RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY

Kyle D. Black, Christina B. Alam, Steven M. Bucher, Ashley J. Giannetti, Lauren D. Godfrey, and Justin D. Wear

Kyle D. Black (kyle.black@bipc.com), is an Associate at Buchanan Ingersoll & Rooney PC in Pittsburgh, PA. Christina B. Alam (Christina.Alam@pnc.com) is Staff Counsel at PNC Bank, National Association in Pittsburgh, PA. Steven M. Bucher (SBucher@gallowaylawfirm.com) is an Associate at Galloway, Johnson, Tompkins, Burr & Smith in Lafayette, LA. Ashley J. Giannetti (Ashley.Giannetti@lewisbrisbois.com) is an Associate at Lewis Brisbois Brisbois Bisgaard & Smith, LLP in Pittsburgh, PA. Lauren D. Godfrey (Lauren.Godfrey@lewisbrisbois.com) is a Partner at Lewis Brisbois Bisgaard & Smith, LLP in Pittsburgh, PA. Justin D. Wear (jwear@manierherod.com) is a Partner at Manier & Herod in Nashville, TN.

This survey reviews recent regulatory developments and court decisions addressing cybersecurity and data privacy issues from October 1, 2017 through September 30, 2018. The first part will discuss statutory and regulatory developments particularly related to breach notification. The second part will discuss standing to sue under Article III, section 2 of the U.S. Constitution, in light of the U.S. Supreme Court's 2016 landmark decision in *Spokeo, Inc. v. Robins*. The third part will discuss cases generally addressing the right to privacy. The fourth part will discuss notable cases involving technology and data privacy concerns, particularly discussing "autodialers" under the Telephone Consumer Protection Act. The fifth part will discuss the Federal Trade Commission's ("FTC") enforcement powers. Finally, the sixth part will discuss notable cases involving fraud-related cybercrimes.

I. STATUTORY AND REGULATORY BREACH NOTIFICATION DEVELOPMENTS

Data breach notification requirements received particular attention in 2018, both abroad and in various states in the U.S. The European General Data Protection Regulation ("GDPR") has certainly made organizations in both the public and private sector, domestic and abroad, more cognizant of their duties to notify the general public following a data security incident. Several U.S. states are following suit and implementing their own strict breach notification requirements. Below are the most recent statutory and regulatory breach notification developments.

A. *European Union*

The most significant data privacy and cybersecurity development in 2018 was undoubtedly the European Union's enactment of the GDPR. Effective May 25, 2018, the GDPR is significant because it applies to more than just entities in the European Union ("EU"). The GDPR also applies to entities anywhere in the world that offer goods or services to EU citizens or monitor the behavior of EU citizens.[1] Therefore, even entities in the United States may be subject to the GDPR's extraterritorial reach.

The GDPR demonstrates the growing importance and value placed on providing breach notification to affected individuals. For example, the GDPR provides strict breach notification requirements to both consumers and applicable EU member state supervisory authorities. Any "data controller" becoming aware of a breach must, without undue delay and where feasible within 72 hours, notify the applicable member state supervisory

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (Apr. 27, 2016), Art. 3(2).

authority.[2] The controller must also, without undue delay, notify affected data subjects.[3] Notification to both supervisory authorities and data subjects must satisfy certain form and content requirements.[4]

The GDPR is also significant because it lays out hefty fines for data controllers in violation of the GDPR. Violations of certain GDPR provisions may subject a data controller to administrative fines up to 10,000,000 euros or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[5] For violations of more serious provisions of the GDPR, data controllers may be subject to administrative fines up to 20,000,000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[6]

B. *South Dakota*

South Dakota enacted its own data breach notification statute on March 21, 2018, thereby becoming the 49th state to require notification to consumers following a data breach. Effective July 1, 2018, South Dakota's breach notification statute shares a number of similar provisions found in other data breach notification statutes across the country. For example, South Dakota only covers electronic data.[7] Consumer notification must be made within 60 days after discovery of a breach.[8] Like other statutes, South Dakota does allow for a delay in notification if a law enforcement agency determines that notice will interfere with a criminal investigation.[9] But South Dakota requires that the subsequent notice must be made no later than 30 days after the law enforcement agency determines that notice will no longer compromise the criminal investigation.[10] If more than 250 South Dakota residents are affected by the breach, the South Dakota Attorney General must be notified.[11] South Dakota provides a more expansive definition of "personal information." Like most other states, "personal information" includes, when combined with a consumer's first name or first initial and last name, their Social Security number, their driver's license number, or financial account number.[12] But South Dakota's definition of "personal information" also includes health information "as defined in 45

2. *Id.*, Art. 33(1).
3. *Id.*, Art. 34.
4. *Id.*, Art. 33(3).
5. *Id.*, Art. 84(4).
6. *Id.*, Art. 83(5).
7. *See* S.D. Codified Laws § 22-40-19(1) (defining "breach of system security" as the unauthorized acquisition of unencrypted *computerized data* . . . ." (emphasis added)).
8. *Id.*, § 22-40-20.
9. *Id.*, § 22-40-21.
10. *Id.*
11. *Id.*, § 22-40-20.
12. *Id.*, § 22-40-19(4).

C.F.R. § 160.103," or an employer-assigned identification number in combination with a required security code, access code, password, or biometric data used for authentication purposes.[13]

C. *Alabama*

On March 27, 2018, Alabama became the 50th state to require consumer notification following a data breach. Effective June 2, 2018, the Alabama Data Breach Notification Act of 2018 only covers electronic data.[14] Consumer notification must be made within 45 days after discovery of a breach.[15] The Alabama Attorney General must be notified if more than 1,000 residents have to be notified of a breach, and notification to the Alabama Attorney General must be made within 45 days after discovery of the breach.[16] Like most states, Alabama defines "personal information" to include, when combined with a consumer's first name or first initial and last name, their Social Security number, their driver's license number, and financial account number.[17] But Alabama's definition of "personal information" also includes information regarding a consumer's medical history, as well as their health insurance policy number.[18] The notice to consumers must include the date of the breach, description of the sensitive personally identifying information compromised, actions taken to restore data security and confidentiality, steps affected individuals can take to protect themselves from identity theft, and contact information of the covered entity.[19]

D. *Arizona*

On April 11, 2018, Arizona enacted House Bill 2154, amending its data breach notification law. Effective August 1, 2018, the amendments expand the definition of "personal information" to include, when combined with the consumer's first name or first initial and last name, the following data elements: (1) a private key that is unique to an individual and is used to authenticate or sign an electronic record; (2) health insurance identification numbers; (3) information about the individual's medical treatment or diagnosis; (4) taxpayer identification number; (5) passport numbers; or (6) biometric data.[20] Consumer notification must now be made within 45 days of determination of the breach.[21] The Arizona Attorney General and

13. *Id.*
14. Ala. Code. §§ 8-38-1 — 8-38-12.
15. *Id.*, § 8-38-5(b).
16. *Id.*, § 8-38-6(a).
17. *Id.*, § 8-38-2(6).
18. *Id.*
19. *Id.*, § 8-38-5(d).
20. Ariz. Rev. Stat. § 18-551(11).
21. *Id.*, § 18-552(B).

the "three largest nationwide consumer reporting agencies" must now be notified if 1,000 or more Arizona residents are given notice of the breach.[22] Failure to provide consumer or regulatory notice within the 45-day requirement may result in a fine of up to $500,000.[23] However, consumer notification is no longer required if an independent forensic firm or law enforcement agency determines that the breach is "not reasonably likely to result in substantial economic loss to affected individuals."[24] Also, should a covered entity provide substitute notice, it is no longer required to give notice to statewide media.[25] Instead, the covered entity must provide the Arizona Attorney General with a written explanation that "demonstrates the facts necessary for substitute notice."[26]

E. *Oregon*

In March 2018, Oregon enacted Senate Bill 1551, amending its Consumer Identity Theft Protection Act. Effective June 2, 2018, Oregon's breach notification law now applies to any person who "otherwise possesses" personal information involved in a data breach.[27] The definition of "personal information" is also expanded to include, when combined with an individual's first name or first initial and last name, any "information that a person reasonably knows or should know would permit access to [a] consumer's financial account."[28]

