Data Breach Notification Law: Policy Analysis Paper #2

Antonio Shields

School of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Prof. Lora Pitman

March 26, 2023

The intent of this paper will be the continued discussion of the Data Breach Notification Law. This discussion will focus on the political aspects of enacting the data breach notification law both domestically and internationally, including the United States' laws on data breach notifications both State and Federal, the General Data Protection Regulation (GDPR) in the European Union, and the Privacy Amendment Act of 2017 in Australia.

The data breach notification law is a section of data breach laws that according to Schuessler and Fulk (2017), "the United States has taken a decentralized or distributed approach by leaving it up to individual states to develop their own data breach laws." (p. 3). The data breach laws in every state vary in definition, scope, and notification parameters. California was the first state to enact data breach laws in 2002 and South Dakota was the last state to go into effect in 2018. The variations of state laws over that 16-year span have caused compliance issues when businesses have consumers in multiple states. When it comes to state and federal government authority, states would prefer to make their own respective laws and maintain state authority as opposed to giving authority over to the federal government. The federal government's interest in establishing a federal data breach notification law first came in 2005. A data security breach occurred at a large data broker, ChoicePoint, where they disclosed that they sold approximately 145,000 Social Security Numbers, addresses, and other personal data to business owner impersonators (Regan, 2009, p. 4). This breach caused members of Congress to push for federal legislation to be put in place, which immediately received pushback from 44 state attorney generals that collectively wrote a letter to Congress to express their concerns about making a federal data breach notification law (Schuessler & Fulk, 2017, p. 4). Members of Congress have since 2005 continued to propose bills for a federal data breach law, but remained at an impasse with some state officials due to unwillingness to concede authority, some fear the

federal law will be stricter than their respective state's current law, and some fear the federal law will be less strict than their respective state's current law. Until the issues between the federal government and state officials are resolved and the majority is able to come to a consensus, the United States will continue to have state-dependent data breach laws in place.

The European Union (EU), through an agreement between the European Parliament and the Council of the European Union, became the first to establish one unified data breach law for all the countries that are members of the EU and all EU citizens in 2015 (Garrison & Hamilton, 2019, p. 99). This data breach law is known as the General Data Protection Regulation (GDPR). It was introduced to unify all the provisions that the 28 member states were using at the time. The GDPR was introduced to replace directives that were set to expire (Garrison & Hamilton, 2019, p. 100). The EU, prior to the GDPR, was operating primarily using the 1995 Data Protection Directive 95/46/EC and because of the increase in data breaches and lack of enforcement, there was a need for new legislation (Garrison & Hamilton, 2019, p. 100). The GDPR gave more rights to the consumer to have control over how their respective information is used by any business. The Data Breach Notification Obligation (DBNO) is part of the GDPR and can be found in articles 2(2), 4(7), 4(12), 33, 4, and 3(4) of the GDPR (Nieuwesteeg, 2018, p.4). The GDPR went into effect in 2018 and is considered one of the stricter data breach laws in the world.

In Australia, the Privacy Amendment Act of 2017, which includes the Mandatory Data Breach Notification (MDBN) was enacted in 2017. Legislation attempts for The Privacy Amendment Act go back to 2013 when the Labour Government introduced the 2013 version of the bill, but it was not until public feedback was received that the final form of the bill was pass

by the Federal Parliament in 2017 (Alazab, Hong, & Ng, 2021, p. 6). The Privacy Amendment Act of 2017 did not go into effect until a year later in 2018.

The data breach laws both domestic and international vary from each other and continue to be amended based on needs and technological upgrades. The GDPR has shown that it is possible to have a unified law instead of individual states or countries creating and enforcing their own laws, but from a political standpoint, state officials are there to do what is best for their citizens and the ability to maintain control of over making those decisions is what the federal government and state officials have to sort out.

Works Cited

Alazab, M., Hong, S., & Ng, J. (2021). Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Future Generation Computer Systems, 116,* 22-29.

Garrison, C., & Hamilton, C. (2019). A comparative analysis of the EU GDPR to the US's breach notifications. *Information & Communications Technology Law, 28*(1), 99-114.

Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU Data Breach Notification Obligation. *Computer Law & Security Review*, *34*(6), 1232–1246. https://doi.org/10.1016/j.clsr.2018.05.026

Regan, P. (2009). Federal Security Breach Notifications: Politics and Approaches. *Berkeley Technology Law Journal, 24*(3), 1103-1132.

Schuessler, J. H., Nagy, D., Fulk, H. K., & Dearing, A. (2017). Data breach laws: Do they work? *Journal of Applied Security Research, 12*(4), 512–524. https://doi.org/10.1080/19361610.2017.1354275