly unreasonable searches in violation of citizens' rights under the U.S. and Illinois Constitutions.[48] The district court dismissed the plaintiff's complaint and amended complaint and denied the plaintiff's request for leave to file a third complaint, finding such amendment would be futile.[49] Then, the plaintiff appealed to the Seventh Circuit.[50]

The appellate court concluded that Naperville's collection of residents' data from the smart meters constituted a search, but held that Naperville's smart meter ordinance overcame the presumption that a warrantless search is unreasonable.[51] Citing the Supreme Court's *Camera v. Municipal Court* decision,[52] the Seventh Circuit explained that the fact that Naperville collects residents' energy data without any prosecutorial intent decreases residents' expectation of privacy.[53] The intrusion on privacy is also limited by the circumstances that the information is collected without physical entry, there is little risk of corollary prosecution, and the utility will not provide the data to third parties without a warrant or court order.[54] The Seventh Circuit further held that Naperville's interest in collecting and using the data from the smart meters will assist the city in modernizing its electrical grid, which outweighs the residents' privacy interest.[55] Accordingly, although the Seventh Circuit found that Naperville's collection of residents' data from the smart meters constituted a search, it held that the search was reasonable.[56]

## V. First Year of GDPR Enforcement

In late May 2019, the first full year of enforcement of the European Union's ("EU") GDPR[57] came to a close. Given its potential for massive fines up to 4 percent of a company's global annual turnover, the enforcement of the GDPR was a point of great interest and speculation. The following subsections discuss an overview report from the European Data Protection Board ("EDPB") regarding enforcement mechanisms, a case involving the judicial interpretation

48. *Id.*; *see* Ill. Const. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized.").

49. *Naperville Smart Meter Awareness*, 900 F.3d at 524–25.

50. *Id.* at 525.

51. *Id.* at 525–29.

52. 387 U.S. 523, 530–31 (1967).

53. *Naperville Smart Meter Awareness*, 900 F.3d at 528.

54. *Id.*

55. *Id.*

56. *Id.* at 529.

57. Regulation 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 (General Data Protection Regulation), 2016 O. J. (L 119) 1 [hereinafter GDPR].

of the consent requirement under the GDPR, and a guideline on consent adopted by the EDPB.

### A. GDPR Enforcement Overview

The EDPB[58] released an overview of the implementation and enforcement of the GDPR on February 25, 2019.[59] The primary focus of this report was the cooperation mechanism and consistency findings—that is, how the various data protection authorities were coordinating on enforcement. The conclusion was that "the GDPR cooperation and consistency mechanism work quite well in practice."[60]

The GDPR Enforcement Overview focused on the consistency of opinions. It noted that, from the time the GDPR was implemented, the EDPB endorsed sixteen guidelines prepared by the Article 29 Working Party, the predecessor of the EDPB, and adopted five guidelines of its own.[61] The GDPR Enforcement Overview also focused on the "One-Stop-Shop cooperation mechanism, which introduces the obligatory intervention of a Lead Supervisory Authority for the cross-border cases."[62] When an entity has a "main establishment" in a particular jurisdiction, the data protection authority of that jurisdiction is the lead authority for the investigation.[63] In the absence of a "main establishment" in any EU jurisdiction, which is likely the case for U.S. companies, the various data protection authorities must coordinate to identify a "lead authority" prior to using the "One Stop Shop" mechanism.[64] The GDPR Enforcement Overview found that 642 procedures were initiated to identify a lead authority, which, to date, have resulted in no disputes in the selection of the lead authority.[65]

The GDPR Enforcement Overview summarized the "One Stop Shop" procedures and found that there were forty-five initiated with lead authorities from fourteen different countries.[66] These forty-five represent the cases that proceeded to the "One Stop Shop" procedure which involves cooperation between the lead authority identified and any other concerned authorities to reach a coordinated decision.[67] It found that, of those forty-five, twenty-three are at the

58. "The . . . EDPB is an independent European Union body, which contributes to the consistent application of data protection rules throughout the [EU], and promotes cooperation between the EU's data protection authorities." *About EDPB*, Eur. Data Prot. Bd., https://edpb.europa.eu/about-edpb/about-edpb_en (last visited Aug. 29, 2019). It was established by the GDPR and succeeded the Article 29 Working Party, which served that purpose prior to the effective date of the GDPR. *See id.*

59. Eur. Data Prot. Bd., First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities (2019) [hereinafter EDPB Enforcement Overview], http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf.

60. *Id.* at 1.

61. *Id.* at 2; *see also infra* Part V.C. (discussing Article 29 Guidelines endorsed by the EDPB).

62. EDPB Enforcement Overview, *supra* note 59, at 2.

63. *Id.* at 3.