If a covered entity is required to give notice, the entity is also now specifically required to take reasonable measures necessary to (1) "determine sufficient contact information" for the intended notice recipient, (2) "determine the scope of the [data] breach," and (3) "restore the reasonable integrity, security and confidentiality of the personal information" impacted.[29] The contents of a consumer notification letter must now include the contact information of the covered entity.[30] Consumer notification must be made within 45 days of the discovery of the breach, unless law enforcement asks to delay notification.[31]

Covered entities are also now prohibited from requiring affected individuals to provide credit card or debit card numbers or accept any other service in order to receive free credit monitoring or identity theft protection

22. *Id.*
23. *Id.*, § 18-552(L).
24. *Id.*, § 18-552(J).
25. *See* Ariz. H.R. 2154 (Apr. 11, 2018), *available at* https://legiscan.com/AZ/text/HB2154/2018.
26. Ariz. Rev. Stat. § 18-552(F)(4)(a).
27. Or. Rev. Stat. § 646A.604(1).
28. *Id.*, § 646A.602(11).
29. *Id.*, § 646A.604(3)(a).
30. *Id.*, § 646A.604(5)(d).
31. *Id.*, § 646A.604(3)(a).

services.[32] If additional services are offered for a fee, then the covered entity must clearly and conspicuously disclose that the consumer will be charged a fee.[33] The amendments also prohibit consumer reporting agencies from charging a fee for placing, lifting, or removing a security freeze on a consumer's consumer report or protective record.[34]

Oregon's Senate Bill 1551 also amended the state's security safeguards requirements for personal information. The amendments expand the scope of the security safeguards requirements to apply to any person or organization that has "control over or access to" a consumer's personal information.[35] The amendments also expand upon the requisite administrative, technical, and physical safeguards. Specifically, administrative safeguards must be performed "with reasonable regularity."[36] Technical safeguards must now include assessment and steps taken to address "risks and vulnerabilities in network and software design," and "security updates and a reasonable security patch management program" must be applied "to software that might reasonably be at risk of or vulnerable to a breach of security."[37] Physical safeguards must be assessed "in light of current technology," and intrusions must also be regularly monitored and isolated in a timely manner.[38] Entities must also now conduct risk assessments and provide training "with reasonable regularity."[39]

F. *Virginia*

On March 9, 2018, Virginia enacted House Bill 183, creating Va. Code Ann. § 58.1-341.2, a new section under the Virginia Code, separate from the state's main data breach notification statute. Effective July 1, 2018, the new section imposes data breach notification requirements on "signing" income tax preparers when "return information" is affected. Now, tax preparers who sign and prepare income tax returns for Virginia residents must provide notice to the Virginia Department of Taxation in the event of "unauthorized access and acquisition of . . . return information" that the tax preparer maintains, which creates the "reasonable belief" that the information could cause "identity theft or other fraud."[40] The tax preparer will need to provide the Department of Taxation with the name and taxpayer identification number of any affected individual, "as well as the name of the signing income tax return preparer, his preparer tax identification number,

32. *Id.*, § 646A.604(7).
33. *Id.*
34. *Id.*, § 646A.610.
35. *Id.*, § 646A.622(1).
36. *Id.*, § 646A.622(2).
37. *Id.*
38. *Id.*
39. *Id.*
40. Va. Code Ann. § 58.1-341.2(B).

and such other information as the Department may prescribe."[41] Notice must be provided "without unreasonable delay." However, notification is only required if the return information is unencrypted and unredacted.[42]

The new section defines "return information" to include a "taxpayer's identity and the nature, source, or amount of his or her income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, assessments, or tax payments."[43] Of note, the new section does not require consumer (taxpayer) notification. And the new section does not apply to "personal information," so a signing income tax preparer would still need to comply with Virginia's main data breach notification statute under Va. Code Ann. § 18.2-186.6.

G. *Louisiana*

On May 20, 2018, Louisiana signed into law Senate Bill 361, amending its Louisiana Database Security Breach Notification Law.[44] Effective August 1, 2018, the amendments expand the definition of "personal information" to now include state identification numbers, passport numbers, and biometric data.[45] Consumer notification must now be made within 60 days of discovery of a breach, but the Louisiana Attorney General may grant an extension upon request.[46] However, notification is not required if, after a reasonable investigation, the covered entity determines there is no reasonable likelihood of harm to the consumer.[47] The entity must still retain documentation of its investigation for five years, and, if requested, must provide a copy of the documentation to the Louisiana Attorney General within 30 days of receiving the request.[48] Also, substitute notification via email, conspicuous posting on a website, or via statewide media may now be provided if the cost of notification exceeds $100,000, the affected population exceeds 100,000, or if the entity has insufficient contact information.[49] Louisiana also now requires entities to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[50] Louisiana also now requires data be disposed once the data is no longer needed.[51]

41. *Id.*
42. *Id.*
43. *Id.*, § 58.1-341.2(A).
44. La. Rev. Stat. §§ 51:3071–3077.
45. *Id.*, § 51:3073(3).
46. *Id.*, § 51:3074(E).
47. *Id.*
48. *Id.*
49. *Id.*, § 51:3074(G)(3).
50. *Id.*, § 51:3074(A).
51. *Id.*, § 51:3074(B).

H. *Colorado*

On May 29, 2018, Colorado enacted House Bill 18-1128, which amends Colo. Rev. Stat. § 6-1-716, Colorado's breach notification statute. Effective September 1, 2018, the amendments expand the definition of "personal information" to include the following data elements: (1) student, military, or passport identification number; (2) medical information; (3) health insurance identification number; (4) biometric data; and (5) a username or email address, in combination with a password or security questions and answers, that would permit access to an online account.[52]

Colorado also now requires notice be made within 30 days after the determination of a security breach.[53] Where Colorado and federal notification laws conflict, "the law or regulation with the shortest time frame for notice to the individual controls."[54] The amendments also provide specific content requirements for notification letters sent to Colorado residents. Now, notification letters must include the date, estimated date, or estimated date range of the security breach; a description of the acquired personal information; a way for the resident to contact the organization; toll-free numbers, addresses, and websites for consumer reporting agencies and the FTC; a statement that the resident can obtain information from the FTC and consumer reporting agencies about fraud alerts and security freezes; and, if the acquired data included a username or email address in combination with a password or security questions and answers for an online account, a statement directing the person to promptly change the password and security questions or answers or take other steps appropriate to protect online accounts that use the same username or email address.[55]

The amendments also require notification to the Colorado Attorney General in the event that notice of a security breach is made to 500 or more Colorado residents.[56] The amendments also create obligations for governmental entities, such as any Colorado state agency, county, or political subdivision, similar to those discussed earlier.[57]

The bill also amends Colorado's disposal requirements under Colo. Rev. Stat. § 6-1-713, which now requires covered entities that maintain paper or electronic documents containing personal information to develop a written policy for the destruction or disposal of such information once such documentation is "no longer needed."

Under House Bill 18-1128, Colorado also now has information security standards for personal information. Specifically, the bill also creates Colo.

52. Colo. Rev. Stat. § 6-1-716(1)(g)(I)(A).
53. *Id.*, § 6-1-716(2).
54. *Id.*, § 6-1-716(3)(b).
55. *Id.*, § 6-1-716(2)(a.2).
56. *Id.*, § 6-1-716(2)(f).
57. *See* Colo. Rev. Stat. § 24-73-103.

