EMERGING TRENDS IN INTERNATIONAL DATA BREACH LAW

Alexandria Bradshaw*

CITE AS: 1 GEO. L. TECH. REV. 143 (2016)

https://perma.cc/8CCF-VAL5

INTRODUCTION 143

THE DEFINITION OF COVERED INFORMATION IS NOT LIMITED TO FINANCIAL AND HEALTH DATA 144

THE DEFINITION OF "BREACH" IS NOT TIED TO PARTICULAR HARMS EXPECTED TO RESULT FROM THE BREACH 145

SHORTER PERIODS FOR NOTIFICATION TO AUTHORITIES AND AFFECTED INDIVIDUALS 146

INTRODUCTION

We've seen an unprecedented number of breaches in the United States in recent years, spanning both the public and private sectors. Despite how critical data privacy laws are to preventing breaches and sustaining internet health, the U.S. lacks a comprehensive consumer privacy law and national data breach standard, even though there is an emerging thrust of legislation in other nations unifying breach protections under one national privacy law. Instead, the U.S. has a patchwork of privacy laws that leave some personal information unprotected in surprising ways, and a general purpose consumer protection law enforced by the Federal Trade Commission ("FTC") that maps imperfectly onto privacy rights. Legislators have attempted to enact data breach laws; at least 11 bills were introduced in Congress in 2015. However, these bills were stalled largely by disagreement over the extent to which a federal law should preempt more privacy protective state data breach laws.

Nevertheless, other countries have enacted and are beginning to enforce data breach regulations that will have an effect on U.S. companies doing business abroad. Many of these laws are more stringent than similar provisions in U.S. federal laws with breach provisions, such as the Gramm-Leach-Bliley

* Privacy and cybersecurity advisor at Brunswick Group, a global corporate relations and crisis response firm. Prior to joining Brunswick, she was a lawyer at Center for Democracy & Technology, where she focused on commercial data privacy and security issues, including breach preparedness. She is a graduate of Boston College and Harvard Law School.

Act ("GLBA")[1] and Health Information Technology for Economic and Clinical Health Act ("HITECH").[2] The EU's General Data Protection Regulation ("GDPR")[3] and South Africa's Protection of Personal Information Act ("POPI")[4] are two examples. Below is an overview of three aspects of GDPR and POPI that may reflect emerging trends in international data breach law.

THE DEFINITION OF COVERED INFORMATION IS NOT LIMITED TO FINANCIAL AND HEALTH DATA

A major difference between international data breach standards and U.S. law is their applicability. U.S. privacy laws only apply to certain classes of information – GLBA addresses financial data, HITECH and the Health Insurance Portability and Accountability Act ("HIPAA")[5] govern health data, the Family Educational Rights and Privacy Act ("FERPA")[6] regulates maintenance of educational records, and the Children's Online Privacy Protection Act ("COPPA")[7] applies to children's data. FERPA and COPPA do not address data breach, and although GLBA and HITECH (a complementary law to HIPAA) include breach response standards, their protections are limited to financial and health data. Section 5 of the FTC Act gives the FTC power to address "unfair or deceptive" business practices, and has been used to impose penalties for poor data security practices leading to breaches of any type of data.[8] However, Section 5 does not give the FTC authority to put rules in place to prevent breaches or require businesses to notify anyone of a breach. In sum, U.S. federal law provides very few breach protections for information beyond financial or health data.

Both the GDPR and POPI will protect a more expansive group of information than existing U.S. federal laws in the event of a breach. The GDPR applies to "any information relating to an identified or identifiable

[1] 15 U.S.C. § 6801 *et seq* (2012).
[2] 42 U.S.C. § 17921 *et seq* (2009).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 (Apr. 27, 2016) [hereinafter "GDPR"].
[4] Protection of Personal Information Act 4 of 2013.
[5] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 42 U.S.C.).
[6] 20 U.S.C. § 1232(g) (2012).
[7] 15 U.S.C. § 6501 *et seq* (1998).
[8] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

natural person ('data subject')."[9] This includes a person's name, identification number, location data, online identifier or information on the "physical, physiological, genetic, mental, economic, cultural or social identity" of the person. Similarly, POPI's breach provisions apply to all "personal information,"[10] defined as any information related to an individual, including (but not limited to) demographic information and information on their marital, occupational, religious, health, or educational status. "Personal information" also includes the individual's opinions or someone else's opinions on the individual.

