Public Knowledge

May 11, 2018

The Honorable Blaine Luetkemeyer
Chairman
House Financial Institutions Subcommittee
House Financial Services Committee
2230 Rayburn House Office Building
Washington, DC 20515

The Honorable Wm. Lacy Clay
Ranking Member
House Financial Institutions Subcommittee
House Financial Services Committee
2428 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Luetkemeyer and Ranking Member Clay:

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we write to commend the House Financial Institutions and Consumer Credit Subcommittee of the House Financial Services Committee for its focus on data security and breach notification and to offer our view on the Luetkemeyer/Maloney Data Acquisition and Technology Accountability and Security Act. Unfortunately, the bill falls short. We write to express our concerns and to offer our assistance in revising the legislation to meet consumers' needs and expectations.

Before we offer specific feedback on the bill, we make the following observations, which frame our feedback: It is no longer possible to participate in society without providing information to third parties that may, in and of itself be personal, or that, when combined with other data and analyzed, reveals intimate personal information. This is true even for individuals who choose to live their lives entirely offline. For example, even the most basic activities, like renting or buying a place to live, trigger credit checks, which generate digital records of personal information.

Since the Subcommittee held its hearing on "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime," the issue of access to personal information has grabbed headlines in unexpected ways, and consumers have been introduced to unanticipated dimensions of the problem. At the end of March, we learned that an app developer, Aleksandr Kogan, funneled personal information about at least 87 million Facebook users to Cambridge Analytica, a firm that purported to engage in "psychographics" to influence voters on behalf of the Trump campaign. Gallingly, as was Facebook's practice for all apps at that time, when users connected Kogan's app to their Facebook accounts, the app scooped up not only the users' personal information, but also their friends' information – without any notice to the friends or opportunity for the friends to consent.

Facebook/Cambridge Analytica underscores the importance of considering data security not only in terms of traditional data breaches, but also in terms of unauthorized access to private information more broadly. Consumers have a right to expect that third parties will provide adequate protection for their personal information given that the market does not allow consumers to avoid sharing personal information. Yet, the market does not adequately punish firms that fail to protect personal information. Against this backdrop, there can be no question that Congress must pass strong consumer protection legislation.

Scope of the Legislation

The Data Acquisition and Technology Accountability and Security Act is too narrow in its definition of personal information, in its definition of covered entity, and in the harms with which it concerns itself. For example, the definition of personal information includes biometric data only when those data are used in financial transactions. Given that it is impossible to change one's fingerprint, iris scan, or other biometric identifier once it has been compromised, it is imperative that biometric data be protected, regardless of the purpose for the data's collection. The language should also more explicitly cover email account usernames and passwords, because access to an email account is sometimes all that is required to reset the username and password on other accounts and, moreover, because the contents of an email account can be strikingly personal. Similarly, the definition of personal information should cover security questions coupled with their answers.

Moreover, Facebook/Cambridge Analytica taught us that other information, like social media "likes" and the contents of communications, may be useful for influencing an individual in the voting booth, as well as for more mundane marketing and advertising purposes, and these data, when aggregated, may, in fact, be personally identifiable. The definition of personal information, therefore, should be updated to address the panoply of personal information today and to anticipate tomorrow's harms.

We are also concerned that the bill carves out from the definition of personal information "information that is rendered unusable, unreadable, or indecipherable." As a threshold matter, it is unclear whether bill drafters here refer to anonymization or encryption. If the intent is to refer to anonymized data, it is imperative that the bill exempt only data that have been fully anonymized and that cannot be re-identified. Otherwise, the carve-out may render the bill meaningless. To the extent that the bill references encryption, we are concerned that the carve-out exempts data regardless of what encryption methods were used. If out-of-date or unreliable encryption methods were used, it may be trivial for data thieves to render the information usable, readable, or decipherable. Yet, under the legislation, a covered entity that uses an irresponsible encryption method would be off the hook.

The bill's definition of covered entity is also disappointingly narrow, covering federal agencies only for the purposes of requiring security safeguards and failing to cover state and local agencies at all – surely a permissible use of federal power under the Commerce Clause.