Rev. Stat. § 6-1-713.5, which requires covered entities to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information and the nature and size of the business and its operations. The security standards must also be placed in contracts with third-party service providers that receive the personal information from the covered entity.[58] Entities must also require third-party service providers, by contract, to implement and maintain reasonable security procedures and practices that are (1) appropriate to the nature of the personal information disclosed, and (2) must be reasonably designed to help protect the information from unauthorized access, use, modification, disclosure, or destruction.[59]

I. *California*

On June 28, 2018, California signed into law Assembly Bill 375, also known as the California Consumer Privacy Act of 2018 ("the Act"). Operative January 1, 2020, the Act is similar to the GDPR, in that both grant individuals the right to access and delete their personal information held by a business under certain circumstances. The Act provides an expansive definition of "personal information" to mean "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[60] The Act also includes a list of data sets that fall within its scope.[61]

The Act only applies to certain for-profit businesses that do business in California, control the collection or processing of consumers' personal information, and meet one of the following thresholds: (1) have annual gross revenues in excess of $25 million; (2) annually process personal information of 50,000 or more California consumers, households, or devices; or (3) derive 50% or more of its annual revenues from selling consumers' personal information.[62]

The Act provides a number of enforcement tools for both California consumers and the California Attorney General. In pertinent part, the Act creates a private right of action for any consumer whose unencrypted personal information is acquired without authorization as a result of a business's failure to implement and maintain reasonable security procedures to protect personal information.[63] A consumer bringing an action must also

58. Colo. Rev. Stat. § 6-1-713.5(2).
59. *Id.*
60. Cal. A.B. 375 (June 28, 2018), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=California+Consumer+Privacy+Act+of+2018.
61. *Id.*, § 1798.140(o)(1).
62. *Id.*, § 1798.140(c)(1)(A)–(C).
63. *Id.*, § 1798.150(a)(1).

provide notice to the Attorney General within 30 days of the action being filed.[64] The Attorney General must then review the action and either prosecute the action in place of the consumer, allow the action to proceed, or attempt to stop the action.[65] Also, intentional violations of the Act may be assessed a $7,500 penalty for each violation.[66]

II. STANDING

Standing "is a threshold jurisdictional question" that ensures a suit is "appropriate for the exercise of the [federal] courts" judicial powers.[67] The federal courts' standing requirement stems from Article III, section 2 of the United States Constitution, which provides that the "judicial Power shall extend to all Cases [and] Controversies."[68] In other words, a federal court's jurisdiction is limited to actual cases or controversies.[69] In order to determine whether a party has standing, the party invoking federal jurisdiction must show that the party "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."[70]

In pertinent part, in order to establish an injury-in-fact, "a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized.'"[71] In 2016, in its decision in *Spokeo, Inc. v. Robins*, the Supreme Court of the United States elaborated more on the "concreteness" requirement, explaining that concreteness "is quite different from particularization."[72] The Court explained that a concrete injury is one that "actually exist[s]" and is "real, not an abstract."[73]

The Court clarified that "concreteness" is not necessarily synonymous with "tangible."[74] An "intangible injury" can be sufficiently concrete to constitute an injury-in-fact.[75] In order to determine whether an intangible harm constitutes an injury-in-fact, "history and the judgment of Congress play important roles."[76] However, the Court did note that a plaintiff cannot automatically satisfy the injury-in-fact requirement just because "a statute

64. *Id.*, § 1798.150(b)(2).
65. *Id.*, § 1798.150(b)(3).
66. *Id.*
67. Pye v. United States, 269 F.3d 459, 466 (4th Cir. 2011) (citing Steel Co. v. Citizens for a Better Env't, 118 S. Ct. 1003 (1998)).
68. U.S. Const. art III, § 2, cl. 1.
69. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).
70. *Id.* at 1547 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).
71. *Id.* at 1548 (quoting *Lujan*, 504 U.S. at 560).
72. *Id.* at 1548.
73. *Id.*
74. *Id.* at 1549.
75. *Id.*
76. *Id.*

grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[77] That is, one cannot "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement."[78] In other words, a technical violation of a statute may not rise to the level of an injury-in-fact for constitutional purposes.

Recent federal court cases have had the opportunity to apply *Spokeo*'s elaborated standing analysis. The Ninth Circuit Court of Appeals held that the plaintiff had Article III standing to sue, but ultimately failed to show any "personally identifiable information" compromised under the Video Privacy Protection Act ("VPPA"). In *Eichenberger v. ESPN, Inc.*,[79] the plaintiff, Chad Eichenberger, downloaded ESPN's video streaming application on his Roku streaming device.[80] The plaintiff downloaded the application to watch sports-related news and events.[81] The plaintiff subsequently learned that ESPN was sharing his Roku device serial number and the names of the videos he watched to a third party, Adobe Analytics.[82] The plaintiff did not consent to ESPN's sharing his information with Adobe.[83]

The plaintiff sued ESPN, asserting that ESPN violated the VPPA by disclosing his "personally identifiable information" to Adobe.[84] The district court dismissed the action, finding that the information that ESPN disclosed did not constitute "personally identifiable information" under VPPA.[85] The plaintiff appealed.

On appeal, the defendant first argued that the plaintiff lacked Article III standing because he has not alleged a concrete harm.[86] However, the Ninth Circuit disagreed. The court explained that the VPPA provision at issue, 18 U.S.C. § 2710(b)(1), codified a context-specific extension of the substantive right to privacy.[87] The provision particularly states that "[a] video tape service provider who knowingly discloses . . . personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person . . . ."[88] The court explained this provision does not describe a procedure that video service providers must follow.[89] Instead, the provision generally protects a consumer's substantive privacy interest

77. *Id.*
78. *Id.*
79. 876 F.3d 979 (9th Cir. 2017).
80. *Id.* at 981. Roku allows users to view videos and other content on their televisions by means of Internet streaming.
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.* at 982.
85. *Id.*
86. *Id.*
87. *Id.* at 983.
88. *Id.*
89. *Id.*

in his or her video-viewing history.[90] The court looked to the provision's legislative history as well as historical practice to confirm that the VPPA identified a substantive right to privacy that suffers any time a video service provider discloses otherwise private information.[91] The court concluded that every violation of 18 U.S.C. § 2710(b)(1) "present[s] the precise harm and infringe[s] the same privacy interests congress sought to protect" by enacting the VPPA.[92] Thus, the court held that the plaintiff did have Article III standing to sue.

However, the court found that the allegedly disclosed information did not constitute "personally identifiable information" within the meaning of the VPPA. The VPPA defines "personally identifiable information" to "include[] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[93] The court further explained that "personally identifiable information" must include more information than that which, by itself, identifies an individual as having watched certain videos.[94] Instead, the term "personally identifiable information" covers some information that is "capable of" identifying a person, as well as information that, standing alone, identifies a person.[95]

In order to determine what information is "capable of" identifying an individual, the court adopted the Third Circuit's "ordinary person" test, which states that information that "readily permit[s] an ordinary person to identify" a particular individual as having watched certain videos is "personally identifiable information" under VPPA.[96] The court explained, and the plaintiff conceded, that the information disclosed (his Roku device serial number and the names of the videos that he watched) cannot identify an individual unless it is combined with other data in Adobe's possession—data that ESPN never disclosed and apparently never even possessed.[97] The court concluded that an ordinary person could not use the information that ESPN allegedly disclosed to identify an individual.[98] Thus, the court held the plaintiff failed to state a claim upon which relief can be granted.[99]

---

90. *Id.*
91. *Id.*
92. *Id.* at 984 (quoting Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037, 1043 (9th Cir. 2017)).
93. *Id.* at 984 (quoting 18 U.S.C. § 2710(a)(3)).
94. *Id.*
95. *Id.*
96. *Id.* at 985 (citing In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 284 (3d Cir. 2016)).
97. *Id.* at 985–86.
98. *Id.* at 986.
99. *Id.*

The Ninth Circuit Court of Appeals held that receiving an overly revealing credit card receipt, unseen by others, is not a sufficient injury to confer Article III standing. In *Bassett v. ABM Parking Services, Inc.*,[100] when the plaintiff, Steve Bassett, used his credit card at an ABM parking garage, he received a receipt displaying the card's full expiration date. The plaintiff filed a putative class action lawsuit against ABM, asserting a violation of 15 U.S.C. § 1681c(g) of the Fair Credit Reporting Act, which requires that businesses redact certain credit card information on printed receipts. The plaintiff alleged only a statutory violation and a potential for exposure to actual injury.[101] The district court granted ABM's motion to dismiss, finding that the plaintiff failed to allege a sufficiently concrete injury, and explaining that the plaintiff alleged nothing more than a "possible risk of [identity] theft."[102]