64. *See id.*

65. *Id.* Of those 642 procedures, 306 are closed and the lead authority identified. *Id.*

66. *Id.* at 4.

67. *Id.* at 3–4.

informal consultation level, sixteen are at draft decision level, and six are final decisions.[68] The GDPR Enforcement Overview also highlighted cooperation in the form of 444 mutual assistance requests, but noted that no joint operations have yet been commenced.[69] Overall, the GDPR Enforcement Overview found that cooperation mechanisms were working.[70] The EDPB can intervene as a dispute resolution body, and the GDPR Enforcement Overview noted that this had not happened during the period in question.[71]

The GDPR Enforcement Overview also summarized enforcement statistics. The total number of cases reported by supervisory authorities from various countries was 206,326, which include complaints about GDPR violations, data breach notifications, and other cases. Of those, 94,622 were initiated by complaints while 64,684 were initiated on the basis of data breach notification by the controller.[72] Of those cases, 52 percent have been closed, and one percent were challenged before the national court.[73] The various corrective powers employed by supervisory authorities were also outlined, including: issuing warnings that processing operations are likely to infringe the GDPR, issuing reprimands that operations have infringed the GDPR, ordering the controller or processor to comply with data subject requests or to bring operations into compliance with the GDPR, and imposing administrative limitations, bans, and fines.[74] Finally, the GDPR Enforcement Overview noted that the total amount of administrative fines imposed was 55,955,871 Euros.[75]

## B. *CNIL v. Google LLC*

Immediately after the GDPR's effective date, France's data protection authority—Commission Nationale de l'Informatique et des Libertés ("CNIL")—received complaints regarding Google's practices and began investigating. First, CNIL determined that, although Google had European headquarters in Ireland, it lacked a "main establishment" in the European Union. Therefore, CNIL concluded the "One Stop Shop" mechanism was not applicable and that CNIL was competent to make any decision regarding processing operations carried out by Google.[76]

CNIL carried out online inspections in September 2018 to assess compliance. CNIL found that Google had violated its obligations of transparency in disclosing required information, and its obligation to have a legal basis for processing user data to generate personalized advertisements.

68. *Id.* at 4.
69. *Id.* at 5.
70. *See id*. at 6.
71. *Id.*
72. *Id.* at 7.
73. *Id.*
74. *Id.* at 8.
75. *Id.*
76. Commission Nationale de l'Informatique et des Libertés, *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

The obligation of information transparency stems from Article 12 of the GDPR, which requires disclosures to be made "in a concise, transparent, intelligible and easily accessible form, using clear and plain language," and Article 13, which sets out the categories of information that must be provided to the data subject at the time when personal data is obtained.[77] CNIL found that the information required by Article 13 was not provided in the form required by Article 12 because it was "excessively spread out across several documents" and noted a user would have to "cross-check and compare" provisions from different documents to understand which data is collected according to the various settings they have chosen.[78] CNIL also noted that some information is difficult to find, requiring the user to "perform many actions and combine several document resources. . . . [F]ive actions are necessary for the user to access the information relating to personalised advertising and six for geolocation."[79] This analysis led CNIL to conclude "there is an overall lack of accessibility to the information provided by the company in the context of the processing in question."[80]

CNIL found that the information was not "clear" and "intelligible" due to the fact that the data processing "is particularly extensive and intrusive."[81] After detailing the vast litany of data processed and shared by Google, CNIL noted that, although the company provides a "Privacy check-up" and "Dashboard" that allow the user some amount of control over the data, these tools are only mobilized after an account is created and presuppose an active approach and initiative on the part of the data subject.[82] For all of these reasons, CNIL concluded there was a breach of the transparency and information obligations provided for by Articles 12 and 13 of GDPR.[83]

CNIL also found that Google failed to validly obtain consent for personalized ad processing. CNIL found that consent on the part of users of Google's services was not fully informed due to the same deficiencies that resulted in breach of the transparency and information obligations.[84] CNIL also found that Google sought consent to processing via an opt-out mechanism—the box indicating consent to display of personalized advertising was checked by default, and the user had to navigate to a new page by clicking a "More options" button and then uncheck the box to withhold consent—and determined that this did not satisfy GDPR's requirement that consent be conveyed through "a freely given, specific, informed and unambiguous indication of the data subject's agreement."[85] Google argued

77. Commission Nationale de l'Informatique et des Libertés, Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 Pronouncing a Financial Sanction Against GOOGLE LLC 11–12 (Jan. 21, 2019), https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf (analyzing GDPR, *supra* note 57, arts. 12(1), 13(1), at 39, 40–41).

78. *Id.* at 13–14.

79. *Id.* at 14.

80. *Id.* at 15.

81. *Id.*; *see id.* at 15–18.

82. *Id.* at 18.

83. *Id.* at 19.

84. *Id.* at 21–22.

