Study G-300 August 26, 2014

Memorandum 2014-34

State and Local Agency Access to Customer Information from Communication Service Providers: Federal Privacy Statutes

In 2013, the Legislature enacted Senate Concurrent Resolution 54 (Padilla), which directs the Commission[1] to make recommendations to revise the statutes that govern the access of state and local government agencies to customer information from communications service providers. The revisions are intended to do all of the following:

(1) Modernize the law.
(2) Protect customers' constitutional rights.
(3) Enable state and local agencies to protect public safety.
(4) Clarify procedures.

In conducting the study, the Commission is first analyzing existing law that affects government access to the customer information from communication service providers. Memorandum 2014-33 began the discussion of relevant federal statutory law, by examining the Electronic Communication Privacy Act of 1986. This memorandum completes the discussion of federal statutory law, by surveying other federal statutes that might have some relevance to the study. A future memorandum will examine California statutes protecting private information.

In preparing this memorandum, the staff searched broadly for federal statutes that touch on consumer privacy and consulted secondary sources that describe federal privacy laws. To assess whether a federal privacy statute is relevant to this study, the staff considered whether the statute satisfies the following criteria:

- The statute restricts disclosure of private information.

1. Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

- The disclosure restriction could apply to information held by a communication service provider.

A statute that meets both of those criteria is relevant, because it could restrict government access to customer information of a communication service provider. Any such restrictions would need to be considered in preparing proposed legislation for use in California. Statutes of this type are discussed under the heading "Applicable Disclosure Restrictions."

Some statutes meet the first criteria, but do not appear to meet the second. In other words, they restrict disclosure of certain information but it seems unlikely that such information would ever be "customer information of a communication service provider" within the meaning of SCR 54. If the staff is correct that the statutes could not apply to information held by a communication service provider, then they are not relevant to our study. These statutes are discussed under the heading "Inapplicable Disclosure Restrictions."

Finally, there are some privacy-related statutes that do not actually restrict disclosure of private information. These statutes are clearly not relevant to our study, because they do not impose restrictions that would need to be reflected in the proposed legislation that the Commission will be drafting. For the sake of completeness, those statutes are very briefly described, under the heading "No Restriction on Disclosure."

The contents of this memorandum are organized as follows:

APPLICABLE DISCLOSURE RESTRICTIONS 3
Health Insurance Portability and Accountability Act of 1996 3
Cable Communication Policy Act of 1984 7
Privacy Protection Act of 1980 8
Family Education Rights and Privacy Act of 1974 10
INAPPLICABLE DISCLOSURE RESTRICTIONS 11
Confidentiality of Alcohol and Drug Abuse Patient Records 11
Right to Financial Privacy Act of 1978 12
Driver's Privacy Protection Act of 1994 12
Privacy Act of 1974 13
Fair Credit Reporting Act of 1970 13
NO RESTRICTION ON DISCLOSURE 14

The Commission invites public input on the matters discussed in this memorandum and any other point that is relevant to this study. Any interested person or group can submit formal comment to the Commission, either in

writing or at a meeting. The staff is also open to receiving informal input, and is willing to meet with any interested group.

APPLICABLE DISCLOSURE RESTRICTIONS

The federal statutes that are described below are relevant to this study because they impose restrictions on the disclosure of certain information and those restrictions could be applicable to a communication service provider. Consequently, when the Commission reaches the point of drafting proposed legislation for California, it will need to be careful not to undermine or conflict with the requirements of these federal laws.

Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[2] addresses a number of issues relating to health insurance and healthcare administration. HIPAA is relevant to this study because it requires the Secretary of Health and Human Services to adopt regulations protecting the privacy of individual healthcare information.[3] The key requirements of those regulations (hereafter the "HIPPAA Privacy Rule"[4]) are discussed below.