Because the bill's data breach notice requirements do not apply to federal agencies, federal agencies are only subject to the consumer notification requirements in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. This provides insufficient protection for consumers. First, the OMB Memorandum is policy guidance that, by its nature as guidance, is less legally-enforceable than statutory law and that can be rescinded or changed by subsequent administrations with relative ease, depriving consumers of the durability and predictability of statutory law. Moreover, the guidance itself provides less protection for consumers than the draft legislation would. Whereas the draft bill requires consumer notification of a data breach when "there is a reasonable risk that the breach

of data security has resulted in identity theft, fraud, or economic loss to any consumer,"[1] the OMB Memorandum defers to each federal agency to decide whether or not to notify consumers of a data breach.[2]

The legislation is similarly anemic when it comes to the harms the bill seeks to address. The bill is only concerned with "identity theft, fraud, or economic loss."[3] These are a fraction of the harms an individual could suffer as the result of a data breach or unauthorized access to personal information and may not, for some people, be the most serious harms. For example, an individual who has been the victim of domestic violence or abuse could suffer stalking or otherwise be re-victimized if her breached data ends up in the wrong hands. Individuals could also suffer reputational harm if personal emails or photographs are breached and posted online. And, as we learned in the Facebook/Cambridge Analytica saga, an individual whose information landed in Cambridge Analytica's hands may have had her political views targeted or manipulated, raising the specter of harms to democracy.

Security Safeguards

We appreciate the draft legislation's mandate that each covered entity develop, implement, and maintain data security safeguards and are particularly pleased with the administrative requirement in Section 3(b). However, we are concerned that the draft does not require data minimization. One effective way to diminish the harms of a data breach may be to reduce the amount of personal information covered entities maintain in the first place. When a covered entity maintains extraneous personal information, that information is unnecessarily at risk in the event of a breach.

Requirements

In addition to the concern noted above about federal agencies' exemption from the legislation's data notification requirements, the notification requirements themselves fall short of the protections consumers expect and deserve.

First, we are concerned that covered entities must only notify law enforcement agencies and consumer reporting agencies if the data breach "involves personal information relating to 5,000 or more customers."[4] This standard would mean that law enforcement and consumer protection agencies need not be notified of the vast majority of data breaches. For example, Massachusetts Assistant Attorney General Sara Cable testified at the hearing that less than one percent of data breaches in Massachusetts meet the 5,000-person threshold.[5] While it is likely appropriate to draw lines around what magnitude of data breach warrants limited federal law

[1] Data Acquisition and Technology Accountability and Security Act, 115th Cong. § 4(b)(2) (2018)

[2] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-17-12, MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: PREPARING FOR AND RESPONDING TO A BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 29 (2017).

[3] *E.g.* Data Acquisition and Technology Accountability and Security Act, 115th Cong. § 3(a)(1) (2018).

[4] Data Acquisition and Technology Accountability and Security Act § 4(b)(1).

[5] *Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime Before H. Comm. on Financial Services, Subcomm. on Financial Institutions and Consumer Credit*, 115th Cong. (2018) (statement of Sara Cable, Assistant Attorney General, Massachusetts).

enforcement resources, a line that excludes more than ninety-nine percent of data breaches (assuming Massachusetts is representative) is ineffective. To wit, if covered entities believe they will never have a data breach that meets the reporting threshold, the legislation may fail to achieve its intended purpose of encouraging entities to adopt better cybersecurity measures.

Second, we are concerned that law enforcement agencies and consumer reporting agencies must only be notified when "there is a reasonable risk that the breach of data security has resulted in or will result in" enumerated harms[6] and that consumers only need be notified of a data breach when "there is a reasonable risk that the breach of data security *has* resulted in" enumerated harms.[7] Since the days of Justice Brandeis, individual ownership and control of one's own personal information has been the basis for privacy law in the United States.[8] There is increasing consensus that this principle should endure in the digital age.[9] With this principle in mind, the harm occurs when personal information is acquired or accessed in a way that is unanticipated or unauthorized by the individual to whom the information pertains. As a result, individuals should be notified of a data breach upon discovery of the breach. Moreover, codifying the harm standard simply allows the entity that has already failed to sufficiently protect sensitive personal information to determine, in its sole discretion – when it has every financial incentive to keep a data breach secret – whether or not consumers have been or will be harmed and thus whether or not consumers should be informed of the breach.

