The Alabama Data Breach Notification Act of 2018

By Edward A. Hosp and Starr T. Drum

Senate Bill 318, which became the Alabama Data Breach Notification Act ("the Act") was introduced in the Alabama Senate by Senator Arthur Orr on Tuesday, February 13, 2018. It was revised significantly at every stage of the legislative process before receiving final passage on March 27. The bill was signed by Governor Kay Ivey on March 28 and became Act 2018-396. The new law went into effect on June 1.

The primary intent–and one could argue the only effect–of the legislation is to require timely notice to affected individuals when their personal information has been compromised, and to provide an enforcement mechanism for the Alabama Attorney General when a covered entity fails to provide that notice. Thus, *only* the failure to notify affected individuals and, when the breach affects more than 1,000 individuals, the attorney general, of a breach subjects an entity to penalties under the Act.[1] That said, there are actions that businesses are "required" to take, and, therefore, should be aware of, under various additional provisions of the new law.

The Alabama State Bar, in conjunction with the Alabama Supreme Court and the Administrative Office of Courts, created the Alacourt.com and Personal Identifying Information Task Force that is reviewing how lawyers and Alacourt address personal identification information, which also includes review of the new data breach law and its effect on the profession. Mike Ermert (*mike@hwnn.com*) and Tom Heflin (*tom@tomheflinlaw.com*) are the Alabama State Bar points of contact. The task force will make recommendations in the near future that will be applicable to our members.

I. What Entities Are Covered?

It is difficult to imagine any business operating in today's world that would not be covered by the new Alabama law. According to the definitions, a "covered

entity" is a person or a business of any kind that acquires what the law calls "Sensitively Personally Identifying Information" ("SPII"). The Act covers SPII of any individual–customer, employee, contractor or any other person.

II. What Is a "Breach Of Security"?

A "breach of security" or "breach" is defined as the "unauthorized acquisition of data in electronic form containing [SPII]." Multiple instances of unauthorized acquisition by the same source constitute a single breach.

III. What Data Is Considered "Sensitive"?

The new law requires notice when SPII in electronic form is acquired by an unauthorized entity. SPII is defined to include non-truncated data points that could facilitate identity theft, financial fraud or other harm when combined with the person's first name or initial and their last name. These include:

- Social Security number or tax ID number;
- Driver's license number, state-issued identification card number, passport number or military identification number;
- Bank account number, credit card number or debit card number (in combination with any security code, access code, password, expiration date or PIN);
- Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis;
- An individual's health insurance policy number or subscriber identification number *and* any unique identifier used by a health insurer to identify the individual;
- A user name or email address (in combination with a password or security question and answer that would permit access to an online account).

Thus, while a business should evaluate its security program, take steps to prevent data breaches in order to comply with other applicable laws and prevent financial and reputational damage, failure to do so would not result in the imposition of a penalty under the new Alabama law.

IV. What Is Required Before a Breach?

Act 2018-396 includes a few "requirements" for businesses that are preventative in nature. Specifically, the Act requires a covered entity to conduct an assessment of its data security, and then establish reasonable security measures to protect SPII from being breached. The Act also requires businesses to take reasonable steps when disposing of SPII to mitigate the risk of it falling into the wrong hands.

With respect to the evaluation and implementation of reasonable security measures, the Act provides guidance on how this should be done, but, as noted above, the only provisions of the Act that include an enforcement mechanism relate to the failure of an entity to provide notice to individuals or the Attorney General after a breach. Thus, while a business should evaluate its security program, take steps to prevent data breaches in order to comply with other applicable laws and prevent financial and reputational damage, failure to do so would not result in the imposition of a penalty under the new Alabama law.

Under the Act, what is required of a business for both the evaluation of its security needs and the implementation of reasonable security measures is expressly tied to the relative size of the entity, as well as the amount and type of SPII the business has in its possession. Also relevant to what is reasonable for a business to implement is the cost that would be incurred to put in place and to maintain certain security measures. In implementing a system of security, the Act instructs an entity to consider all of the following:

- Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security. An owner or manager may designate himself or herself;
- Identification of internal and external risks of a breach of security;
- Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards;

- Retention of service providers, if any, who are contractually required to maintain appropriate safeguards for SPII;
- Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of SPII; and
- Keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures.