General Prohibition

The HIPAA Privacy Rule generally prohibits the disclosure of protected health information by covered entities and their business associates.[5]

"Protected health information" is a defined term, which is in turn comprised of a series of other nested definitions.[6] For present purposes, it is sufficient to say that protected health information generally means information, in any form, created or received by specified entities, that relates to health condition, treatment, or payment for treatment, and that either identifies the subject of the information or makes it reasonably possible to determine that person's identity.[7]

2. P.L. 104-191 (1996).
3. *Id.* at § 264.
4. 45 C.F.R. § 164.500 *et seq*. See also 45 C.F.R. § 160.101 *et seq.*
5. 45 C.F.R. § 164.502(a).
6. See C.F.R. § 160.103 (defining "protected health information," "individually identifiable health information," and "health information").
7. *Id.*

Exceptions

The general prohibition is subject to a number of exceptions. Many of the exceptions relate to health care administration. Exceptions for government access that appear to be relevant to this study include the following:

- **Required by law**.[8] Information may be disclosed if the disclosure is required by law (e.g., legally required disclosure of suspected abuse, neglect, domestic violence,[9] certain serious wounds,[10] or communicable disease exposure[11]).
- **Use in adjudicative proceeding.** Information may be disclosed pursuant to a court order (or order of an administrative tribunal) in the course of a judicial or administrative proceeding.[12] Disclosure is also authorized pursuant to a subpoena, discovery request, or other lawful process, without a court order, provided that notice was given to the subject of the requested information or the disclosed information is subject to a protective order that limits its use.[13]
- **Court-ordered law enforcement access.**[14] Information may be disclosed to law enforcement pursuant to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer.
- **Grand jury subpoena.**[15]
- **Administrative request.**[16] An administrative subpoena (or similar investigative instrument) can be used to authorize disclosure where the information sought is "relevant and material to a legitimate law enforcement inquiry," the request is specific and limited, and "de-identified" information could not be used.
- **Incapacitated person suspected of being victim of crime.**[17]
- **Decedent suspected of being victim of crime.**[18]
- **Evidence of crime on disclosing entity's premises.**[19]
- **Information regarding patient identity and location.**[20]
- **Healthcare emergency.**[21] In a healthcare emergency, information may be disclosed to law enforcement if necessary to alert law

8. 45 C.F.R. § 164.512(a).
9. *Id.* at (c).
10. *Id.* at (f)(1)(i).
11. *Id.* at (b)(1)(iv).
12. *Id.* at (e)(i).
13. *Id.* at (e)(ii).
14. *Id.* at (f)(1)(ii)(A).
15. *Id.* at (f)(1)(ii)(B).
16. *Id.* at (f)(1)(ii)(C)
17. *Id.* at (f)(3)(ii).
18. *Id.* at (f)(4).
19. *Id.* at (f)(5).
20. *Id.* at (f)(2).

enforcement to the commission of a crime, the location of a victim, or the identity, description, or location of the perpetrator.

- **Serious threat to health and safety**.[22] Information may be disclosed based on a good faith belief that disclosure will prevent or lessen a serious and imminent threat to health or safety, or to identify or apprehend a violent criminal or a person who has escaped from a correctional facility.

As can be seen, those exceptions cover a lot of ground and most of them do not require a warrant issued by a court on a showing of probable cause.

Scope of Application

The prohibition on disclosure of protected health information only applies to a "covered entity" or a covered entity's "business associate."[23] A covered entity is a health plan, a health care clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.[24]

Could a covered entity ever be a "communication services provider" within the scope of the Commission's study? Perhaps, with regard to communication services that the covered entity provides. Some healthcare providers operate communication systems for use by their patients. Patients may be able to log onto the provider's website and send private messages to a doctor, fill prescriptions, access test results, and make appointments. In areas where medical facilities are inconveniently remote, providers may use online chat or videoconferencing to "meet" with patients. To the extent that a healthcare provider offers such communication services on its own equipment, it could be considered a communication service provider.