85. *Id.* at 22 (quoting GDPR, *supra* note 57, para. 32, at 6); *see id.* at 22–24.

that it was wrongly being subjected to requirements for consent for sensitive data in Article 9 rather than the lower standard for Article 6 processing, but CNIL concluded that the "same terms of expressing consent apply in the same way, whether consent is obtained under Article 6 of the GDPR, for the implementation of processing for a specific purpose, or collected, pursuant to Article 9 of the GDPR."[86] The result of this analysis was the imposition of a fine of fifty million Euros, accompanied by publication of the decision for two years.[87]

## C. EDPB Endorsement of Article 29 Guidelines

The Article 29 Working Party, which was set up under the Data Protection Directive, promulgated guidelines on various aspects of the GDPR in the two years leading up to the GDPR effective date of May 25, 2018.[88] On that date, the EDPB succeeded the Article 29 Working Party. On that same date, the EDPB had its first plenary meeting and adopted sixteen Article 29 Guidelines,[89] including, of particular interest, "Guidelines on consent under Regulation 2016/679, WP259 rev.01" ("Consent Guidelines").[90] The Consent Guidelines provide a thorough analysis of the concept of consent as used in the GDPR. Consent is one of the six lawful bases to process personal data as identified in Article 6 of the GDPR. Briefly summarized, consent is only a lawful basis if the data subject is offered control and a genuine choice.

The four elements of consent, according to the definition of the term in Article 4(11) of the GDPR, are that consent must be (i) freely given, (ii) specific, (iii) informed, and (iv) an unambiguous indication of the data subject's wishes. The Consent Guidelines address each of these elements in turn.

### 1. Consent Free / Freely Given

A data subject must have "real choice" in the sense that she cannot feel compelled to consent due to the possibility of enduring negative consequences if she does not consent.[91] Therefore, consent cannot be bundled into all-or-nothing terms and conditions. Similarly, the tying of consent to receiving a service or as a provision of a contract must also be carefully analyzed. An example of improper

86. *Id.* at 24.

87. *Id.* at 28.

88. *See* Eur. Data Prot. Supervisor, *Glossary*, Europa, https://edps.europa.eu/data-protection/data-protection/glossary/a_en (last visited Aug. 26, 2019) (defining "Article 29 Working Party").

89. *Endorsement 1/2018*, Eur. Data Prot. Bd. (May 25, 2018), https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

90. Article 29 Data Protection Working Party, Guidelines on Consent Under Regulation 2016/679 (Apr. 10, 2018) [hereinafter Consent Guidelines], https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030; *see* GDPR, *supra* note 57, art. 6(1)(a), at 36 (providing that processing shall be lawful if consent is given); *id.* art. 4(11), at 34 (defining "consent").

91. Consent Guidelines, *supra* note 90, at 5.

consent is if a photo editing app states that a user must consent to the use of her geolocation data to use the app. Because geolocation data is not necessary to provide the photo editing services, this type of consent is improper.[92] The Consent Guidelines recommend a strict interpretation of what data is "necessary for the performance of a contract" and limiting required consent to only that data. As noted, "[t]here needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract."[93]

Another element of whether consent is freely given relates to an imbalance of power. One place this is likely to arise is in the workplace. The Consent Guidelines note that it is "problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given."[94] Granularity of choice also affects whether consent is freely given. In particular, when processing involves multiple purposes, the data subject must have the option to consent to some but not all of the processing.[95]

### 2. Specific

The stated purpose for data collection must be specific, explicit, and legitimate.[96] The primary focus of this restriction is to prevent what is termed "function creep" where the purpose for collection is blurred after the initial collection and the use of the data expands.[97] To prevent this, the consent must be specific to the purpose, and if the controller wishes to use the data for another purpose, the controller must obtain additional consent. To enable this, the controller must provide a separate opt-in for each purpose.[98]

### 3. Informed

Informed consent relates to the requirement for transparency, which is one of the fundamental principles of the GDPR. It is essential for a data subject to be properly informed so that consent can be given freely and for a specific purpose.[99] If the user is not properly informed, a user's control of his data is illusory, and this "consent" is not a lawful basis for processing. Therefore, the consent will be invalid, and the controller may be in breach of Article 6 of the GDPR, absent a different lawful basis for the processing.[100]

92. *Id.* at 5–6 (citing GDPR, *supra* note 57, art. 7(4), at 37 ("When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.")).
93. *Id.* at 8.
94. *Id.* at 7.
95. *Id.* at 10.
96. *Id.* at 12 (citing GDPR, *supra* note 57, art. 5(1)(b)).
97. *Id.*
98. *Id.*
99. *Id.* at 12–13.
100. *Id.* at 13.

