PREPARED TESTIMONY AND STATEMENT FOR THE RECORD
OF

WOODROW HARTZOG
ASSOCIATE PROFESSOR OF LAW
SAMFORD UNIVERSITY'S CUMBERLAND SCHOOL OF LAW

HEARING ON

"WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?"

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE
U.S. HOUSE OF REPRESENTATIVES

January 27, 2015
2123 Rayburn House Office Building
Washington, DC

I. INTRODUCTION

Chairman Burgess, Vice Chairman Lance, Ranking Member Schakowsky, and Members of the Committee, thank you for inviting me to appear before you and provide testimony. My name is Woodrow Hartzog and I am an associate professor of law at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School. I write extensively about information privacy law issues and have published well over a dozen law review articles and other scholarly works. Most relevant to this hearing, I have spent the past three years researching the law and policy of data protection, data security, and responses to data breaches.[1] My comments today will address what I've learned from this research.

Instead of debating the finer points of any specific proposal for data breach legislation, I will focus my remarks on how the fundamental goals of data protection should guide any federal response to data breaches. These comments are made in my personal, academic capacity. I am not serving as an advocate for any particular organization. My remarks will focus on two points.

First, I will argue that sound data breach legislation should be minimally preemptive of existing state and sector-specific data breach laws. It is not yet clear what the most effective approach to data protection and breach response is. Multiple regulatory bodies are still needed to protect our personal information in order to ensure the adequate resources and experimentation necessary to respond to constantly evolving threats and new revelations about our vulnerability. Additionally, preemption threatens to water down some of the important existing robust data breach protections. There is a real risk that preemptive federal legislation would do more harm than good. Our critical data protection infrastructure will be weakened if federal legislation scales back protection, consolidates regulatory authority, and sets specific rules in stone. Data breach law must offer robust protection and be able to evolve quickly.

Second, I will argue that sound data breach legislation must also incorporate requirements for data security. While data breach notification is important, we must be sure we do not ask too much of it. The law should require, not just encourage, reasonable data security practices from companies that collect, process, and share personal information. This will fortify the protection of personal information in the United States and help ensure that fewer breach notifications need to be sent at all.

---

[1] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014), available at http://ssrn.com/abstract=2312913; Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015), available at http://ssrn.com/abstract=2461096; Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA PRIVACY & SECURITY LAW REPORT 577 (2014), available at http://ssrn.com/abstract=2424998; Woodrow Hartzog & Daniel J. Solove, *The FTC as Data Security Regulator: FTC v. Wyndham and its Implications*, 13 BNA PRIVACY & SECURITY LAW REPORT 621 (2014), http://docs.law.gwu.edu/facweb/dsolove/files/BNA%20FTC%20v%20Wyndham%20FINAL.pdf.

II. THE GOALS OF DATA BREACH LEGISLATION

Data breach laws are relatively new. In the early 2000s it became clear that personal data was a critical component of our national infrastructure and that the threat to this data was mounting. The Privacy Rights Clearinghouse has reported that since 2005 there have been over 4400 data breaches made public with a total of over 932 million records breached.[2] Unfortunately, data protection is a process largely hidden from consumers, who typically have no way of knowing if databases containing their personal information were compromised. It became clear that a legal response was necessary to ensure that companies were motivated to protect personal data and to keep users and the public informed about data breaches.

The first state data beach statute was passed by California in 2003.[3] Since that time, 47 states have adopted some form of data breach legislation. Additionally, federal legislation such as the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act also contain a notification requirement.[4] The main component of data breach legislation is to require companies to notify certain people and entities in the event of a breach. Many data breach laws often require companies to provide some measure of reasonable security for their data.

While the particular details of these laws vary, together they demonstrate a commitment to three clear goals. In order to be effective, data breach legislation must provide: 1) Transparency, 2) Data protection, and 3) Consumer remedies. The patchwork of existing state and federal sector-specific laws already further these goals. General federal legislation that preempts this protection and fails to ensure that these goals will continue to be realized will cripple our critical data protection infrastructure. Hard won consumer protections will be lost. In short, any data breach legislation that fails to advance these three goals will be counterproductive.