The Privacy Rule also applies to a "business associate" of a covered entity. A business associate is an entity that provides services to a covered entity that involve access to protected health information.[25] Could a business associate ever be a communications service provider? Probably. A healthcare provider might wish to provide the types of communication services described above, but may not wish to do so directly. If it were to contract with an internet communication

21. *Id.* at (f)(6).
22. *Id.* at (j).
23. 45 C.F.R. § 164.502(a).
24. 45 C.F.R. § 106.103.
25. *Id.*

company to develop and operate such services, that communication service provider would be a business associate of the covered entity.

Importantly, entities that simply serve as a communication "conduit" are not considered to be business associates.[26] However, "[t]he conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services."[27] For example, suppose that a patient exchanges messages with a doctor using a proprietary messaging system on the provider's website. The information contained in that system would be subject to the Privacy Rule because the healthcare provider is a covered entity. But the patient's ISP, which is used to access the healthcare provider's system would not be a covered entity or a business associate of a covered entity. It is acting only as a communication conduit.

Preemption

HIPPA and its implementing regulations expressly preempt contrary state laws.[28] However, the state may ask for an exception to preemption, by submitting a request to the federal Secretary of Health and Human Services.[29] The Secretary may grant such an exception if it is determined that the state law is stricter than the Privacy Rule or provides for certain specified types of data collection.[30]

Conclusion

There do appear to be circumstances where an entity subject to the HIPAA Privacy Rule could also be classified as a communication service provider (with respect to particular services). If so, there could be overlap between the requirements of HIPAA and California law on government access to customer information from communication service providers. When drafting proposed legislation in this study, the Commission will need to take care to avoid undermining or conflicting with the requirements of the HIPAA Privacy Rule.

---

26. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 17 (Jan. 25, 2013) (to be codified at 45 C.F.R pts. 160, 164).
27. *Id.*
28. 42 U.S.C. §§ 1320d-2(c)(2), 1320d-7; 45 C.F.R. § 160.203.
29. 45 C.F.R. § 160.204.
30. 45 C.F.R. § 160.203.

Cable Communication Policy Act of 1984[31]

The Cable Communication Policy Act of 1984 ("CCPA") was enacted to promote competition and deregulate the cable industry.[32] It is relevant to this study because it contains a provision that protects the privacy of subscriber information.

General Prohibition

The CCPA generally forbids a cable operator from disclosing personally identifiable information about a subscriber, without the subscriber's consent.[33]

Exceptions

The CCPA's general prohibition on the disclosure of subscriber information is subject to exceptions, the most relevant for our purposes being an exception for disclosure to law enforcement pursuant to a court order.[34]

A showing of probable cause is not required for the issuance of such an order. Instead, the government need only show "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case…."[35] However, the subject of the order must be given an opportunity to appear and oppose the issuance of the order.[36]

Scope of Application

The CCPA prohibition only applies to cable operators. A cable operator is a person "who provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system, or … who otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system."[37]

Could a cable provider be a communication service provider within the scope of our study? In many cases, yes.

It is not clear whether a cable company that provides *only* television services would be a communication service provider within the meaning of Senate Concurrent Resolution 54. Television is clearly a medium for mass

31. 47 U.S.C. ch. 5, subch. V–A.
32. 47 U.S.C. § 521.
33. 47 U.S.C. § 551(c).
34. *Id.* at (c)(2)(B), (h).
35. *Id.* at (h)(1).
36. *Id.* at (h)(2).
37. 47 U.S.C. § 522.

communication, but it does not provide means by which individuals can communicate.

In any event, cable companies are increasingly *also* providing Internet and telephone service over the same equipment that carries television programming. Clearly, a cable company that provides those services is a communication service provider.

Preemption

The CCPA expressly supersedes inconsistent state laws.[38] However, it does not preempt the entire field that it regulates.[39]

Conclusion

Because the CCPA restricts access to customer information of entities that could be communication service providers within the scope of the current study, the Commission will need to be careful not to undermine or conflict with the CCPA's requirements when drafting proposed legislation for California.