### 4. Unambiguous Indication of Wishes

Article 4(11) of the GDPR states that valid consent requires an unambiguous indication by means of a statement or by a clear affirmative action.[101] This means the data subject must have taken a deliberate action to consent, which can be collected through written or recorded statement, including by electronic means. The use of pre-checked boxes is invalid under the GDPR, as is reliance on the user's merely proceeding with a service (such as installing a program) as indication of consent.[102] "[C]onsent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service."[103] The Consent Guidelines note that it may be necessary to interrupt the user experience when a less disruptive indication of consent would result in ambiguity.[104]

### 5. Additional Issues

Beyond the four elements of consent, the Consent Guidelines elaborate on some other areas of concern. One area is how to meet the heightened threshold of "explicit consent," which is required in Article 9 of the GDRP relating to special categories of data.[105] This is a higher standard than "regular" consent and requires the user to agree explicitly through means like filling in an electronic form or by using an electronic signature.[106] The Consent Guidelines suggest the use of two-stage verification where the data subject receives an e-mail outlining the requested consent to use of a specific set of information for a specific purpose, and the user responds with an e-mail saying "I agree," for example.[107]

## D. Judicial Consent Interpretation—Planet49[108]

On March 21, 2019, an Opinion of the Advocate General addressed questions posed by the Federal Court of Justice in Germany relating to the interpretation of

101. *Id.* at 15.
102. *Id.* at 16.
103. *Id.*
104. *Id.*
105. *Id.* at 18–20 (citing GDPR, *supra* note 57, art. 9(2)(a) (addressing "Processing of Special Categories of Personal Data")).
106. *Id.* at 18.
107. *Id.* at 19.
108. Opinion of Advocate General, Case C-673/17, Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband e.V. (Mar. 19, 2019), http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=5067883 (interpreting GDPR, *supra* note 57, arts. 4, 6, 7, 94–95, at 33–37, 86; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive], *repealed by* GDPR, *supra* note 57, art. 94, at 86; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 [hereinafter ePrivacy Directive]).

consent requirements in view of the collective guidance of the ePrivacy Directive, the Data Protection Directive, and the GDPR. Among other things, the opinion addressed the question whether consent to placing a cookie on the user's computer could be obtained through an opt-out mechanism.

To participate in a lottery organized by Planet49, a user had to enter her personal information into a webpage. That page included text stating that the user consented to the placing of cookies on her computer for the purpose of tracking her online behavior in order to generate personalized advertising directed to her. The user's consent (required by the ePrivacy Directive) was obtained through a pre-checked box accompanying the text; consent was inferred if she failed to uncheck the box.[109]

The Advocate General found there was no valid consent for several reasons. First, it is "virtually impossible to determine objectively whether or not a user has given his consent" in this circumstance because of the pre-checked box.[110] Therefore, it cannot be shown that consent is actively given. Secondly, participation in the lottery and consenting to the installation of cookies was part of the same act—clicking on the participation button—which fails the requirement that consent must be "separate."[111] A data subject cannot express two intentions (participation in the lottery and installation of cookies) at the same time. Finally, Planet49's webpage also included an unchecked box relating to marketing that was required to be checked to participate in the lottery, but the Advocate General found that the user was not fully informed that only the other pre-checked box would result in the installation of cookies, and therefore fully informed consent was not given.[112]

Ultimately the Advocate General concluded that there was no valid consent. The court also noted the firm requirement that, in regard to consent involving cookies, "[t]he clear and comprehensive information a service provider has to give to a user, under Article 5(3) of [the ePrivacy] Directive . . . , includes the duration of the operation of the cookies and the question of whether third parties are given access to the cookies or not."[113]

## VI. Conclusion

Privacy law is rapidly evolving and shows no sign of slowing down. We expect to see state legislatures continue to introduce privacy laws on many topics including e-commerce, IoT, and biometrics. There will likely be active enforcement efforts from the FTC and the possibility of consumer class action

109. *Id.* at paras. 24–25; *see id.* at paras. 7–9 (citing ePrivacy Directive, *supra* note 108, arts. 2, 5, at 43–44).

110. *Id.* at para. 88.

111. *Id.* at paras. 63–66, 89; *see id.* at para. 60 (citing Data Protection Directive, *supra* note 108, art. 7(a) (requiring "unambiguous" consent)).

112. *Id.* at paras. 89–92.

113. *Id.* at para. 121 (citing ePrivacy Directive, *supra* note 108, art. 5(3)).

suits in California as the California Consumer Privacy Act[114] goes into effect. The EU will likely continue to wrestle with the more intricate and nuanced interpretations of its provisions around such elements as consent in different contexts.

114. S. 1121, 2017–18 Reg. Sess., 2018 Cal. Legis. Serv. Ch. 735 (West) (to be codified at CAL. CIV. CODE §§ 1798.100–1798.199).