V. What Is Required After a Breach?

A. Good Faith Investigation And Evaluation

Section 4(a) requires an entity that has suffered a breach to conduct a "good faith and prompt investigation" to determine:

- The scope of the breach;
- Whose information was compromised, and the nature of that information;
- Whether the breached information is "reasonably likely to cause substantial harm" to the person(s) whose information was lost; and
- Measures to be taken to restore security of the information and system breached.

Section 4(b) provides factors to consider in determining whether the breach is "reasonably likely to cause substantial harm." These factors include that the information is in the physical possession of an unauthorized person; that the information has been copied or downloaded; that the information has been used by an unauthorized person; and/or if the breached information has been made public.

It is imperative that a business maintain careful records of its activities following a breach, particularly relating to a determination of whether the breach was one that was "reasonably likely to cause substantial harm." Section 5 of the Act, which relates to the provision of notice, explicitly requires that records relating to this determination be maintained by the affected entity for five years.

B. Notice to Affected Individuals

Section 5 of the Act requires an entity that has determined it has suffered a breach of information that is "reasonably likely to cause substantial harm" to give notice of the breach to the affected Alabama residents. Notice must be given "*as expeditiously as possible* and without unreasonable delay," but in no event more than 45 days from the determination of the breach. Notice can (and should) be delayed when requested by federal or state law enforcement based on a criminal investigation or national security issues.

The time to inform individuals (and the attorney general under Section 6) begins to run from the date of the determination that the breach is "reasonably likely to cause substantial harm" and not from the date of the determination of the occurrence of the breach.

Section 5(d) sets forth the requirements for notice to affected Alabama residents. Notice must be in writing (mail or email) and must include the following:

- The date of the breach;
- The SPII that was breached;
- The actions taken to restore the confidentiality of the data;
- The actions that the impacted individual can take to protect himself/herself from the breach; and
- Information about how to contact the covered entity with questions.

Under certain circumstances, a business may be entitled to use substitute notice. The substitute notice provision is available under four circumstances:

- Insufficient contact information regarding the affected individuals;
- Excessive cost relative to the size and resources of the business;
- Where the breach affected more than 100,000 people; or
- Where the cost of notice would exceed $500,000.

In general, under the substitute notice provision, the entity must (1) post a conspicuous notice of the breach on its website for at least 30 days, and (2) place notice of the breach in print and broadcast in the area where affected individuals reside. However, the attorney general has the authority to approve an alternative method of substitute notice that can be proposed by the entity.

C. Notice to the Attorney General

The Act also requires written notice to the attorney general in the event the breach affects more than 1,000 Alabama residents. It is important that businesses not confuse the individual notice requirements with the requirement to notify the attorney general. Notice of a breach is ***always*** required to the affected individual–even if only one person is affected. Notice to the attorney general is only required if the number of affected Alabama residents exceeds 1,000 people.

As with the requirement for notice to individuals, notice to the attorney general must be made "as expeditiously as possible," but in no event more than 45 days after the determination that the breach is "reasonably likely to cause substantial harm."

The notice provided to the attorney general must include:

- A description of the "events surrounding the breach;"
- The number of Alabama residents affected;
- Services being offered to those affected by the breach; and
- Contact information for a point person[2] regarding the breach.

The Act provides that information provided to the attorney general marked as "confidential" will not be subject to any open records or freedom of information request. There is no provision that sets forth any mechanism for a business to make a determination of what should be confidential, but given the sensitive nature of a data breach and the potential harm to both the individuals and the business, it is reasonable to lean heavily toward designating the notice to the attorney general as "confidential."

D. Notice to Credit Reporting Agencies

Section 7 requires an entity suffering a breach that impacts an excess of 1,000 Alabama residents to also notify all nationwide consumer reporting agencies of the breach.

VI. What if a Third-Party Vendor I Use Suffers a Breach? (Or, What if I Am a Third-Party Vendor?)

Section 8 requires a third-party vendor (termed "third-party agent" under the Act) that suffers a breach to notify the covered entity of the breach within 10 days.

Once receiving that notice, the covered entity must provide the notices to affected individuals, the attorney general and consumer credit reporting agencies as set forth in Sections 5, 6 and 7 of the Act.

Where there is a breach of a third-party agent, the time for a covered entity to provide notice begins to run when the covered entity receives notice of the breach from that third-party entity.

