

Executive Summary of Written Testimony of Dr. David B. Thaw

Submitted to the U.S. House of Representatives

Committee on Energy and Commerce – Subcommittee on Commerce, Manufacturing, and Trade

July 18, 2013: Hearing on "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"

In this written testimony, I provide detailed information on two core issues relevant to my understanding of the Subcommittee's current agenda on data security:

- I. whether to address consumer security breach notification as an initial matter, separate from and before moving to address broader information security regulation of custodians of consumer data; and
- II. in the event a "risk of harm" threshold is adopted for consumer security breach notification, what burden of proof should be required to trigger notification requirements.

My recommendations are as follows:

1. that the Subcommittee consider consumer breach notification *concurrently with* comprehensive information security regulations; and
2. that if a risk-of-harm threshold is adopted for consumer breach notification, an *affirmative* presumption of notification be implemented.

The first recommendation is based on my research on the efficacy of breach notification and comprehensive information security regulation, which reveals that the *combination of both regimes is as much as four times more effective than is breach notification alone*. It also considers the risks of "definitional lock-in" whereby statutory or regulatory definitions may be adopted for one purpose (consumer breach notification) that are not well suited, or later easily adopted by entities, to other purposes such as comprehensive information security regulation.

The second recommendation is based on the risk that adopting a *negative* presumption for notification can disincentivize thorough information security investigations, which are one of the most important tools in protecting consumers against future data breaches and securing existing information systems.

Finally, I also offer a preliminary proposal for an alternate notification regime, as well as a general suggestion that a single consumer protection regulator should not have *sole* responsibility for all regulated entities, specifically including those operating critical infrastructure.

Written Testimony of

Dr. David B. Thaw

Visiting Assistant Professor of Law, University of Connecticut
Affiliated Fellow, Yale Law School Information Society Project

Submitted to the U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

July 18, 2013

Hearing on "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"

Members of the Subcommittee:

Thank you for the opportunity to testify before the Subcommittee on the important issues of data security and consumer protection. In this written testimony, I provide detailed information on two core issues relevant to my understanding of the Subcommittee's current agenda on data security:

- I. whether to address consumer security breach notification as an initial matter, separate from and before moving to address broader information security regulation of custodians of consumer data; and
- II. in the event a "risk of harm" threshold is adopted for consumer security breach notification, what burden of proof should be required to trigger notification requirements.

I. Addressing Breach Notification Separate from Comprehensive Information security Regulation

I understand the Subcommittee intends to address the issue of breach notification first and separate from the issue of comprehensive information security regulation. I caution against this approach for two reasons:

1. Comparative Efficacy: breach notification alone is *substantially less effective* at preventing reportable security breach incidents than is the combination of breach notification and comprehensive information security regulation; and

Written Testimony of Dr. David B. Thaw

2. Definitional Lock-In: adopting standards for breach notification in the absence of comprehensive information security regulation will create "definitional lock-in" for categories defined to serve the purpose of breach notification but not well suited for later adoption to broader, comprehensive information security regulation

Comparative Efficacy

My research into the efficacy of existing information security regulations,¹ specifically including the breach notification statutes present in most U.S. jurisdictions, compared the effectiveness of breach notification statutes and comprehensive information security regimes. I combined qualitative, semi-structured interviews of Chief Information Security Officers (CISO) at key U.S. organizations with quantitative analysis of data breach incidence from 2000 through 2010. The results first describe the effects of each regime at driving information security practices within organizations, based primarily on the CISO interviews.

Of particular note to the Subcommittee, the interviewees reported that a primary effect of breach notification laws was to focus intensive effort on encryption of portable devices and media containing personal information.² While effective at reducing the number of reportable breaches, some respondents reported that this resulted in focusing *too* much on only one area of security³ – effectively leaving other venues available for attack. These attacks affect not only potential compromise of personal information as defined in existing breach notification statutes, but also the ability of outside attackers to compromise the integrity of critical infrastructure systems.

Such attacks are not hypothetical – in 1983, for example, a hacker group compromised the security of Memorial Sloan-Kettering Cancer Center in New York and gained access that effectively would have allowed them to alter the radiation treatment protocols of patients.⁴ This compromise led to the addition in 1986 of a felony enhancement to the Computer Fraud and Abuse Act for damaging computer systems relating to medical care.⁵

As noted by the CISOs I interviewed from the healthcare sector, breach notification statutes forced them to focus increased resources on encryption – without receiving additional resources to maintain existing programs. The resultant reallocation of security budgets directed resources

¹ See generally David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. (forthcoming 2014), <http://ssrn.com/abstract=2241838>.

² *Id.* at 29-30, 61-64.

³ *Id.*

⁴ See S. Rep. 99-432 (1986), at *2-3, 12.