A. Transparency

It is important to understand these values that animate data breach legislation in order to carefully craft law. Transparency is perhaps the most salient and important goal of data breach legislation. Transparency is primarily achieved through the notification function of these laws. While specific details vary, generally data breach notification laws require companies to notify affected individuals and, in some circumstances, media, the public, and centralized organizations, in the event of a data breach.[5] While public discussion

---

[2] PRIVACY RIGHTS CLEARINGHOUSE, *Chronology of Data Breaches: Security Breaches 2005 – Present*, https://www.privacyrights.org/data-breach.

[3] CAL. CIV. CODE §§ 1798.29, .82, .84 (2012).

[4] 16 C.F.R. § 682.3(a); 45 C.F.R. §§ 164.308-.314; 16 C.F.R. §§ 314.3-314.4.

[5] *Id.*; ALASKA STAT. § 45.48.010 *et seq.*(2007); ARIZ. REV. STAT. § 44-7501 (2013); ARK. CODE § 4-110-101 *et seq.* (2004); CAL CIV. CODE §§1798.29, .82, .84 (2012); COLO. REV. STAT. § 6-1-716 (2002); CONN. GEN. STAT. § 36a-701b (2011); DEL. CODE tit. 6, § 12B-101 *et seq.* (2011); FLA. STAT. §§501.171, 282.0041, 282.318(2)(i) (2010); GA. CODE §§ 10-1-910, -911, -912 § 46-5-214 (West); HAW. REV. STAT. § 487N-1 *et seq.*(2008); IDAHO STAT. §§ 28-51-104 to -107 (2008) ; 815 ILL. COMP. STAT. ANN. §§ 530/1 to 530/25 (2008); IND. CODE §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*(2014); IOWA CODE §§ 715C.1, 715C.2 (2015);

about the efficacy of breach notification usually focuses on the individual whose data was compromised, there are actually four different constituencies that are served by the transparency goal of breach notification.

Of course, transparency primarily benefits individuals affected by a breach. When people are notified quickly of a breach, they know to look for evidence of fraud and identity theft. They can take remedial measures such as credit monitoring or even a credit freeze. If account credentials are compromised, notification prompts people to change their usernames and passwords on the compromised website as well as any other service where they use the same credentials.

Breach notification also benefits other companies that have personal data. News of data breaches travels quickly between chief security officers and others in charge of protecting the personal data controlled by a company. Companies that are in similar situations to those suffering a breach can learn how they might avoid the same fate. By learning the details of how information was compromised and what kinds of businesses and information is being targeted, other companies can proactively respond new threats.

Breach notification also advances the discipline and study of data security. By learning about new threats and tactics, industry experts and academics in the field of data security can improve the discipline of protecting data. Breach notifications can be aggregated to reveal important facts and trends that benefit an entire field, especially when laws require that notification be given to a centralized organization in addition to consumers. For example, the State Attorneys General in both California and New York have issued comprehensive reports that analyze the data obtained from breach notification laws.[6] These reports provide critical insights into the evolving threats to personal data.