THE DEFINITION OF "BREACH" IS NOT TIED TO PARTICULAR HARMS EXPECTED TO RESULT FROM THE BREACH

U.S. laws that include data breach provisions generally only require notification to regulatory authorities or affected persons if the breach is expected to result in a particular type or level of harm. GLBA, for example, only requires notification when the incident is expected to result in "substantial harm." The law leaves it up to the regulated entity to determine whether the incident meets this threshold. HITECH requires notification when the breach "compromises the security or privacy" of the information and, similar to GLBA, leaves it up to the breached entity to determine whether the incident reaches this level. Even some state breach laws tie notification to demonstrated or expected harm;[11] many only require notification when the breach is expected to cause concrete harms such as fraud or identity theft.

In contrast, under POPI, any suspicion that personal information has been accessed or acquired by an unauthorized person must be reported to both the affected individual and the enforcing agency (the "Information Regulator") regardless of the harm the incident might cause. Likewise, the GDPR triggers notification to the member nation's supervisory authority when any personal data has been breached, whether or not the breach will cause harm. The GDPR does limit *consumer* notification slightly; it only requires notification to an individual when the breach is "likely to result in high risk to the rights and freedoms" of that person.[12] Given European views of privacy, this limitation is likely to be interpreted in a more privacy protective manner than U.S. law.

---

[9] GDPR, *supra* note 3, at art. 4(1).
[10] Protection of Personal Information Act 4 of 2013 § 5(a)(ii).
[11] *See e.g.*, Ark. Code § 4-110-101 *et seq*; Fla. Stat. § 501.171; Iowa Code §§ 715C.1-715C.2; La. Rev. Stat. § 51:3071 *et seq*.
[12] GDPR, *supra* note 3, at art, 33(1).

SHORTER PERIODS FOR NOTIFICATION TO AUTHORITIES AND AFFECTED INDIVIDUALS

POPI and the GDPR also require notification in a shorter timeframe than many U.S. laws. POPI requires breach notification to authorities and affected individuals "as soon as reasonably possible after discovery of the compromise" and the notification must be made in writing with sufficient information to allow the individual to take protective measures. The GDPR is similarly strict. Notice must be provided "without undue delay and, where feasible, not later than 72 hours after having become aware of it."[13] These standards are markedly shorter than HITECH, which requires notification "without unreasonable delay,"[14] but gives entities up to 60 days to notify stakeholders after a data breach is discovered. Moreover, although many U.S. state laws require notification "as soon as possible"[15] or "as expeditiously as practicable,"[16] state laws that put a time limit in place for notification often give breached organizations 45 or more days to notify.[17]

What do these trends mean for American companies? While the GDPR and POPI cannot determine data breach response standards for countries outside of their jurisdiction, they are certainly persuasive authority. The GDPR applies to every EU member state – most of which do business with and host offices for companies across the globe – and it asserts authority whenever companies handle EU citizens' data, regardless of whether the company is in the EU. Additionally, South Africa's legislative framework and its constitutional courts serve as a model for many nations. At least one expert credits South Africa's influence over international jurisprudence to it being "not American, thus rendering [its] reasoning more politically palatable to domestic audiences in an era of extraordinary U.S. military, political, economic, and cultural power."[18] Chances are these sentiments will only increase in the years to come. Data breach legislation will likely move swiftly ahead in other nations, whether or not the Trump Administration or next Congress decide to push for it at home. U.S. companies must prepare now to comply with these new standards if they expect to remain globally competitive.

---

[13] *Id.*
[14] 42 U.S.C. § 17932 (2009).
[15] Wyo. Stat. Ann. §40-12-501.
[16] Fla. Stat. § 501.171.
[17] *See e.g.*, Ohio Rev. Code Ann. § 1349.19 *et seq.*; Vt. Stat. Ann. tit. 9 §§ 2430, 2435; Wis. Stat. §134.98.
[18] Anne-Marie Slaughter, A Global Community of Courts, 44 Harv. Int'l L.J. 191, 198 (2003).