The third-party agent is required to cooperate with the covered entity and provide the covered entity with "information in the possession of the third-party agent so that the covered entity can comply with its notice obligations."

In general, this section places the requirement for providing notice to affected individuals and to the attorney general on the covered entity and not the third-party agent. However, a change was made in the senate to clarify that the parties may enter into a contractual arrangement that would allow that burden to be shifted to (and satisfied by) the third-party agent. It is important for this (and other) reason(s) to carefully review and negotiate contracts where SPII will change hands.

VII. Penalties and Enforcement

There are two provisions in SB318 under which an entity could face penalties. First, Section 9(a) provides that a violation of "this Act" is a violation of the Alabama Deceptive Trade Practices Act ("DTPA"), but is not a criminal offense under the DTPA. As noted above, the bill was clarified in the senate to make it clear that only violations "of Sections 5, 6, or 7 of this Act" (the notice provisions only) are considered violations of the DTPA. Further, section 9(a)(1) states that a violation of the Act does not establish a private cause of action.[3]

Section 9(a)(2) provides that the penalty provisions of the DTPA apply if a party has "knowingly engaged in a violation of this act." This section clarifies that for the purposes of this act, "knowingly" shall mean "willfully or with reckless disregard." As such, in order to apply the DTPA to a violation, there must be a heightened level of culpability on the part of the covered entity. Although the penalty provisions of the DTPA provide that a violation is subject to a civil penalty of up to $2,000 per violation, this section of the Act caps possible penalties under the DTPA at $500,000 per breach.

Section 9(b)(1) provides a per breach civil penalty of $5,000 per day (theoretically commencing no sooner than the 46th day after a breach) against an entity that fails to take reasonable steps to comply with the Act.

Section 9(b)(2) allows the attorney general–and only the attorney general–to bring an action on behalf of individuals. This provision may allow the attorney general to pursue an action against an entity for the breach itself–rather than for a failure to notify. However, damages are limited in such an action to "actual damages."

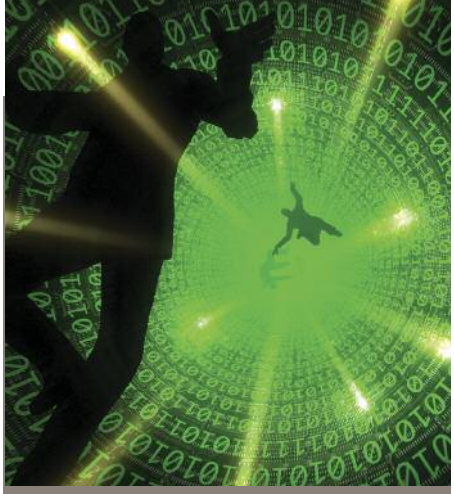
VIII. Entities Subject To Existing Federal or Other Alabama Data Breach Standards

An exemption section, Section 11, was included in the bill for entities that are subject to data breach standards under federal laws or regulations. Under Section 11, an entity subject to such standards that complies with those standards and that provides notice of a breach to affected individuals pursuant to those standards is exempt from the act–as long as it also provides a copy of the individual notice to the attorney general if more than 1,000 Alabama residents are affected.

The goal of this section is to ensure that an entity subject to federal data breach standards, such as the Gramm-Leach-Bliley Act ("GLBA") or the Health Insurance Portability and Accountability Act ("HIPAA") is not required to alter its existing procedures and systems as a result of this Act.

A. GLBA

The potential breach notification obligations under the GLBA vary by industry and regulator. Title V, Subtitle A of the GLBA governs the treatment of nonpublic personal information about consumers by financial institutions. The definition of "financial institution" is exceedingly broad–often broader than many businesses realize.[4] A full list of activities that would bring a business within scope is listed in Section k(4) of the Bank Holding Act.[5] The GLBA requires financial institutions to design, implement and maintain standards to protect nonpublic consumer information,[6] which become promulgated as the Safeguards Rule. The Safeguards Rule is implemented and enforced by eight different federal and state agencies, depending on the type of financial institution at issue.[7] Banks are regulated in this regard



Where there is a breach of a third-party agent, the time for a covered entity to provide notice begins to run when the covered entity receives notice of the breach from that third-party entity.

by the federal banking agencies (e.g., Federal Reserve, FDIC, OCC). State departments of insurance enforce the Safeguards Rule against insurance companies. The SEC regulates brokers, dealers, investment companies and investment advisors. The Federal Trade Commission (FTC) has become a sort of "catch-all" regulator of the GLBA for financial institutions who do not fall within one of these or other enumerated categories, such as nonbank mortgage lenders, loan brokers, tax preparers, providers of real estate settlement services and debt collectors.