⁵ See *id.*, see also 18 U.S.C. §§ 1030(a)(5), (c)(4)(A)(i)(II).

Written Testimony of Dr. David B. Thaw

away from where those CISOs believed they were needed most.⁶ I describe this phenomenon as "Locking the Bank or Vault Door and Leaving the Back Window Open."⁷ The key takeaway for the Subcommittee on this point is that focusing *solely* on consumer breach notification may have detrimental effects to other, critical areas of information security.

My quantitative research also presents information of substantial import to the Subcommittee's work. By analyzing periodic breach incidence data from January 1, 2000 through December 31, 2010, I determined that the combination of consumer breach notification and comprehensive information security regulation was as much as four times more effective at preventing reportable breaches of consumers' personal information than was breach notification alone.⁸

Definitional Lock-In

Approaching the issue of breach notification separately will generate an effect I describe as "definitional lock-in" – key definitions in regulations will be determined at an early stage, based on limited scope of purpose not well-suited the broader purposes later envisioned. Specifically, key definitions such as the subject of information to be protected (often referred to as "Personal Information") will be defined for the purposes of consumer breach notification; purposes that are very different than those appropriate to comprehensive information security regulation. Lock-in occurs as a result of the substantial cost to organizations of later "re-classifying" information based on additional categories established by new regulation. This process, when applied to existing data,⁹ is often cost-prohibitive and may raise regulatory burdens too high for effective compliance, thus pressuring legislators and regulators to retain existing definitions.

To be specific, consider the example of the types of information that should be subject to protection. In the case of breach notification, this information is most commonly referred to as "personal information" or "personally identifiable information." These terms have widely varying definitions. At the state level, a least common denominator exists: the combinations of an identifying item, most commonly an individual's name, with one of three categories of more sensitive information:

- the individual's Social Security Number;
- the individual's financial account numbers, along with any identification code necessary to access the account; or

⁶ Thaw, *supra* note 1, at 63.

⁷ *Id.* at 61.

⁸ *Id.* at 58.

⁹ as differentiated from new data generated as technology advances

Written Testimony of Dr. David B. Thaw

- the individual's government-issued identification number (usually driver's license or state ID)

The stated purpose of most jurisdictions' breach notification statutes is to enable consumers to take steps to protect themselves by requiring custodians of this information to inform consumers when those custodians have lost control of this information.¹⁰ Yet many other types of information may pose a great harm to consumers. For example:

- medical records
- wills
- diaries
- private correspondence (including e-mail)
- financial records
- photographs of a sensitive or private nature; [and]
- similar information

are all categories of information federal criminal law considers sufficient to warrant substantial criminal sentence enhancements for individuals convicted of computer crimes involving identity theft.¹¹ The Department of Health and Human Services,¹² the Department of the Treasury,¹³ and the Federal Trade Commission¹⁴ each have offered additional definitions of information they consider to be "sensitive" to consumers. All of this information should be the subject of consumer protection. Additionally, consumers should be informed whenever this information is subject to unauthorized disclosure as is necessary to take steps to protect themselves.

These categories are hardly comprehensive of the types of information that need to be protected by comprehensive information security regulations. Corporate trade secrets, including sensitive data about products not yet available outside the United States, sensitive business development plans, information about critical infrastructure systems such as water, electric, or telecommunications grids, and information security plans are all sensitive information that are

¹⁰ See, e.g., CAL. BILL. ANALYSIS, S.B. 1386, Cal. Assembly, 2001-2002 Reg. Sess. (Aug. 23, 2002) (Senate Third Reading, analysis of Saskia Kim).

¹¹ See UNITED STATES SENTENCING GUIDELINES MANUAL § 2B1.1(b)(16), see also § 2B1.1 Application Notes.

¹² See 45 C.F.R. § 160.103, definition of "individually identifiable health information."

¹³ See 12 C.F.R. Part 30, App. B, § (I)(C)(2)(b) ("Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the bank for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual.")

¹⁴ See generally Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMM'N at 5, available at http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf (suggesting a broad definition of personal information that includes "other sensitive information").

Written Testimony of Dr. David B. Thaw

not the province of the general consumer. Yet a failure to secure this information may have costly effects, and not just to the organization experiencing the breach. If a business partner of a new pharmaceutical fails to properly secure their information systems, or the information technology services provider to a major financial institution or exchange fails to implement appropriate controls on administrative accounts, substantial negative effects to the broad economy may result if those systems are compromised. None of these eventualities necessarily involves consumer information, but each clearly demonstrates a public interest in collective security.

If a definition of information to be protected is developed based solely on consumer breach notification, the downstream information security implications will be costly. Either organizations must engage in expensive reclassification of information and redesign of their information security programs when new regulations are subsequently implemented, or large areas of information may be left vulnerable if the regulations fail to expand the definition of information to be protected. In either case, the cost of considering breach notification separate from comprehensive information security measures would be high.