The Ninth Circuit agreed, holding that the plaintiff failed to allege a concrete injury. The court explained that the plaintiff's alleged injury is not supported by historical practice.[103] The court explained the plaintiff's alleged "'exposure' to identify theft—caused by ABM's printing of his credit card expiration date on a receipt that he alone viewed—does not have 'a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'"[104]

The court also noted that ABM never disclosed Bassett's information to a third party.[105] The court further distinguished this matter from cases involving unconsented text messages and consumer reports, explaining that "[w]hereas an undisclosed receipt may not 'cause harm or present any material risk of harm,' unconsented text messages and consumer reports divulged to one's employer necessarily infringe privacy interests and present harm."[106]

The court emphasized one of the holdings in *Spokeo*, that Congress's creation of a prohibition "does not mean that a plaintiff automatically satisfies the injury-in-fact requirement" just because "a statute grants [him] a statutory right and purports to authorize [him] to sue to vindicate that right."[107] Thus, the court explained that the plaintiff cannot merely "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."[108]

100. 883 F.3d 776 (9th Cir. 2018).
101. *Id.* at 777.
102. *Id.* at 778.
103. *Id.* at 780–81.
104. *Id.* at 780 (quoting *Spokeo*, 136 S. Ct. at 1549).
105. *Id.*
106. *Id.* at 781.
107. *Id.* (quoting *Spokeo*, 136 S. Ct. at 1549).
108. *Id.*

The Eighth Circuit Court of Appeals held a plaintiff failed to establish a fairly traceable injury sufficient to confer Article III standing. In *St. Louis Heart Center, Inc. v. Nomax, Inc.*,[109] the defendant, Nomax, Inc., transmitted via facsimile 12 advertisements promoting a potassium tablet to the plaintiff, St. Louis Heart Center. Each facsimile listed a fax number where the Heart Center could return a form to request product samples.[110] Six of the facsimiles included a box to check "[i]f you wish to no longer receive faxes from Nomax, Inc."[111] The other facsimiles included a box to check next to the statement: "Please do NOT fax to this office."[112] The faxes also listed the name, telephone number, and the email address of a contact person at Nomax.[113]

Heart Center filed a putative class action lawsuit against Nomax, asserting that Nomax violated the Telephone Consumer Protection Act ("TCPA") because the faxes failed to include proper opt-out notice required by the regulations implementing the TCPA.[114] Regarding its injury, Heart Center alleged the facsimiles caused it "to lose paper and toner that were consumed when receiving facsimiles, and that the transmissions interfered with the Heart Center's use of its fax machine and telephone line."[115] Additionally, Heart Center alleged its employees' time was wasted when they had to receive, review, and route the faxes.[116] Lastly, Heart Center alleged the faxes "interrupted the Heart Center's 'privacy interests in being left alone.'"[117]

During trial, Heart Center's president testified that he never gave Nomax consent to have advertising faxes sent to his office.[118] However, Heart Center's president acknowledged that the "class action was 'based upon the fact that the facsimiles that were sent did not have the proper opt-out notice,' and was 'not based upon the fact that consent was not given.'"[119] Heart Center's president also testified he did not attempt to opt out of receiving future faxes because the faxes did not have the proper opt-out notices.[120]

The district court dismissed the action for lack of standing, concluding that Heart Center had "'not alleged a concrete or particularized harm resulting from receiving faxes that [the Heart Center] both invited and did

109. 899 F.3d 500 (8th Cir. 2018), *pet'n for cert. filed* (Dec. 19, 2018).
110. *Id.* at 502.
111. *Id.*
112. *Id.*
113. *Id.*
114. *Id.* at 504 (citing 47 C.F.R. § 64.1200).
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*
120. *Id.*

not rebuke.'"[121] On appeal, the Eighth Circuit agreed that Heart Center lacked Article III standing to sue Nomax.[122] The court assumed that Heart Center may have satisfied the first requirement of Article III standing, in that Heart Center's allegations about loss of toner and paper, wasted time, and invasions of privacy "are sufficient to allege an injury in fact."[123] However, the court determined that Heart Center could not satisfy the second requirement that the injury be "fairly traceable" to the alleged violation of the TCPA because Heart Center conceded for purposes of the lawsuit that the faxes were not transmitted without consent.[124] Furthermore, the court explained that whether or not the faxes contained a proper opt-out notice, their transmission would have used Heart Center's paper and toner, and occupied its phone lines regardless. Because there was "no 'causal connection between the injury and the conduct complained of,'" the Heart Center has not established traceability.[125]

The court explained that although the faxes did not technically have the requisite opt-out notice, the notice still sufficiently conveyed to recipients the means and opportunity to opt-out of receiving future faxes.[126] Thus, the court concluded that the technical violation in the opt-out notices did not cause actual harm or create a risk of real harm.[127]

III. RIGHT TO PRIVACY

One of the fundamental rights sought to be protected by data privacy and cybersecurity statutes is an individual's right to privacy. Recent court cases have elaborated on an individual's right to privacy in terms of data privacy and cybersecurity concerns. Of note, in 2018, the United States Supreme Court issued a landmark decision concerning the right to privacy of one's cell phone records. Specifically, the Court held that individuals maintain a legitimate expectation of privacy in the records of their physical movements as captured by cell service providers, and, as a result, the government conducts a "search" for Fourth Amendment purposes when it accesses such records.

In *Carpenter v. United States*,[128] Mr. Carpenter was a suspected accomplice in a series of armed robberies committed in Michigan and

121. *Id.* at 503.
122. *Id.*
123. *Id.* at 504 (citing Florence Endocrine Clinic, PLLC v. Arrive Med., LLC, 858 F.3d 1362, 1366 (11th Cir. 2017) and Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037, 1043 (9th Cir. 2017)).
124. *Id.*
125. *Id.* (quoting *Lujan*, 504 U.S. at 560).
126. *Id.*
127. *Id.*
128. 138 S. Ct. 2206 (2018).

Ohio. Prosecutors applied for court orders under the Stored Communications Act ("SCA") to obtain Carpenter's cell phone records.[129] Under the SCA, the government can compel the disclosure of certain telecommunication records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[130] The court orders allowed the government access to 127 days of cell-site records and two days of cell-site location information ("CSLI") records, resulting in 12,898 location points cataloging Carpenter's movements.[131]

Carpenter was tried for six counts of robbery and six counts of carrying a firearm during a federal crime of violence.[132] The district court denied Carpenter's motion to suppress the cell-site data provided by the cell service providers.[133] At trial, the government introduced cell-site data that placed Carpenter's phone near four of the charged robberies.[134] Carpenter was ultimately convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.[135] The Sixth Circuit Court of Appeals affirmed the district court's denial of Carpenter's motion to suppress, holding that Carpenter lacked a reasonable expectation of privacy in the location information collected by the government because he had voluntarily shared that information with the third party cell service providers.[136]

The United States Supreme Court, however, reversed the conviction and held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[137] Thus, the Court determined that the government's actions constituted a search, which generally requires probable cause and a warrant, which the government did not have.