Certain regulators, pursuant to the Safeguards Rule as implemented by each regulator, require or at least recommend notice to affected individuals following a data breach of nonpublic personal information. For example, the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," promulgated by the federal banking agencies, requires notice to affected individuals upon unauthorized access to "sensitive customer information" when there has been misuse of that information or misuse is reasonable possible.[8] The FTC Safeguards Rule itself does not mention individual notice,[9] but subsequent guidance published by the FTC recommends that non-bank financial institutions notify impacted individuals in the event of a security breach.[10] The information that typically qualifies under the Safeguards Rule as implemented is much broader than under Alabama's data breach notification statute.

B. HIPAA

The HIPAA Breach Notification Rule[11] requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services (HHS), and in some cases, the media, of a breach of unsecured Protected Health Information ("PHI"). While there is substantial overlap between the definition of PHI and that of SPII in the Alabama Act, the definition of "covered entity" under HIPAA is much narrower than under Alabama's new Act–only health care providers, health plans and health care clearinghouses are within scope.[12] If a HIPAA-covered entity experiences a potential security breach that impacts SPII of Alabama residents, it should comply with its notice obligations under HIPAA, which involves performing a four-part risk assessment to determine the risk of harm to impacted individuals, and then, if warranted, supplying notice to such persons within 60 days.

C. Alabama State Law-Based Exemption

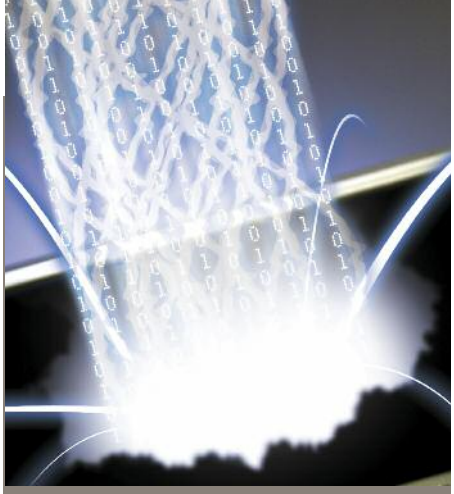
The senate floor substitute added a new Section 12 that provides an

exemption similar to Section 11 for entities that are subject to Alabama state law data breach requirements that are at least as strict as the provisions of this legislation. This change was made to accommodate an anticipated change in Alabama law based on recommendations of the National Association of Insurance Commissioners ("NAIC"). Section 12 of the Alabama Act states that when an entity is subject to a data breach and notification provision of state law that is at least as stringent as the Act, the company need only comply with that law, without regard to the requirements of SB318.

IX. Entities Subject to International Data Security and Privacy Regulations

Although the Act provides for state and federal exemptions, there is no exemption for entities covered by international laws such as the GDPR. The GDPR is European regulation, but its requirements extend beyond the boundaries of the European Union and apply where an entity:

1. Has an establishment as a controller or processor in the European Union, even if the processing of personal data takes place outside of the European Union;
2. Offers goods and services to individuals in the European Union;
3. Monitors the behavior of individuals in the European Union (*e.g.* through an application that tracks location or activity); or



Section 12 of the Alabama Act states that when an entity is subject to a data breach and notification provision of state law that is at least as stringent as the Act, the company need only comply with that law, without regard to the requirements of SB318.

4. Provides processing services for a controller established in the European Union.

The GDPR applies both to controllers (entities that determine why and how personal data is processed), and to processors (entities who process personal data at the direction of controllers). The GDPR also regulates all "personal data," which is much more broadly defined than SPII as "any information relating to an identified or identifiable natural person."[13]

In terms of data protection, the GDPR requires an organization to "implement appropriate technical an organizational measures to ensure a level of security appropriate to the risk."[14] Though the GDPR does not impose specific data security requirements, it offers some examples of "appropriate" security measures as:

- Pseudonymization;
- Encryption;
- The ability to ensure the continuous confidentiality, integrity, availability and resiliency of processing systems and services;
- The ability to restore access and availability to personal data in the event of a physical or technical incident; and
- Processes for regular testing, assessment and evaluation of the security measures in place.