KAN. STAT. § 50-7a01 *et. seq.* (2008); KY. REV. STAT. ANN. §§ 365.732, 61.931 to 61.934 (West); LA. REV. STAT §§ 51:3071 *et seq.* 40:1300.111 to .116 (West); ME. REV. STAT. tit. 10 § 1347 et seq. (2009); MD. CODE COM. LAW §§ 14-3501 et seq. (2013), MD. STATE GOVT. CODE §§ 10-1301 to -1308 (2007); MASS. GEN. LAW § 93H-1 *et seq.* (2006); MICH. COMP. LAW §§ 445.63,445.72 (2014); MINN. STAT. §§ 325E.61, 325E.64 (2011); MISS. CODE § 75-24-29 (2014); MO. REV. STAT. § 407.1500 (2014); MONT. CODE §§ 2-6-504, 30-14-1701 *et seq.* (2014); NEB. REV. STAT. §§ 87-801, -802, -803, -804, -805, -806, -807 (2014); NEV. REV. STAT. §§ 603.A.010 *et seq.*, 242.183 (2013); N.H. REV. STAT. §§359-C:19, -C:20, -C:21 (2009); N.J. STAT. ANN. § 56:8-163 (2012); N.Y. GEN. BUS. LAW § 899-aa, N.Y. STATE TECH. LAW 208 (McKinney 2014); N.C. GEN. STAT. §§ 75-61, 75-65 (2012); N.D. CENT. CODE § 51-30-01 *et seq* (2008).; OHIO REV. CODE §§ 1347.12, 1349.19, 1349.191, 1349.192 (2004); OKLA. STAT. §§ 74-3113.1, 24-161 to -166 (2014); OR. REV. STAT. § 646A.600 to .628 (2011); 73 PA. STAT. §2301 *et seq*. (2013); R.I. GEN. LAWS § 11-49.2-1 *et seq*. (West); S.C. CODE § 39-1-90 (West); TENN. CODE § 47-18-2107 (2014); TEX. BUS. & COM. CODE §§ 521.002, 521.053 (2014), TEX. ED. CODE § 37.007(b)(5) (2013); UTAH CODE §§ 13-44-101 *et seq*. (2010); VT. STAT. tit. 9 § 2430, 2435 (2007); VA. CODE § 18.2-186.6, § 32.1-127.1:05 (2012); WASH. REV. CODE § 19.255.010, 42.56.590 (2013); W.V. CODE §§ 46A-2A-101 *et seq*. (West); WIS. STAT. § 134.98 (2009); WYO. STAT. § 40-12-501 *et. seq.* (2007); D.C. CODE § 28-3851 *et seq*. (2013); 9 GCA § 48-10 *et seq.*; 10 LAWS OF PUERTO RICO § 4051 *et seq.*; V.I. CODE tit. 14, § 2208.

[6] Kamala D. Harris, *California Data Breach Report* (October 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf; Eric T. Schneiderman, *Information Exposed: Historical Examination of Data Breaches in New York State* (2014), http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf.

Finally, breach notification raises the public awareness of threats to data and the importance of vigilance and data protection. When data breaches are made public due to notification laws, sometimes by laws mandating notice be given directly to media, the public becomes better informed of the importance of data protection. Ideally, this helps create a more cautious and sophisticated public that is less likely to be careless when sharing and protecting their personal data. Additionally, breach notifications can encourage productive communication between consumers and companies that collect personal information. When breaches are more on the minds of consumers they are more likely to enquire about and demand responsible data practices, either in negotiations or in the marketplace.

B. Data Protection

Sound data breach legislation should also motivate companies to protect data. Pure notification statutes encourage companies to protect data by facilitating a reputational and financial penalty for those suffering a breach. Companies are not eager to have their data breaches made public. Not only does this news tend to tarnish a company's reputation in the eyes of current and potential consumers, but it also can negatively affect a company's reputation among its peers and potential partners or investors. Additionally, the cost of notification can be significant if the breach involves a large number of records. The reputational and financial cost of notification gives companies the incentive to protect data to minimize the likelihood of a breach. These costs also encourage companies to audit their data, assess risk, and develop a breach response plan ahead of time, all of which benefit those whose personal data is at risk.

Data breach legislation can also obligate companies to provide reasonable data security practices. Indeed, many state and sector-specific laws have data security requirements in addition to notification requirements.[7] As I argue below, mere incentives to secure data are not sufficient, given the critical importance of data protection in the modern world. Data breach legislation must require reasonable data security from companies.

C. Remedies for Individuals

Finally, data breach legislation should provide remedies for individuals affected by a breach. The most common kind of remedy is some provision of services like credit monitoring or facilitation of a credit freeze. These services help an individual respond to identity theft and fraud. Data breach statutes differ as to the extent these services are to be offered or suggested.[8] These statutes also differ as to who the services and information are to be offered to. Some laws only provide remedies to those who have been actually

[7] *See e.g.* MASS. GEN. LAW § 93H-2 (West 2006); ARK. CODE ANN. § 4-110-104(b) (Supp. 2007); 2008 CONN. ACTS No. 08-167 (Reg. Sess.); NEV. REV. STAT. ANN. § 603A.210 (West Supp. 2007); N.C. GEN. STAT. § 75-64(a) (2007); OR. REV. STAT. ANN. § 646A.622(1) (West Supp. 2008); R.I. GEN. LAWS § 11-49.2-2(2) (Supp. 2007); UTAH CODE ANN. § 13-44-201(1)(a) (Supp. 2007); 45 C.F.R. §§ 164.308-.314.