Privacy Protection Act of 1980

The Privacy Protection Act of 1980 ("PPA")[40] protects against police searches of the work product and other documentary materials of a journalist.

General Prohibition

The PPA generally prohibits the following:

> Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce…[41]

A similar prohibition applies to "documentary materials, other than work product materials."[42]

38. 47 U.S.C. § 556(c).
39. *Id.* at (a)-(b).
40. 42 U.S.C. § 2000aa.
41. *Id.* at (a).
42. *Id.* at (b).

Exceptions

The PPA's general prohibitions do not apply if there is "probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate…."[43]

That exception is subject to a further narrowing exception. It does not apply if the crime being investigated "consists of the receipt, possession, communication, or withholding of such materials or the information contained therein."[44] However, that limitation is itself subject to exceptions. It does not apply if the information sought relates to national defense, classified data, specified restricted data, or child pornography.[45]

There is also an exigency exception if there is reason to believe that immediate seizure is necessary to prevent death or serious bodily injury.[46] If the material to be seized is not work product, the general prohibition is also subject to exceptions where disclosure is sought for the following purposes:

- To prevent the destruction, alteration, or concealment of the documents.[47]
- To seize materials that have not been produced in response to a lawful subpoena, after the exhaustion of all appellate remedies.[48]

Scope of Application

The PPA affirmatively restricts government searches in criminal investigations, without regard to the place to be searched. It would therefore seem to apply to a government search of information held by a communication service provider. This does not seem far-fetched. Government could seek to obtain a journalist's email messages or notes held by an Internet Service Provider or cloud-storage service.

Discussion

It is easy to see how a government request to access a journalist's information held by a communication service provider could trigger the application of the PPA. In that case, the PPA would overlap with whatever state law governs access to customer information generally. In drafting proposed legislation, the

43. *Id.* at (a)-(b).
44. *Id.*
45. *Id.*
46. *Id.* at (a)(2), (b)(2).
47. *Id.* at (b)(3).
48. *Id.* at (b)(4).

Commission will need to give thought to how it can avoid creating a conflict between state law and the PPA. This will potentially be more difficult than accommodating the requirements of HIPAA and the CCPA. In those cases, it should be readily apparent that the entity being asked to disclose information is a healthcare provider or cable operator, thereby triggering the special federal statutory requirements.

By contrast, the applicability of the PPA may not be apparent to the communication service provider who is being asked to disclose customer information. The provider may have no idea that the customer at issue is a journalist. The Commission will need to give this issue careful attention.

Family Education Rights and Privacy Act of 1974

Among other things, the Family Education Rights and Privacy Act of 1974 ("FERPA")[49] protects the privacy of student education records.[50]

General Prohibition

Schools that are subject to FERPA must have written permission from a student's parent in order to release any information from a student's educational record.[51]

Exceptions

The general prohibition is subject to a number of exceptions. For our purposes, the most relevant exceptions are those that govern the following types of disclosure:

- Disclosure to the juvenile justice system, to serve the student's needs.[52]
- Disclosure to respond to an emergency.[53]
- Disclosure pursuant to a grand jury subpoena.[54]
- Disclosure pursuant to a subpoena issued for law enforcement purposes.[55]
- Disclosure to a child welfare agency.[56]

49. 20 U.S.C. § 1232g.
50. *Id.*
51. *Id.*
52. *Id.* at (b)(1)(E)(ii).
53. *Id.* at (b)(1)(I).
54. *Id.* at (b)(1)(J)(i).
55. *Id.* at (b)(1)(J)(ii).
56. *Id.* at (b)(1)(L).

- Disclosure pursuant to a court order or lawfully issued subpoena, with advance notice to the student's parents (except in cases of suspected child abuse).[57]

Scope of Application

FERPA applies to all educational institutions that receive funding from the U.S. Department of Education, except for post-secondary educational institutions.[58] Could such a school also be a communication service provider? Probably. Many schools provide proprietary messaging systems that allow students and parents to check grades online and send email messages to teachers and administrators. Such systems would seem to be communication services.