A "data breach" is also defined more broadly under the GDPR than under the Act and includes any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed."[15] The breach notification provisions under the GDPR require an affected processor entity to notify the controller of a breach "without undue delay."[16] A controller who is notified of a breach by a processor or who is independently subject to a data breach must notify a European supervisory authority of the breach within 72 hours after becoming aware of it.[17] Communications to affected individuals must be made by the controller "without undue delay" where the breach is "likely to result in a high risk to the rights and freedoms of natural persons."[18]

An organization that fails to comply with the data security and data breach notification requirements of the GDPR can be exposed to penalties of up to €10,000,000 or 2 percent of their worldwide annual revenue– whichever is greater.[19] While the penalties for GDPR violations are serious and have been receiving a

lot of attention recently, it is important for a company with an international presence or reach to keep in mind that the GDPR is just one of many international data protection laws that the Act does not exempt. And unlike the Act, a number of international laws, including the GDPR, explicitly allow for civil remedies in addition to regulatory fines, even where the affected individual cannot demonstrate material damages.[20]

X. Potential Civil Liability under the Act

It is important to note that although Section 9(a)(1) of the Act explicitly forecloses a private right of action under Section 8-19-10 (Alabama Unfair and Deceptive Trade Practices Act), that does not necessarily mean that a business who sustained a data breach affecting Alabama residents would be immune from a civil lawsuit. That same section also states that "[n]othing in this act may otherwise be construed to affect any right a person may have at common law, by statute, or otherwise." Thus, the Act may not prevent litigants from bringing a lawsuit arising out of a covered entity's failure to timely notify, or out of a covered entity's data breach generally, if the suit is based on a common law cause of action. Plaintiffs lawyers have presented various theories in data breach cases around the country in recent years–some of the more common causes of action include negligence, negligence per se, breach of contract and unjust enrichment.[21]

The impact that the standards in the Alabama Act–both the notification requirements and the proactive data security requirements–will have on civil litigation remains to be seen. It is at least plausible that litigants on both sides will look to the standards to either prosecute or defend a company's actions both before and after a data breach. For example, will the 45-day deadline serve as a benchmark in private lawsuits to measure "timely" notice? Will a company be more likely to be deemed negligent if it did not contractually require its third-party vendor to safeguard personal information, as is required under the Act? Or, will the prohibition on a private right of action limit or even prohibit private litigants from relying on the statute in support of their common law claims? Questions like these would be matters of first impression for Alabama courts.

The doctrine of negligence per se poses an especially interesting question here in terms of the possibility of the Act's requirements serving to establish a duty or standard of care. Alabama allows a plaintiff to proceed with a negligence claim under a statute that does not otherwise provide a cause of action under the doctrine of *negligence per se*.[22] The doctrine of negligence per se "arises from the premise that the legislature may enact a statute that replaces the common-law standard of the reasonably prudent person with an absolute, required standard of care." *Parker Bldg. Servs. Co. v. Lightsey ex rel. Lightsey*, 925 So. 2d 927, 930-31 (Ala. 2005) (citing *Thomas Learning Ctr., Inc. v. McGuirk*, 766 So.2d 161, 171 (Ala. Civ. App. 1998)). To state a claim under a negligence per se theory, the plaintiff must establish "(1) The statute must

have been enacted to protect a class of persons, of which the plaintiff is a member; (2) the injury must be of the type contemplated by the statute; (3) the defendant must have violated the statute; and (4) the defendant's statutory violation must have proximately caused the injury." *Anderson v. United States*, 2016 WL 270965, at *1 (N.D. Ala. Jan. 22, 2016) (citing *Parker Bldg. Servs. Co. v. Lightsey ex rel. Lightsey*, 925 So. 2d 927, 931 (Ala. 2005)). In the abstract, the Alabama Act should serve as an effective vehicle for a negligence per se claim following a data breach. However, some courts outside Alabama have refused to allow negligence claims to go forward where the respective state data breach notification statutes have not provided for a private right of action.[23] Alabama businesses–and Alabama lawyers–will have to wait and see how Alabama courts will treat such claims now that Alabama's own data breach law is on the books.