[8] *See e.g.* CAL CIV. CODE § 1798.29 (West 2012) (requiring consumer notification including the time of breach and the toll free numbers and addresses of credit card reporting agencies in California); MD. STATE GOVT. CODE § 10-1305 (West 2007) (requiring consumer notice of the information breached, along with the contact information of the state Attorney General, the FTC and credit reporting agencies).

harmed. Others provide some form of a remedy for all individuals affected by a breach. Additionally, the breach laws in 17 states provide for a private cause of action for individuals.[9] These protections help individuals recover from the loss of their personal information.

III. THE IMPORTANCE OF MINIMAL PREEMPTION

Sound federal data breach legislation should only minimally preempt existing state and sector-specific data notification and security laws. Minimal preemption respects existing consumer protections and the ongoing uncertainty of how to best protect data in the information age. Existing federal data protection legislation has respected the multiple approaches to data protection. Legislation that weakens existing state and federal consumer protections by preempting them with weaker protections will jeopardize individuals. Legislation that frustrates the diversity of approaches and ability for laws to be modified will stunt the natural and important evolution of data protection policy.

A. State and Sector-Specific Protections Should Be Preserved

The current patchwork of state and sector-specific data breach laws covers a broad range of data and offers different forms of protection. Almost all of these laws advance the goals of transparency, protection, and remedies. There are three main ways by which aggressive federal preemption would be counterproductive.

First, federal legislation would leave people more vulnerable if it replaced robust substantive protections in state and sector-specific laws with weaker requirements. For example, if federal data protection legislation applied to fewer companies or kinds of personal information than existing law, mandated a showing of harm before companies were required to send notification, or failed to require notice to a centralized organization like the Office of the State Attorney General, it would reduce the level of protection many or most Americans currently have.

Second, data breach legislation would be counterproductive if it created gaps in protection. Federal data breach legislation that preempts all state data breach laws could fail to cover data breaches that only affect the residents of one state. Additionally, preemptive legislation that only covered digitized records would fail to cover breaches involving paper records, which remain a significant target for data thieves.

[9] ALASKA STAT. § 45.48.010 *et seq.* (West 2007); CAL CIV. CODE §§ 1798.29, .82, .84 (West 2012); DEL. CODE tit. 6, § 12B-101 *et seq*. (West 2011); La. Rev. Stat §§ 51:3071 *et seq.* 40:1300.111 to .116 (West); MD. CODE COM. LAW §§ 14-3501 et seq. (West 2013), MD. STATE GOVT. CODE §§ 10-1301 to -1308 (West 2007); MASS. GEN. LAW § 93H-1 *et seq.* (West 2006); MINN. STAT. §§ 325E.61, 325E.64 (West 2011); N.H. REV. STAT. §§359-C:19, -C:20, -C:21 (2009); NEV. REV. STAT. §§ 603.A.010 *et seq.*, 242.183 (2013); N.C. GEN. STAT. §§ 75-61, 75-65 (West 2012); OR. REV. STAT. § 646A.600 to .628 (West 2011); R.I. GEN. LAWS § 11-49.2-1 *et seq*. (West); S.C. CODE § 39-1-90 (West); TENN. CODE § 47-18-2107 (2014); VT. STAT. tit. 9 § 2430, 2435 (West 2007); VT. STAT. tit. 9 § 2430, 2435 (West 2007); WASH. REV. CODE § 19.255.010, 42.56.590 (West 2013); D.C. CODE § 28-3851 *et seq.* (2013).

Finally, as I argue below, data breach legislation would be regressive and harmful if it consolidated total responsibility for data breach notification and security into one regulatory agency. Data protection is part of the critical infrastructure in the United States and requires multiple regulators who bring specific expertise and additional resources into the fold.