Conclusion

A government attempt to obtain the content of a student's educational records contained within a school's proprietary communication system would seem to be governed by both FERPA and general law on government access to customer records from a communication service provider. The Commission will need to bear this in mind when preparing proposed legislation in this study, to avoid undermining or conflicting with the protections afforded by FERPA.

INAPPLICABLE DISCLOSURE RESTRICTIONS

The federal statutes that are described below do not appear to be relevant to this study. While they do impose restrictions on the disclosure of certain information, those restrictions appear to be inapplicable to a communication service provider in California. Because the statutes appear to be irrelevant, they are described in less detail than the statutes above.

Confidentiality of Alcohol and Drug Abuse Patient Records

Federal law protects the confidentiality of certain alcohol and drug abuse treatment patient records and prohibits the disclosure of those records without patient consent:

> Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly

57. *Id.* at (b)(2).
58. *Id.*

> assisted by any department or agency of the United States shall … be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under … this section.[59]

As indicated, there are exceptions to that general prohibition. The most relevant for our purposes are an exception for disclosure pursuant to court order for the purposes of a criminal investigation[60] or for other good cause.[61]

The staff does not see any significant likelihood that a federally-assisted or federally-operated drug or alcohol treatment program would also be a communication service provider. Consequently, the provisions protecting against disclosure of the patient records of such programs does not seem relevant to the current study.

Right to Financial Privacy Act of 1978

The Right to Financial Privacy Act of 1978 ("RFPA") protects the confidentiality of personal financial records.[62]

RFPA requires that *federal* government agencies provide individuals with notice and an opportunity to object before a bank or other specified institution can disclose personal financial information to a *federal* government agency.[63] Because RFPA does not apply to state government agencies, its requirements are not described further. (State law governing access to personal financial information will be discussed in a future memorandum.)

Driver's Privacy Protection Act of 1994

The Driver's Privacy Protection Act of 1994 ("DPPA")[64] prohibits a "State department of motor vehicles, and any officer, employee or contractor thereof, from knowingly disclosing or otherwise making available to any person or entity"[65] the "personal information"[66] or "highly restricted personal information"[67] "about any individual obtained by the department in connection with a motor vehicle record."[68]

---

59. 42 U.S.C. § 290dd-2(a).
60. *Id.* at (c).
61. *Id.* at (b)(2)(C).
62. 12 U.S.C. § 3401 *et seq.*
63. *Id.* § 3402.
64. 18 U.S.C. § 2721 et seq.
65. *Id.* § 2721(a).
66. *Id.* § 2721(a)(1).
67. *Id.* § 2721(a)(2).
68. *Id.* § 2721(a)(1), (2).

The DPPA's general prohibition only applies to a Department of Motor Vehicles. The staff does not see any way in which the DMV could be classified as a communications service provider. More importantly, the DPPA does not apply to the disclosure of information "[f]or use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions." In other words, the law does not impose any restriction on government access to the protected information.

For those reasons, the DPPA is not relevant to the current study.

Privacy Act of 1974

The Privacy Act of 1974 ("Privacy Act")[69] "establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."[70] The Privacy Act prohibits the disclosure of such records except in specified circumstances.[71]

The Privacy Act only regulates the disclosure of federal agency records. It seems very unlikely that federal agencies would be communication service providers within the scope of the current study, especially with regard to the records they maintain to perform their administrative functions. Moreover, there is an exception to the general prohibition for disclosure to a government entity, including a state entity, for law enforcement purposes. The agency seeking the records need only submit a written request.[72]

For those reasons, the Privacy Act is not relevant to the current study.