The Court's decision hinged on its interpretation of the "third-party doctrine," which generally allows the government to subpoena records without a warrant when the defendant has shared that information with a third party and thus, abandoned their reasonable expectation of privacy.[138] Here, the Court expressly declined to extend the third-party doctrine to include cell phone location records. In doing so, the Court distinguished the types of information typically at issue in third-party doctrine cases, such as dialed phone numbers and bank records, to the "exhaustive chronicle of

129. *Id.* at 2212.
130. *Id.* (quoting 18 U.S.C. §2703(d)).
131. *Id.*
132. *Id.*
133. *Id.*
134. *Id.*
135. *Id.*
136. *Id.* at 2213.
137. *Id.* at 2217.
138. *Id.* at 2219.

location information casually collected by wireless carriers today."[139] The Court noted that a cell phone is almost a "feature of human anatomy" that tracks nearly the exact movement of its owner.[140] Thus, a cell phone provides "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[141]

The Court recognized that the government will be able to use subpoenas to acquire records from a third party in the majority of investigations.[142] Thus, the Court ultimately held that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party."[143]

The Second Circuit Court of Appeals held that the Computer Fraud and Abuse Act ("CFAA")[144] was not unconstitutionally vague, and that suppression of evidence is not a remedy available for violating the SCA.[145] In *United States v. Gasperini*,[146] the defendant, Fabio Gasperini, an Italian citizen, created and distributed a computer virus to approximately 155,000 computers worldwide. The computer virus was aimed at accomplishing a number of different tasks, including copying usernames and passwords, coordinating attacks on certain websites, and clicking on banner advertisements which caused Gasperini to earn money for every click.[147]

Gasperini was indicted on several felony charges for the computer intrusion.[148] Following a jury trial, Gasperini was acquitted of all felony charges and was convicted only of misdemeanor computer intrusion in violation of the CFAA, which was a lesser-included crime within one of the computer intrusion felonies.[149] The district court sentenced Gasperini to the statutory maximum of one year.[150] Gasperini appealed the conviction, arguing that the CFAA was unconstitutionally vague, and the district court erred by not suppressing evidence obtained pursuant to search warrants under the SCA and by Italian law enforcement agents.[151]

The Second Circuit determined that Gasperini failed to assert a legitimate claim that the CFAA was unconstitutionally vague. The court explained that the CFAA punishes anyone who "intentionally accesses

139. *Id.*
140. *Id.* at 2218 (quoting Riley v. California, 134 S. Ct. 2473 (2014)).
141. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400 (2012)).
142. *Id.* at 2222.
143. *Id.*
144. 18 U.S.C. § 1030.
145. 18 U.S.C. §§ 2701–2712.
146. 894 F.3d 482 (2d Cir. 2018).
147. *Id.* at 485–86.
148. *Id.* at 486.
149. *Id.*
150. *Id.*
151. *Id.* at 485.

a computer without authorization . . . and thereby obtains . . . information from any protected computer."[152] Gasperini argued that the statute is unconstitutionally vague because it does not define the terms "access," "authorization," and "information," and because the statute's definition of "protected computer" is overly broad.[153] As an initial matter, the court noted that Gasperini failed to raise the issue of unconstitutional vagueness at the district court, and thus he was required to show the district court's ruling was plain error, which Gasperini failed to do.[154] But even assuming the statute's application may be unclear in some marginal cases, the court explained that Gasperini's conduct fell squarely and unambiguously within the core prohibition of the statute.[155] The court explained that since the CFAA was enacted to address "computer crime," which was principally understood as "hacking" or trespassing into computer systems or data, Gasperini's actions no doubt fell within the core meaning of the phrase "*accesses* a computer without *authorization* . . . and thereby obtains . . . *information* from [a] protected computer."[156]

Next, the court determined that the district court did not err in admitting evidence obtained under warrants from the SCA or by Italian law enforcement agents.[157] The court explained that the SCA limited the potential remedies for violations to specific remedies that do not include suppression of evidence in a criminal case.[158] Thus, Gasperini had not requested any form of relief authorized under the SCA.[159] Further, the court found that the Italian officials' search of Gasperini's home in Italy was done at the request of United States officials but not controlled by United States officials. Accordingly, the Italian searches did not have to be held to the constitutional standards that would apply to domestic searches conducted by United States officers.[160] Thus, the court affirmed the district court's decision.

The Second Circuit Court of Appeals held that individuals with nonstigmatizing medical conditions might still have a right to privacy in their

152. *Id.* at 486 (quoting 18 U.S.C. § 1030(a)(2)(C)).

153. *Id.*

154. *Id.* at 487 (citing Federal Rule of Criminal Procedure 52(b) and United States v. Marcus, 560 U.S. 258, 262 (2010)).

155. *Id.* at 487.

156. *Id.* (citing United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015)) (emphasis added).

157. *Id.* at 488.

158. *Id.* at 488–89 (citing 18 U.S.C. § 2707(b) & (d)).

159. *Id.* at 489.

160. *Id.* The court also determined that the district court did not abuse its discretion in allowing the government to introduce screenshots of various websites taken by the Internet archive, more commonly known as the "Wayback Machine." The court found that the government sufficiently laid the basis for the authenticity of the evidence and thus, it was well within the district court's discretion to admit it. *Id.* at 490.

medical records. In *Hancock v. County of Rensselaer*,[161] the plaintiffs were employees of the Rensselaer County Jail who were provided healthcare through Samaritan Hospital.[162] Samaritan Hospital provided a nurse at Rensselaer County Jail with electronic access to Samaritan's entire medical records system.[163] The nurse taped the login information to an inside drawer at the nurse's desk at Rensselaer County Jail, thus allowing anyone access to the medical records.[164] Of note, the Rensselaer County Sheriff enforced a sick leave policy that penalized employees for taking excessive amounts of sick leave.[165] The plaintiffs believed that the Rensselaer County Sheriff was improperly using this access to their medical records to investigate and monitor the plaintiffs' use of sick leave.[166]

The plaintiffs filed suit against Rensselaer County, the Sheriff, the nurse, and Rensselaer County Jail's chief of corrections, alleging violations of the CFAA and the Fourteenth Amendment of the United States Constitution.[167] The district court dismissed the plaintiffs' CFAA claims and later granted summary judgment in favor of the defendants on the plaintiffs' Fourteenth Amendment claims.[168] In its grant of summary judgment, the district court reasoned that the plaintiffs did not have a constitutionally protected interest in medical privacy because the medical conditions described in their records were insufficiently stigmatizing.[169]

The Second Circuit affirmed the district court's dismissal of the plaintiffs' CFAA claims because the plaintiffs failed to plead economic damages as required under the CFAA.[170] Furthermore, CFAA covers damages based on, in pertinent part, "potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals."[171] The plaintiffs argued that the Sheriff's ability to access their medical records to enforce his sick leave policy could have a chilling effect on the plaintiffs' inclination to seek medical care.[172] However, the court held the plaintiffs' concerns remained merely a hypothetical, and the plaintiffs failed to plead facts sufficient to "nudge their claims across the line from conceivable to plausible."[173]

161. 882 F.3d 58 (2d Cir. 2018).
162. *Id.* at 61.
163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.*
167. *Id.* at 62.
168. *Id.* at 63.
169. *Id.*
170. *Id.* at 63–64 (citing 18 U.S.C. § 1030(g)).
171. *Id.* at 63 (citing 18 U.S.C. § 1030(c)(4)(A)(i)(II)).
172. *Id.* at 64.
173. *Id.* (quoting Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007)).

The court, however, vacated the district court's grant of summary judgment on the plaintiffs' Fourteenth Amendment claims. The court acknowledged that the constitutional right to privacy is not absolute, as there are situations in which the government has a legitimate interest in accessing an individual's medical records.[174] The court explained that a constitutional violation depends on whether the individual's interest in privacy outweighs the government's interest in breaching it.[175] Where, as in this case, the government acts in its executive capacity, the court assesses whether the executive action was so "arbitrary" as to "shock the conscience."[176] Furthermore, when balancing the interest of privacy involving medical conditions, the court proceeds on a case-by-case basis, examining various factors.[177]

The court rejected the defendants' assertion that only sufficiently serious medical conditions give rise to any interest in privacy.[178] The court acknowledged that determining the strength of a privacy interest requires taking into account the seriousness of the condition and the stigma associated with it.[179] However, the court explained that other factors are relevant, such as how detailed the medical record is and whether a plaintiff has done anything to indicate a lack of interest in privacy in the particular information at issue.[180] Furthermore, the court explained that identifying the strength of the individual privacy interest does not end the inquiry.[181] Under the above-referenced "shock-the-conscience" standard, "even the weakest privacy interests cannot be overridden by totally arbitrary or outright malicious government action."[182]

Ultimately, the court held that the district court improperly treated the seriousness and stigma of each the plaintiffs' diagnosis as a threshold inquiry without considering other aspects of the individual privacy interest or the government's reasons for breaching confidentiality.[183] Thus, the court remanded so the district court could more thoroughly analyze the Fourteenth Amendment claims.