If federal legislation must be preemptive, it should only preempt state laws that address the same specific area as that federal law, for example, the notification response time. A better alternative would be for federal legislation to serve as a floor, not a ceiling for regulation. This would allow state and sector-specific laws to be more protective, but not less. Ideally, preemptive data breach legislation would strengthen data breach law by introducing new features not present in existing statutes and regulations.

B. Data Breach Law Must Be Capable of Evolution and Continued Experimentation

Data breach legislation should be minimally preemptive because multiple approaches are still needed to determine the best approach to data security and breach notification. While general principles can be agreed upon, more data is needed to determine the most effective particularized requirements of breach legislation. For example, the definition of personal information to be covered by the statute has been in flux since California passed the first data breach statute in 2003. Many breach laws contain a trigger requirement for notification that in some way is dependent upon a perceived risk of harm, which is a dubious and contested concept in policy and academic circles. The time frame for notice among statutes also varies between 5 to 30 days or is a more general standard such as "within the most expedient time possible and without unreasonable delay." A consensus has not even been reached on the optimal form and content of the notification itself.

Data breach law must remain nimble while such uncertainty persists. If the preemptive effect of federal data breach legislation is not minimized and specific rules are set in stone, data protection policy cannot effectively evolve. Continued experimentation and analysis is necessary before any federal law regarding data protection should have dramatic preemptive effect.

IV. DATA SECURITY REQUIREMENTS MUST BE INCLUDED AND PRESERVED IN BREACH LEGISLATION

Data breach laws serve an important function in generating transparency and helping people respond when their information has been breached. But the effectiveness of breach notification in protecting personal information is limited. Under a pure breach notification scheme, providing reasonable data security is voluntary. Companies protect data to the extent they minimize the risk of a reputational and financial penalty associated with notifying its customers of a breach. This risk calculation will be different for all companies. Not all companies fear reputational penalties, particularly if the data they are holding is not that of their own customers.

We must not ask breach notification to do more work than it is capable of. Specifically, data breach law should not let data security be voluntary. If people cannot trust entities that collect and store our personal information, then commerce, innovation, public health, our personal relationships, and our culture will be significantly damaged. Therefore any data breach legislation must include requirements that all entities collecting personal data reasonably secure it.

Legislating data security protections is challenging because of the ever-evolving threats to personal information as well as the fact that data security protections are heavily dependent upon context. As a result, it is notoriously difficult to create specific data security rules that are broadly applicable. Any such specifications risk being simultaneously over-protective in some situations and under-protective in others. Thus, the best approach is to seek flexible standards amenable to clarification and modification over time. Additionally, data breach legislation should ensure that multiple regulatory bodies create and enforce data security policy. Legislation reducing both expertise and available resources to protect data would make people more vulnerable to data breaches.

A. The FTC Should Have Rulemaking Authority for Data Security

The FTC's regulation of privacy and data security under Section 5 of the Federal Trade Commission Act has served a critical function for the U.S. system of data protection. Under this statute, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[10] The FTC has used this authority to regulate companies under theories of deceptive promises of data security and unfair data security practices.

Starting with its first privacy-related actions in the late 1990s, the FTC has evolved into the most important data protection agency in the United States. The FTC plays two critical roles within the U.S. data protection ecosystem. It fills significant gaps left by the patchwork of statutes, torts, and contracts that make up the U.S. data protection scheme. The FTC also stabilizes the volatile and rapidly evolving area of data protection and provides legitimacy and heft for the largely sectoral U.S. approach to data protection.

The FTC has been effective using a case-by-case approach under Section 5. However, the agency is limited because although the FTC has specific rulemaking authority under COPPA and GLBA, for Section 5 enforcement—one of the largest areas of its jurisprudence—the FTC has only Magnuson-Moss rulemaking authority, which is so procedurally burdensome that it is largely ineffective.[11]

Specific rulemaking authority for data security would have several benefits. Rules would help the FTC further clarify data security standards in combination with its data security complaints. The FTC's current jurisdiction under Section 5 is limited to commercial entities. An effective grant of rulemaking authority would also cover non-profit entities and entities not engaged in commerce, such as educational institutions. Finally, effective

[10] 15 U.S.C. § 45(a)(1).
[11] Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended at 15 U.S.C. §§ 45–46, 49–52, 56–57c, 2301–2312 (2012)).

data security rulemaking authority for the FTC would also include the ability to issue civil penalties against companies that fail to provide reasonable data security.