In summary, on these bases – the decreased efficacy, misallocation of resources, and risks of definitional lock-in – I strongly urge the Subcommittee to address consumer breach notification and comprehensive information security concurrently.

II. Considerations if a "Risk-of-Harm" Threshold is Adopted for Breach Notification

When considering the issue of consumer breach notification, legislators and regulators frequently confront the issue of *when* to require notification. Among existing law, some jurisdictions require notification in all cases of loss-of-control (subject to the "encryption exception"¹⁵) whereas others adopt what is known as a "risk-of-harm" threshold. This Section of my testimony takes no position as to which approach is preferable – the empirical data on this result remains mixed. (In Section III, I introduce a preliminary proposal for an alternate regime.)

Rather, the focus of this Section addresses the *information security implications* of certain formulations of the risk-of-harm threshold. Specifically, I note to the committee that some formulations negatively impact information security procedures and outcomes.

¹⁵ To the best of my knowledge, no current U.S. jurisdiction, inclusive of (unclassified) federal regulations, *requires* notification to *consumers* in the event of loss of control of unencrypted and otherwise unsecured personal information subject to notification requirements under applicable law.

Written Testimony of Dr. David B. Thaw

Risk-of-harm thresholds may have many forms, but generally can be categorized according to the *affirmative* or *negative* presumption of notification. An *affirmative* presumption of notification requires a data custodian who experiences a breach to affirmatively demonstrate that the specified risk of harm threshold *is not satisfied* before they are exempted from consumer notification requirements. A *negative* presumption of notification *does not* require a data custodian who experiences a breach to notify consumers *unless* an investigation reveals that the specified risk of harm threshold has been satisfied.

A negative presumption of notification carries substantial, worrisome implications for information security procedures and outcomes. Specifically, this presumption disincentivizes organizations from conducting thorough security investigations.

Organizations have incentives to limit the scope and scale of investigations that may uncover information potentially exposing the organization to liability. For example, when conducting comprehensive information security assessments, auditing and consulting firms often work together with law firms so that the results of these assessments will be privileged as attorney-client work product and thus not subject to discovery in civil litigation or regulatory investigations. Clients of such firms often desire to learn about the risks they face, but do not want to incur liability for failure to remediate security vulnerabilities identified in the assessment. This problem is particularly compounded when faced with low-probability/high-risk vulnerabilities for which the cost of remediation is high. While generally protected by the business judgment rule, executives of publicly-traded organizations still bear a fiduciary duty to act in the best interests of their shareholders. A risk analysis might well reveal that the probability is sufficiently low not to justify the direct costs of remediation when combined with the cost of business disruption and other indirect cost. While I do not suggest that organizations engage in willful ignorance of their legal or regulatory obligations, my research data and professional experience support the conclusion that organizations can have substantial incentive not to pursue a comprehensive investigation if it might trigger additional regulatory compliance requirements.¹⁶ Conversely, if pursuing that investigation might alleviate the organization of regulatory compliance requirements (e.g., exempt the organization from consumer notification), my research and professional experience support the conclusion that organizations can have substantial incentive to thoroughly pursue that investigation.

Thus I strongly recommend that, if the Subcommittee considers use of a risk-of-harm threshold, that it adopt an *affirmative* presumption of notification. This will avoid disincentivizing thorough information security investigations, which are one of the most important tools in protecting consumers against future data breaches and securing existing information systems.

¹⁶ See generally Thaw, *supra* note 1.

Written Testimony of Dr. David B. Thaw

III. Preliminary Proposal for a Bifurcated Notification Regime

As noted in Section II above, for the reasons therein, I take no position as to whether a strict loss-of-control or a risk-of-harm threshold is preferable from an information security perspective. In this final Section, I briefly introduce an alternate notification regime I am currently developing. This proposal builds on similar regimes found in states such as New York,¹⁷ Massachusetts,¹⁸ and Virginia,¹⁹ each of which require notification to central state regulatory authorities in addition to notification to consumers in the event of a reportable data breach.

Under such a bifurcated notification regime, organizations experiencing a loss-of-control of any covered data would be required to report that incident to a centralized reporting authority, most likely a federal regulator such as the Federal Trade Commission. Consumer reporting would be triggered in certain cases deemed appropriate to where consumers can take steps to protect themselves and/or when consumers have an interest in awareness that their sensitive information was subject to unauthorized disclosure.

This bifurcated notification regime, if properly implemented, could achieve many of the goals of consumer breach notification while mitigating the risks of "over-notification" often raised by critics of strict loss-of-control regimes.²⁰ Specifically, consumers would receive appropriate notification, while all incidents would nonetheless be reported. Thorough information security investigations would be a requirement under this regime as part of the centralized reporting requirement. Additionally, the regulatory agency receiving the reports would have the ability to follow-up in cases where they suspect consumer notification should have occurred but did not, to follow-up if there is evidence a broader pattern of information security deficiencies may be present, or to follow-up and provide support if it believes the organization requires additional information security and/or law enforcement support.