IV. TECHNOLOGY

As previously mentioned, data privacy and cybersecurity laws generally protect an individual's right to privacy. An extension of that right to privacy

174. *Id.* at 65.
175. *Id.*
176. *Id.* at 66 (citing O'Connor v. Pierson, 426 F.3d 187, 203 (2d Cir. 2005)).
177. *Id.*
178. *Id.*
179. *Id.* at 67.
180. *Id.*
181. *Id.* at 68.
182. *Id.*
183. *Id.*

is the right to be left alone. For example, the Telephone Consumer Protection Act ("TCPA") was enacted in 1991 to restrict unwanted telephonic solicitations. Enforced by the Federal Communications Commission ("FCC"), the TCPA generally prohibits calls made by an "automatic telephone dialing system" ("autodialer") to numbers without prior consent.[184]

What constitutes an "autodialer" has been the subject of many disputes arising under the TCPA. Autodialers are defined as equipment with the "capacity . . . to store" or dial telephone numbers by using a random or sequential number generator.[185] In a Declaratory Ruling and Order in 2015, the FCC extended the meaning of "capacity" to include devices that could be modified in the future to function as autodialers.[186]

The D.C. Circuit Court of Appeals pared back the FCC's interpretation of the TCPA definition of an "automatic telephone dialing system" by limiting it to devices with the "present capacity" to place calls randomly or sequentially. *ACA International v. FCC*[187] was the culmination of multiple petitions for review lodged with the D.C. Circuit Court of Appeals challenging, among other things, the FCC's interpretation of "capacity." In *ACA International*, the D.C. Circuit concluded that the FCC's application of the term "capacity" exceeded the TCPA's legislative intent to regulate unwanted calls from telemarketers.[188] The court explained that the FCC's view potentially extended to every smartphone that *could be* programmed to make automatic calls by downloading an application.[189] This meant that any caller making an unwanted call using a smartphone could be subject to the TCPA's statutory penalties, even if the autodialing feature was never actually downloaded, let alone used.[190] Instead, the court concluded that "capacity" was limited to the device's ability at the time of use.[191] Under this interpretation, "present capacity" would include a feature that can be activated by merely pushing a button but exclude modifications like software changes or updates.[192]

Several courts have gone on to apply *ACA International*'s "present capacity" standard. The District Court of Arizona ruled that a third-party text message platform was not an autodialer because it did not automatically store or produce randomly or sequentially generated numbers, nor could it send text messages without human intervention. In *Herrick v. GoDaddy*

184. 47 U.S.C. § 227(b)(1).
185. 47 U.S.C. § 227(a)(1).
186. In re Rules and Regulations Implementing the Tel. Consumer Prot. Act of 1991, 30 F.C.C.R. 7961 (2015).
187. 885 F.3d 687 (D.C. Cir. 2018).
188. *Id.* at 698.
189. *Id.* at 696 (emphasis added).
190. *Id.*
191. *Id.*
192. *Id.*

.com LLC,[193] the plaintiff sued GoDaddy for sending him an unsolicited promotional text message without his consent. GoDaddy contracted with a third-party platform to distribute the messages.[194] To do this, GoDaddy's employees had to (1) upload a pre-programmed list of numbers; (2) log in to the platform; (3) draft the message; (4) select the recipient numbers, as well as the date and time they would be sent; and (5) enter a 12-digit code to confirm the user was human.[195] The platform would then send the message.[196] GoDaddy filed a motion for summary judgment claiming that the platform was not an autodialer.[197]

Based on *ACA International*, the court limited its inquiry to the platform's "present capacity."[198] The court found the platform did not store or produce telephone numbers that were called by using a random or sequential number generator.[199] Instead, the numbers were uploaded by GoDaddy employees.[200] The court also noted that, to operate as an autodialer, the platform would need to be reprogrammed, and even if it was, prior CEO approval would still be required.[201] The court reasoned that such a limitation of access is more than a minor act to enable the autodialing function.[202]

The court also concluded the platform could not dial numbers or send messages without human intervention.[203] It compared the platform GoDaddy used to those used in other cases within the Ninth Circuit that found equipment was not an autodialer based on the level of human intervention.[204] This included devices that required the recipient numbers to be uploaded by a person;[205] messages that were only sent at the user's affirmative direction;[206] and where human intervention was "essential" to the system's ability to send messages.[207] In this case, since the platform could not automatically store and call the numbers using a random or sequential number generator, and because of the level of human intervention required

193. 312 F. Supp. 3d 792 (D. Ariz. 2018) (appeal filed June 7, 2018).
194. *Id.* at 793–94.
195. *Id.*
196. *Id.*
197. *Id.* at 794.
198. *Id.* at 796.
199. *Id.* at 800–01.
200. *Id.* at 800.
201. *Id.*
202. *Id.* at 801 (citing Marks v. Crunch San Diego, 55 F. Supp. 3d 1288, 1292 (S.D. Cal. 2014)).
203. *Id.* at 801.
204. *Id.* at 802.
205. *Id.* (citing Luna v. Shac, LLC, 122 F. Supp. 3d 936, 939 (N.D. Cal. 2015)).
206. *Id.* (citing McKenna v. WhisperText, No.: 5:14-cv-00424-PSG, 2015 WL 428728 (N.D. Cal. Jan. 30, 2015)).
207. *Id.* (citing Gragg v. Orange Cab Co., Inc., 995 F. Supp. 2d 1189, 1194 (W.D. Wash. 2014)).

to send the messages, the court granted GoDaddy's motion for summary judgment.[208]

The Third Circuit Court of Appeals held an SMS text message notification service was not an autodialer because the prior owner of a cell phone number had opted to receive messages, even though the subsequent owner had not. In *Dominguez v. Yahoo, Inc.*,[209] Dominguez received approximately 27,800 text messages from Yahoo's Email SMS Service over the course of 17 months.[210] The prior owner originally opted to receive the messages but did not cancel the subscription after the number changed hands.[211]

Dominguez filed a putative class action against Yahoo on the premise that its SMS Service was an autodialer.[212] The district court granted Yahoo's motion for summary judgment, finding that it was not an autodialer.[213] However, the ruling was vacated and remanded after the FCC issued its 2015 Declaratory Ruling.[214] Dominguez amended his complaint to allege that the SMS Service had the potential capacity to place autodialed calls.[215] Yahoo filed a second motion for summary judgment, and this time the district court granted it by finding that the 2015 Declaratory Ruling was not retroactive and, therefore, did not apply because the facts occurred before it was issued.[216] Applying the "present capacity" standard, the district court found Dominguez failed to produce any evidence that a genuine issue of material fact existed because each of his expert reports were excluded from evidence under *Daubert*.[217] Dominguez appealed. While it was pending, the D.C. Circuit Court issued its ruling in *ACA International v. FCC*.[218]

Confirming *ACA International*'s definition of "present capacity," the Third Circuit rejected Dominguez's "potential capacity" argument.[219] It then went on to consider whether Dominguez's four expert reports, even if admitted into evidence, posed a genuine issue of material fact that Yahoo's SMS Service had the "present capacity" to operate as an autodialer.[220] Three of the reports were rejected because they only addressed its "potential capacity."[221] The fourth report was rejected because it failed to

208. *Id.*
209. 894 F.3d 116 (3d Cir. 2018).
210. *Id.* at 117.
211. *Id.*
212. *Id.*
213. *Id.* at 118.
214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.*
218. *Id.* at 119.
219. *Id.*
220. *Id.* at 119–20.
221. *Id.* at 120.

show how it actually operated as an autodialer.[222] Without any evidence to support Dominguez's claim under the TCPA, the court affirmed summary judgment in Yahoo's favor.[223]

The Second Circuit Court of Appeals confirmed the TCPA only applies to devices that have the current ability to operate as an autodialer, and suggested this may include devices on which an autodial feature exists but is not being used. In *King v. Time Warner Cable Inc.*, [224] King, a Time Warner customer, received 163 calls from the company's automated dialing system. Time Warner's system made automated calls to customers with overdue accounts.[225] The problem was that the calls concerned another customer's account, not King's.[226] After 10 calls, King informed Time Warner about the mix up and asked to be placed on the company's "do not call list."[227] Despite this, she received an additional 153 calls.[228] She then filed suit against Time Warner under the TCPA for receiving calls without her consent.[229]