Conclusion

The handling and potential breach of sensitive personal data are among the greatest risks faced by businesses today. A prudent organization, therefore, must be proactive in addressing these risks and putting safeguards into place to prevent a breach, as well as incident response plans to implement in the event that a breach occurs. One step in formulating such a plan is making a determination about which standards may apply–state, federal or even international–and understanding exactly what is required under each standard. Although Alabama is late to the game with respect to a state-based data breach law, its adoption serves as a reminder to all businesses to make sure they know what their data security and privacy vulnerabilities are and how to deal with them. ▲

Endnotes

1. Contrast this with the recently enacted European General Data Protection Regulation ("GDPR"), enacted on May 25, 2018, which requires entities within the regulation's scope to undertake a number of proactive privacy and security measures and provides for enforcement through both regulators and private causes of action, even where the damage is "non-material." *See* Part IX, *infra*.
2. The Act simply requires that this person be an "employee or agent" of the covered entity, which means that the point person may come from within or outside the covered entity. Presumably, outside counsel would meet the requirement.
3. Despite this language, *see* Section X, *infra*, for a brief discussion of potential civil liability under various common law private causes of action.
4. 15 U.S.C. § 6809(3).
5. 12 U.S.C. § 1843(k).
6. 15 U.S.C. § 6801(b).
7. 15 U.S.C. § 6805(a).
8. 70 Fed. Reg. 15,736 (Mar. 29, 2005) (codified at multiple locations).
9. *See* 16 CFR 314.
10. Federal Trade Commission, Financial Institutions and Customer Information: Complying with the Safeguards Rule, *https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying* (last accessed July 7, 2018).
11. 45 CFR 164.400-414.
12. 45 CFR 160.103.
13. GDPR Art 4(1).
14. GDPR Art. 32(1).
15. GDPR Art. 4(12).
16. GDPR Art. 33(2).
17. GDPR Art. 33(1).
18. GDPR Art. 34.
19. GDPR Art. 83. Other GDPR violations not addressed in this article can subject a company to regulatory penalties of up to €20,000,000 or 4 percent of worldwide annual revenue, whichever is greater. *Id.*
20. *See e.g.* GDPR Art. 82.
21. *See, e.g., Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012); *In re Anthem, Inc. Data Breach Litigation*, 162 F.Supp.3d 953 (N.D. Cal. Feb. 14, 2016); *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2017 WL 1044692 (M.D. Ala. Mar. 17, 2017).
22. *See Smith v. Triad of Alabama, LLC*, 2015 WL 5793318, *11 (M.D. Ala. Sept. 29, 2015) (citing *Allen v. Delchamps, Inc.*, 624 So. 2d 1065, 1067-68 (Ala. 1993)). *See also Bocage v. Acton Corp.*, No. 2:17-CV-01201-RDP, 2018 WL 905351, at *8 (N.D. Ala. Feb. 15, 2018) ("Alabama case law allows negligence *per se* claims to be based on both federal and state statutes even when a private right of action is not contemplated by the statute in question").
23. *In re Anthem, Inc. Data Breach Litigation*, 162 F.Supp.3d at 976-97* (dismissing plaintiffs' negligence claims arising out of defendants' data breach, holding that data breach actions must be brought by the Indiana Attorney General, and discussing cases where other courts did not allow data breach plaintiffs' negligence claims to proceed).

Edward A. Hosp

Ted Hosp is the chair of Maynard Cooper's governmental and regulatory affairs practice group, and is a founder and the immediate past chair of the Alabama State Bar Section on Ethics, Elections & Government Relations Law. He also serves as chair of the Alabama Access to Justice Commission, and is a member and past chair of the ASB Pro Bono Committee.

Starr T. Drum

Starr Drum is a member of Maynard Cooper's cybersecurity & privacy and complex litigation practice groups. Drum has been recognized as a Mid-South Rising Star Super Lawyer since 2016 and has been certified by the International Association of Privacy Professionals in privacy program management and European data protection, and as a Fellow of Information Privacy. She is a frequent speaker and writer on data privacy issues and is also an adjunct professor at the University of Alabama School of Law.