Fair Credit Reporting Act of 1970

The purpose of the Fair Credit Reporting Act ("FRCA")[73] is to ensure accuracy and fairness of credit reporting. The FRCA requires consumer reporting agencies to adopt "reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which

69. 5 U.S.C. § 552a.
70. U.S. Department of Justice, Office of Privacy and Civil Liberties, Privacy Act of 1974, available at http://www.justice.gov/opcl/privacy-act-1974.
71. 5 U.S.C. § 552a(b).
72. *Id.* at (b)(7).
73. 15 U.S.C. § 1681 et seq.

is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information . . . ."[74]

Under the FRCA, credit reporting agencies can only disclose credit rating information for the purposes specified in the Act.[75] Any other disclosure would be a violation of the Act.

The FRCA only regulates credit reporting agencies. The staff does not believe that a credit reporting agency would ever be considered a communications service provider within the meaning of SCR 54. Moreover, the FRCA includes an exception to the general disclosure prohibition for a disclosure to a government agency.[76]

For those reasons, the staff does not believe that the FRCA is relevant to the current study.

NO RESTRICTION ON DISCLOSURE

As explained in the introduction to this memorandum, the staff also examined a number of statutes that appeared to touch on privacy but that do not actually restrict the disclosure of consumer information. Such statutes are not relevant to this study because they do not affect government access to customer information from communication service providers. For the sake of completeness, the statutes falling into this category are listed below:

- **Children's Internet Protection Act of 2001 ("CIPA").**[77] CIPA is designed to limit children's exposure to pornography and explicit online content. It requires that K-12 schools and libraries use internet filters and other technology to protect children from accessing harmful online content.
- **Children's Online Privacy Protection Act of 1998 ("COPPA")**.[78] The goal of COPPA is to put parents in control of what information commercial websites collect from their children online. Websites and online services covered by COPPA must post privacy policies, provide parents with direct notice of their information practices, and get verifiable consent from a parent or guardian before collecting personal information from children.

74. 15 U.S.C. § 1681(b).
75. *Id.*
76. 15 U.S.C. § 1681f.
77. Pub. L. 106-554, Tit. XVII (2000).
78. 15 U.S.C. §§ 6501-6506.

- **Communications Assistance for Law Enforcement Act of 1994 ("CALEA")**.[79] As discussed in Memorandum 2014-33, CALEA was enacted to preserve the ability of law enforcement agencies to conduct electronic surveillance pursuant to court order or other lawful authorization. CALEA requires telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve.
- **Consumer Fraud and Abuse Act of 1985 ("CFAA")**.[80] CFAA addresses improper access of confidential and secure government data. CFAA is primarily a criminal law intended to reduce the instances of malicious interference with computer systems and to address federal computer offenses.
- **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM").**[81] CAN-SPAM regulates solicitation emails and prohibits false or misleading transmission information, deceptive subject headings, and transmission of commercial electronic mail after objection.
- **Electronic Funds Transfer Act ("EFTA")**.[82] EFTA established the rights, liabilities, and responsibilities of all participants in electronic funds transfer activities, with a primary focus on individual consumer rights.
- **Federal Information Security Management Act ("FISMA")**.[83] FISMA was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
- **Federal Trade Commission Act ("FTC Act").**[84] The FTC Act created the Federal Trade Commission, which is "empowered and directed to prevent persons, partnerships, or corporations, [with some exceptions], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[85] Such unfair practices can involve the misuse of consumer information.

79. 47 U.S.C. §§ 1001-1010.
80. 18 U.S.C. § 1030.
81. 15 U.S.C. § 7701 *et seq.*
82. 15 U.S.C. § 1693 *et seq.*
83. 44 U.S.C. § 3541 *et seq.*
84. 15 U.S.C. § 41 et seq.
85. *Id.* § 45(a)(2).

- **Telephone Consumer Protection Act of 1991 ("TCPA")**.[86] TCPA restricts telephone solicitations and the use of automated telephone equipment.

Respectfully submitted,

Brian Hebert
Executive Director

Heather Zimmerman
King Hall Fellow

86. 47 U.S.C. § 227.