King and Time Warner both filed motions for summary judgment. Time Warner's motion was partially based on the premise that its dialing system was not an autodialer.[230] Relying on the FCC's 2015 Declaratory Ruling, the district court rejected this argument because it had the "potential capacity" to place calls randomly or sequentially.[231] The district court granted partial summary judgments in favor of both parties on other grounds.[232] Time Warner appealed the portion of the ruling that defined its system as an autodialer.[233]

ACA International was issued while the appeal was pending.[234] Applying the "present capacity" standard, the Second Circuit reasoned that "capacity" referred to the current ability of the device, not its potential capacity based on additional features.[235] It went on to find that "present capacity" includes a device's features that were not necessarily in use at the time of the offending call or text sent.[236] Notably, however, the court did not go as far as to distinguish what functionalities were required to meet this stan-

222. *Id.*
223. *Id.*
224. 894 F.3d 473, 474 (2d Cir. 2018).
225. *Id.* at 475.
226. *Id.*
227. *Id.*
228. *Id.*
229. *Id.*
230. *Id.* at 475–76.
231. *Id.* at 476.
232. *Id.*
233. *Id.*
234. *Id.*
235. *Id.* at 476–77.
236. *Id.* at 477.

dard.[237] Instead, it vacated the district court's ruling and remanded the case for further consideration of these issues.[238]

V. FTC ENFORCEABILITY

The FTC is widely considered the primary agency responsible for enforcing privacy laws in the United States. Under Section 5 of the Federal Trade Commission Act ("FTC Act"), the FTC is particularly responsible for investigating and preventing unfair and deceptive trade practices.[239] The FTC's enforcement powers are expansive, but they are not without limits. Recent decisions have analyzed the FTC's enforcement powers.

The Eleventh Circuit Court of Appeals held that an FTC order enjoining a company to install a data-security program was not enforceable because the FTC failed to enjoin a specific act of unfair trade practice. In *LabMD, Inc. v. FTC*, [240] a LabMD employee installed a file-sharing application commonly used for downloading music and videos on the employee's work computer.[241] The employee designated the entire "My documents" folder for sharing via the application, thereby making a 1,718-page LabMD file containing sensitive personal information of 9,300 consumers available to two to five million application users.[242] One of the users downloaded the 1,718-page LabMD file and delivered it to the FTC.[243]

After conducting an investigation, the FTC issued a complaint against LabMD.[244] According to the complaint, LabMD had engaged in practices that, taken together, had "'failed to provide reasonable and appropriate security for personal information on its computer networks.'"[245] The FTC asserted that such practices constituted an "'unfair act or practice.'"[246] An administrative law judge ("ALJ") dismissed the complaint.[247] The ALJ concluded the FTC did not prove that LabMD's alleged failure to maintain appropriate data security measures had caused or was likely to cause substantial injury to consumers.[248] However, on appeal, the full FTC Commission reversed, concluding that the enforcement staff had showed the likelihood of substantial injury in two ways: the "unauthorized disclosure of the [1718-page LabMD File] itself caused intangible privacy harm, and

237. *Id.*
238. *Id.*
239. 15 U.S.C. § 45(a)(2).
240. 894 F.3d 1221(11th Cir. 2018).
241. *Id.* at 1224.
242. *Id.*
243. *Id.*
244. *Id.* at 1225.
245. *Id.* (quoting FTC complaint).
246. *Id.* (quoting FTC complaint).
247. *Id.* at 1226.
248. *Id.*

the mere exposure of the [file on the file-sharing application] was likely to cause substantial injury."[249] The FTC issued an order against LabMD requiring it to "implement and maintain a data-security program 'reasonably designed' to the [FTC's] satisfaction."[250]

However, the Eleventh Circuit Court of Appeals held that the FTC's decision was unenforceable. The court explained that, in order to satisfy the constitutional requirements of due process, the FTC order must be "'sufficiently clear and precise'" and meet the FTC's own requirement of "'reasonable definiteness.'"[251] By failing to name a specific act subject to the FTC order and by failing to definitively describe what constituted "reasonably designed" security program, the FTC, in the court's opinion, failed to meet this standard.[252] The court explained the FTC's order would impermissibly mandate a complete overhaul of LabMD's data-security program, and the FTC's order said little about how this was to be accomplished.[253] Thus, the court held that, even assuming LabMD's failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5 of the FTC Act, the FTC's order was unenforceable because it did not enjoin a specific act or practice.[254]

The Ninth Circuit Court of Appeals, sitting *en banc*, concluded that Section 5 of the FTC Act exempts common carriers from the jurisdiction of the FTC only to the extent the common carriers engage in common-carriage activity. In *FTC v. AT&T Mobility LLC*,[255] the FTC brought an enforcement action against AT&T, claiming that AT&T's data-throttling practice was an unfair and deceptive practice in violation of the FTC Act.[256] In response, AT&T moved a district court to dismiss the case, arguing AT&T was exempt from the FTC's jurisdiction due to AT&T's status as a common carrier pursuant to Section 5 of the FTC Act.[257] FTC responded that the exemption applied only to AT&T activities as a common carrier and therefore did not exempt AT&T mobile data practices.[258] The district court denied AT&T's motion to dismiss, concluding that AT&T was not exempt from FTC oversight.

249. *Id.* at 1227.
250. *Id.* at 1230 (quoting FTC order).
251. *Id.* at 1235 (quoting 16 C.F.R. § 3.11; FTC v. Colgate-Palmolive Co., 380 U.S. 374, 392 (1965)).
252. *Id.* at 1236–37.
253. *Id.* at 1237.
254. *Id.*
255. 883 F.3d 848 (9th Cir. 2018) (en banc).
256. *Id.* at 851.
257. *Id.*
258. *Id.* at 852.

On appeal, the key issue before the Ninth Circuit was whether the common carrier exemption in the FTC Act was activity-based or status-based.[259] Similar to the district court, the Ninth Circuit relied on the legislative history, judicial decisions, and deferred to the FTC's interpretation of the provision.[260]

Considering the FTC Act's legislative history, the court noted that Congress had deliberately given the FTC broad enforcement powers and had intentionally chosen not to define the term "common carrier."[261] The court also pointed to the statements of the floor manager of the House bill that would become the FTC Act in favor of the activity-based approach.[262] The court cited to a number of judicial decisions rendered both before and after the adoption of the FTC Act in support of the notion that the common carrier exception is activity-based.[263]

Finally, the court deferred to the interpretations of both the FTC and the FCC urging the court to adopt the activity-based approach that would prevent a gap in the regulation of the common carriers' activities.[264] Thus, the court affirmed the district court's conclusion that AT&T was not exempt from FTC jurisdiction.[265]

VI. CYBERCRIMES

More and more insurance policies are including "computer-fraud" provisions, which generally cover losses arising from fraud conducted through a computer. Coverage for losses from computer fraud may be unpredictable, however, if the fraud is performed in conjunction with social engineering fraud (that is, fraud generally conducted by enlisting the trust of its victims to voluntarily disclose information or perform the fraudulent transaction). Recent decisions have analyzed these computer-fraud provisions in the context of policyholders who are victimized by social engineering fraud.

259. *Id.* at 853–54.
260. *Id.* at 853–56, 858–64.
261. *Id.* at 855–56.
262. *Id.* at 855.
263. *Id.* at 859–62 (citing RR Co. v. Lockwood, 84 U.S. 357 (1873); ICC v. Goodrich Transit Co., 224 U.S. 194 (1912); Santa Fe, Prescott, & Phx. Ry. Co. v. Grant Bros. Constr. Co., 228 U.S. 177 (1913) for decisions issued before the enactment of the FTC Act; and Kan. City S. Ry. Co. v. United States, 282 U.S. 760 (1931); McDonnell Douglass Corp. v. Gen. Tel. Co. of Cal., 594 F.2d 720 (9th Cir. 1979); Telesaurus VPC, LLC v. Power, 623 F.3d 998 (9th Cir. 2010); Nat'l Ass'n of Regulatory Util. Comm'rs v. FCC, 533 F.2d 601 (D.C. Cir. 1976); Comput. & Commc'ns Indus. Ass'n v. FCC, 693 F.2d 198 (D.C. Cir. 1982); Eagleview Techs., Inc. v. MDS Assocs., 190 F.3d 1195 (11th Cir. 1999); FTC v. Verity Int'l, 443 F.3d 48 (2nd Cir. 2006) for decisions issued after the enactment of the FTC Act).
264. *Id.* at 862–64.
265. *Id.* at 864–65.