I stress in my testimony that this proposal is *preliminary*, and I lay out the basic characteristics as guidelines. I encourage the Subcommittee to investigate this proposal – similar versions of which currently are in place in some U.S. jurisdictions, as noted above – to determine what benefits it may afford at the Federal level.

¹⁷ See generally N.Y. GEN. BUS. LAW § 899-aa.

¹⁸ See generally MASS. GEN. LAWS ch. 93H-1 et seq.

¹⁹ See generally VA. CODE ANN. § 18.2-186.6.

²⁰ This is not to suggest I believe over-notification currently is or is not a problem. Rather, I only suggest that if over-notification is of concern to the Subcommittee, a bifurcated notification regime can address such concerns.

Written Testimony of Dr. David B. Thaw

IV. Comments Regarding the Issue of a Unified Regulatory Regime for Information Security

Although I do not understand the Subcommittee's core agenda for this Hearing to include the question of whether information security provisions should be unified under a central regulator, this question is inextricably intertwined into the issue of breach notification.

Information security, also known as "cybersecurity,"²¹ is a layered exercise. I recently discussed this phenomenon in greater detail,²² describing that its challenge is the protection or regulation of four different categories of information systems:

- military and defense operations
- non-military government information systems
- private sector critical infrastructure, and
- non-critical private sector information systems

The competencies required to address threats faced within each of these categories differ in several ways. Military and defense operations, for example, must adopt a more stringent "risk prevention" approach, which they also are better suited to achieve because of the command-hierarchy backed by the threat of criminal punishment inherent in the military.

Private companies operating non-critical information systems, by contrast, have a fiduciary duty to their shareholders to apply the most efficient level of protection – which may differ widely from the "strongest" level of protection. They also lack the ability to enforce as rigid a hierarchy as the military.

Private companies operating critical infrastructure, such as utilities, telecommunications, financial systems, and healthcare systems, bear many of the same characteristics of other private

²¹ As noted by Professor Andrea Matwyshyn, "referring to all of information security, particularly in private sector contexts, as 'cybersecurity' is technically incorrect." Matwyshyn describes this misnomer as ignoring the aspects of physical security inherent in "holistic" protection of data maintained by an enterprise. I concur with this assessment, and further suggest, as consistent with the Administrative/Technical/Physical breakdown described in Part II, Section B of Thaw, *supra* note 1, that such a characterization also overlooks the administrative aspects involved in protecting and security information. See Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, NW. L. REV. at 36, n. 105 (forthcoming 2013) (cited with permission of author); see also David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 101, 122, 137 (2013), <http://ssrn.com/abstract=2226176> (discussing the distinction between purely-technical restrictions on computer usage and comprehensive administrative, technical, and physical restrictions thereon).

²² See David Thaw, *A Flexible Approach to Cybersecurity Regulation*, REG BLOG (July 9, 2013), <https://www.law.upenn.edu/blogs/regblog/2013/07/09-thaw-cybersecurity.html>.

Written Testimony of Dr. David B. Thaw

organizations, but they possess a heightened protection obligation stemming from the substantial negative externalities if their systems fail or are compromised.

This categorization suggests two conclusions the Subcommittee may wish to consider should the subject of single vs. multiple federal regulators arise in its work:

1. Even within industrial sectors, organizations are often substantially heterogeneous with respect to their information security competencies and vulnerabilities. Thus flexibility within regulation, which may be accomplished by delegation of certain rulemaking authority to administrative agencies, is essential.
2. Entities at "higher" tiers of criticality should not be regulated *solely* by regulators at lower tiers. For example, a critical infrastructure provider should not be regulated *solely* by the Federal Trade Commission, whose core competency is protecting consumer information, and must *at least* be regulated by the Federal Communications Commission, whose core competency is understanding the heightened protection obligations that may face providers of critical infrastructure.

Conclusion

In closing, I wish to reiterate my primary recommendations to the Subcommittee:

1. that the Subcommittee consider consumer breach notification *concurrently with* comprehensive information security regulations; and
2. that if a risk-of-harm threshold is adopted for consumer breach notification, an *affirmative* presumption of notification be implemented.

I again thank the Chairman, the Ranking Member, and the Members of the Subcommittee for the opportunity to testify on this important issue. I would be pleased to provide any follow-up information the Subcommittee may find helpful as it proceeds with its work on this topic.

Respectfully submitted,

David B. Thaw, J.D., Ph.D.

Visiting Assistant Professor of Law, University of Connecticut
Affiliated Fellow, Information Society Project, Yale Law School