At a minimum, the discrepancy between when agencies are informed of a breach (when "there is a reasonable risk that the breach . . . has resulted or will result in" harm) and when consumers must be informed (only when the breach has resulted in harm) is inapt. Consumers have a profound interest in knowing when there is a reasonable risk that a data breach will result in harm; consumers can only take steps to avoid the harms of a data breach if they are informed of that breach and the reasonable risk of harm before that harm occurs. And, the need for robust consumer notification requirements is made more acute because covered entities that have suffered a data breach have every financial incentive to conceal news of that breach for as long as possible.

Finally, § 4(b)(3)(D) permits substitute notification where the covered entity lacks sufficient contact information for the majority of affected consumers. This is in stark contrast to other data breach notification rules, like 42 U.S.C. 17932(e) and the OMB Memorandum, which require actual notice to the consumers for whom the breached entity has contact information and permit substitute notification only where the agency does not have sufficient contact information for a particular consumer. The Data Acquisition and Technology Accountability and Security Act should adopt this approach in order to ensure that the maximum number of consumers actually receive notice and the opportunity to protect themselves when their data has been breached.

---

[6] Data Acquisition and Technology Accountability and Security Act § 4(b)(1).

[7] *Id.* at § 4(b)(2) (emphasis added).

[8] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

[9] *E.g. Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary & the S. Comm. on Commerce, Sci., & Transp.*, 115th Cong. (2018) (Statement of Mark Zuckerberg, CEO, Facebook); *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce*, 115th Cong. (2018) (Statement of Mark Zuckerberg, CEO, Facebook); Scott McDonald, President & CEO, ARF, Townhall at ARF Townhall on Research Ethics Partnered with GreenBook (Apr. 26, 2018).

Enforcement

The enforcement provisions of the bill also fall short. First, it prevents state attorneys general from bringing an enforcement action against a financial institution. Given that state AGs are the experienced, front-line enforcers for consumers in their states and given that the bill is primarily concerned with financial harms – and thus likely to disproportionately apply to financial institutions, this is a massive carve-out that leaves consumers vulnerable.[10] The bill also exempts insurance providers.[11]

Moreover, the draft creates a safe harbor from both its data security requirements and its breach notification requirements for entities that comply with Section 501(b) of the Gramm-Leach-Bliley Act, Section 264(c) of the Health Insurance Portability and Accountability Act, or Sections 13402 and 13407 of the HITECH Act.[12] This is true even though neither Gramm-Leach-Bliley nor HIPAA contains statutory data breach notification requirements. While we appreciate the drafters' attempt to make the bill "backward compatible" with the existing sector-specific privacy laws that are the core of traditional American privacy law, this approach is not appropriate where existing sector-specific laws do not statutorily require agencies to promulgate regulations protecting privacy, requiring breach notification, and mandating data security that are at least as robust as the rules contemplated by the legislation.

In short, the enforcement provisions of the draft considerably limit the reach of an already too narrow bill and greatly diminish its utility to consumers.

Preemption

Finally, Section 6 of the draft legislation problematically preempts state laws that better protect consumers. While the federal government should set minimum standards of protection for all Americans, states have been in the vanguard of privacy protection and data breach notification laws and are much-needed "cops on the beat." Even if Congress were to dramatically expand the resources available to federal privacy agencies – a proposal not on the table in this legislation, which leaves enforcement to the FTC's Section 5 authority, or elsewhere – the federal government could not hope to provide adequate protection to consumers on its own. Rather, the states, as laboratories of democracy, should be empowered to innovate and provide greater privacy protections to their residents. Moreover, by preempting state laws, the proposed legislation would deprive residents of states with more protective data breach laws of protections they have come to expect and rely on.

Conclusion

We commend the House Financial Institutions and Consumer Credit Subcommittee of the House Financial Services Committee for its focus on data security and breach notification. However, the Data Acquisition and Technology Accountability and Security Act as currently drafted does not adequately meet Americans' data security protection needs and should not be

[10] Data Acquisition and Technology Accountability and Security Act §§ 5(b)(1), 5(b)(5).
[11] *Id*. at § 5(d).
[12] *Id*. at § 5(e).

approved by the Subcommittee without significant changes. We stand ready to assist bill sponsors and interested Members to improve this bill or to craft data breach legislation that truly protects consumers. If you have any questions or would like more information, please do not hesitate to reach out to me at abohm@publicknowledge.org.

Sincerely,

Allison S. Bohm

CC. Members of the Financial Institutions and Consumer Credit Subcommittee of the House Financial Services Committee