The Ninth Circuit Court of Appeals, in an unpublished opinion, held that social engineering resulting from a spoofed email was not covered under a cyber-crime insurance policy. In *Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co. of America*,[266] the plaintiff, Aqua Star (USA) Corp. ("Aqua Star") regularly conducted business with Zhanjiang Longwei Aquatic Products Industry Co. Ltd. ("Longwei").[267] In the summer of 2013, Longwei's computer system was hacked, and the hacker monitored and intercepted email exchanges between an Aqua Star employee and a Longwei employee.[268] The hacker sent fraudulent emails using spoofed email domains that appeared similar to the Longwei employee's actual email address.[269] Through these emails, the hacker instructed the Aqua Star employee to change the bank account information for Longwei for further wire transfers.[270] Aqua Star made these changes as directed and was defrauded out of $713,890 by the hacker.[271]

Aqua Star sought coverage for its loss under its cyber-crime insurance policy issued by Travelers Insurance Company.[272] The policy stated that Travelers "will pay the Insured for the Insureds' direct loss of, or direct loss from damage to, Money . . . directly caused by Computer Fraud."[273] The policy contained several exclusions, including "Exclusion G," which stated that the policy "will not apply to loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System."[274] Travelers denied Aqua Star's claim, asserting that the loss was not directly caused by computer fraud, and that Exclusion G applied.[275]

Aqua Star sued Travelers for breach of contract and also sought declaratory relief.[276] During discovery, Aqua Star acknowledged that an authorized employee entered the fraudulent bank account information into Aqua Star's computer system.[277] The district court ultimately granted Travelers' motion for summary judgment.[278] The district court held that the entry of

266. 719 F. App'x 701 (9th Cir. 2018).
267. The facts of this case are drawn from the District Court's opinion. *See* Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. C14-1368RSL, 2016 U.S. Dist. LEXIS 88985 (W.D. Wash. July 8, 2016).
268. *Id.* at *1.
269. *Id.* at *2.
270. *Id.*
271. *Id.*
272. *Id.*
273. *Id.*
274. *Id.*
275. *Id.*
276. *Id.*
277. *Id.* at *6.
278. *Id.*

the bank account information was an indirect cause of Aqua Star's loss.[279] Thus, pursuant to Exclusion G, the loss was not covered under the policy.[280]

Aqua Star appealed.[281] However, the Ninth Circuit affirmed the district court's decision, stating that Exclusion G unambiguously provides that the policy will not apply to loss or damages resulting directly or indirectly from the input of electronic data by a person with the authority to enter the insured's computer system.[282] The Ninth Circuit explained that, as Aqua Star's losses were indirectly caused by an authorized employee's entry of data into the computer system, the court's review did not need go any further beyond the policy's plain language.[283] The court determined that the loss was not covered by the specific terms of the policy, and thus affirmed the district court's decision.[284]

The Sixth Circuit Court of Appeals, however, addressing a factually similar dispute did find that social engineering resulting from a spoofed email was covered under a cyber-crime insurance policy. In *American Tooling Center, Inc. v. Travelers Casualty & Surety Co. of America*,[285] American Tooling Center ("ATC") regularly conducted business with YiFeng, a vendor in China.[286] Between 2014 and 2015, ATC received a series of emails purportedly from YiFeng claiming that the vendor changed its bank accounts, and ATC should wire transfer payments to these new accounts.[287] After ATC transferred $834,000, ATC learned that the emails were fraudulent and were sent by a wrongdoer impersonating YiFeng.[288]

ATC sought coverage under the "Computer Fraud" provision of its insurance policy with its insurer, Travelers.[289] The policy stated, in pertinent part, that Travelers "will pay the Insured for the Insured's direct loss of, or direct loss from damage to, Money . . . directly caused by Computer Fraud."[290] The policy also contained several exclusions. The policy particularly excluded from coverage any loss resulting directly or indirectly (1) "from the giving or surrendering of Money . . . in any exchange or purchase, whether or not fraudulent, with any other party not in collusion with an Employee;" (2) "from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System;" or

279. *Id.* *7.
280. *Id.*
281. *Id.*
282. *Aqua Star (USA)*, 719 F. App'x at 701.
283. *Id.* at 702.
284. *Id.*
285. 895 F.3d 455 (6th Cir. 2018).
286. *Id.* at 457.
287. *Id.*
288. *Id.* at 457.
289. *Id.* at 458.
290. *Id.*

(3) "from forged, altered or fraudulent documentation in the preparation of Electronic Data . . . ."[291]

Travelers denied the claim, arguing that ATC did not suffer a "direct loss" as intended by the policy.[292] Travelers also argued that the "giving or surrendering" exclusion applied because ATC transferred the money to the impersonator, believing it to be YiFeng.[293] Travelers also argued that the "input of Electronic Data" exclusion applied, since an ATC employee entered the impersonator's banking information and the amount to be wired into the banking portal, thereby inputting "Electronic Data" into the computer system.[294] Lastly, Travelers argued that the "fraudulent documentation" exclusion applied, because the impersonator's emails were "fraudulent documents" and that the ATC employee relied upon those emails when entering the information into the banking portal to initiate the wire transfer.[295]

ATC sued for breach of contract.[296] Both parties moved for summary judgment, and the district court granted judgment in favor of Travelers.[297] However, on appeal, the Sixth Circuit Court of Appeals reversed this decision.[298] The court applied the commonly used meaning of "direct loss," which a prior unpublished opinion defined as a loss resulting from an immediate or proximate cause, as distinct from remote or incidental causes.[299] The court explained that ATC immediately lost its money when it transferred the $834,000 to the impersonator.[300] The court explained that since there was no intervening event, ATC did in fact sustain a direct loss.[301]

Regarding the "giving or surrendering" exclusion, the court explained that ATC did not transfer the money to the impersonator in exchange for anything from the impersonator, and therefore the fraudulent transfer did not fall within this exclusion provision.[302] The court further noted that this provision was "loosely worded and potentially ambiguous."[303] As such,

291. *Id.* at 463–65.
292. *Id.* at 450.
293. *Id.*
294. *Id.*
295. *Id.*
296. *Id.* at 457.
297. *Id.*
298. *Id.* at 459.
299. *Id.* (citing Acorn Investment Co. v. Mich. Basic Prop. Ins. Ass'n, No. 284234, 2009 WL 2952677 (Mich. Ct. App. Sep. 15 2009)).
300. *Id.*
301. *Id.* at 461.
302. *Id.*
303. *Id.* at 464.

potentially ambiguous language should be construed against the drafter.[304] Regarding the "input of Electronic Data" exclusion, the court noted that the policy's definition of "Electronic Data" excludes instructions or directions to a Computer System.[305] Strictly construed against Travelers, the court viewed the ATC employee's entry of the imposter's banking details as an entry of instructions or directions for the Computer System to issue payment, and therefore did not constitute "Electronic Data."[306] Regarding the "fraudulent documentation" exclusion, as the court already determined that the entry of the information into the Computer System did not constitute "Electronic Data" as provided by the policy, this exclusion was inapplicable.[307] The court concluded that ATC's loss was covered by the policy and none of the exclusions applied, and reversed the decision of the district court granting summary judgment to Travelers.

304. *Id.* (citing Harrah's Entm't. Inc. v. Ace Am. Ins. Co., 100 F. App'x 387, 391 (6th Cir. 2004)).
305. *Id.*
306. *Id.* at 465.
307. *Id.*