A reasonableness standard is thus far the most desirable for regulating data security. Most data security laws adopt some form of a reasonableness standard. What constitutes reasonable data security is determined by context and industry standard practices. Deference to industry keeps regulators from promulgating data security rules in an arbitrary and inconsistent way. This approach builds upon the formidable and evolving body of knowledge in the data security field and common data security practices. There is a consensus that custodians of personal information act unreasonably when they fail to identify their assets and risk, minimize collection and storage, implement administrative, technical, and physical safeguards, and develop data breach response plans.

B. Multiple Regulating Bodies Should Be Responsible for Data Security

Numerous federal agencies require data security from companies in some form, including the Federal Trade Commission (FTC), the Federal Communications Commission, (FCC), the Department of Health and Human Services (HHS), the Securities and Exchange Commission (SEC), and the Food and Drug Administration (FDA). Other agencies, such as the Federal Aviation Administration (FAA) and the National Highway Transportation Safety Administration (NHTSA) have been encouraged to regulate data security in new technologies such as drones and automated cars. These agencies are not redundant in regulating data protection. Rather, they can and do coexist with unique expertise and regulatory authority. Even agencies with overlapping jurisdiction contribute valuable resources and have relatively harmonized approaches to data security.

Data security is not just a national issue. It is also a local issue, sometimes affecting a small but significant group of state residents. Even in the case of large, national breaches, residents of some states are hit harder than others. Federal data breach legislation must preserve the ability of states to regulate data security. States are nimble and capable of continued experimentation regarding the best approach to regulating data security. They are also closer to those whose data was compromised. Finally, states provide additional resources to alleviate the strain and cost of enforcement on federal agencies.

V. CONCLUSION

Sound federal data breach legislation should provide better transparency, more robust data security, and more effective remedies for individuals affected by a breach. However, legislation that replaces strong consumer protections with weaker ones, creates gaps in protection, and frustrates the ability for data protection law to evolve will do more harm than good. The modern threat to personal data is still relatively new. The concept of data breach legislation is newer still. It is too early to start rolling back protections and consolidating agencies to cut costs. Instead, sound data breach legislation should reinforce the current trajectory of data protection law which involves multiple approaches and constantly evolving robust consumer protection.

BIOGRAPHY

Woodrow Hartzog is an Associate Professor at Samford University's Cumberland School of Law and Affiliate Scholar at the Center for Internet and Society at Stanford Law School.

Professor Hartzog is an internationally-recognized expert in the area of privacy, media, and robotics law. He has been quoted or referenced in many articles and broadcasts, including *NPR, the New York Times, the Los Angeles Times*, and *USA Today*.

Professor Hartzog's work has been published in numerous scholarly publications such as the *Columbia Law Review, California Law Review*, and *Michigan Law Review* and popular national publications such as *CNN, Wired*, *Bloomberg, New Scientist*, *The Atlantic*, and *The Nation*. He serves on the advisory board of the Future of Privacy Forum.

Before joining the faculty at Cumberland School of Law, Professor. Hartzog worked as a trademark attorney at the United States Patent and Trademark Office in Alexandria, Virginia, and as an associate attorney at Burr & Forman LLP in Birmingham, Alabama. He also served as a clerk for the Electronic Privacy Information Center in Washington, D.C., and was a Roy H. Park Fellow at the School of Journalism and Mass Communication at the University of North Carolina at Chapel Hill.

Professor Hartzog holds a Ph.D. in mass communication from the University of North Carolina at Chapel Hill, an LL.M. in intellectual property from George Washington University Law School, a J.D. from Samford University's Cumberland School of Law, and a B.A. from Samford University.