Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 27 | Issue 1 Article 3

2010

Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws

Mark Burdon

CONTEXTUALIZING THE TENSIONS AND WEAKNESSES OF INFORMATION PRIVACY AND DATA BREACH NOTIFICATION LAWS

Mark Burdon†

Abstract

Data breach notification laws have detailed numerous failures relating to the protection of personal information that have blighted both corporate and governmental institutions. There are obvious parallels between data breach notification and information privacy law as they both involve the protection of personal information. However, a closer examination of both laws reveals conceptual differences that give rise to vertical tensions between each law and shared horizontal weaknesses within both laws. Tensions emanate from conflicting approaches to the implementation of information privacy law that results in different regimes and the implementation of different types of protections. Shared weaknesses arise from an overt focus on specified types of personal information which results in 'one size fits all' legal remedies. The author contends that a greater contextual approach which promotes the importance of social context is required and highlights the effect that contextualization could have on both laws.

I. INTRODUCTION

Data breach notification laws appear to have been a successful addition to legal frameworks relating to the protection of personal information. For example, as a result of these laws, numerous information security failings have been reported that have affected both corporate and governmental institutions.[1] They have uncovered a major social problem that has the capacity to affect millions of

† PhD Candidate/Research Associate, Faculty of Law/Information Security Institute, Queensland University of Technology. The author gratefully acknowledges funding from Australian Research Council Grant DP0879015 'A new legal framework for identifying and reporting Australian data breaches.'

1. *See, e.g.*, Open Security Foundation, *Periodic PDF Reports*, http://datalossdb.org/reports †last visited Sept. 10, 2010) (detailing the numerous data breaches that have been notified since the inception of US state-based notification laws).

citizens.[2] They have highlighted that general levels of corporate information security practices are inadequate. It is not surprising that these apparent successes have been instrumental in the proliferation of data breach notification laws throughout the United States (US) and beyond. Only a handful of US state legislatures have not yet enacted a data breach notification law[3] and it is possible that a federal law will be implemented this year.[4] Other jurisdictions have also followed suit, including the European Union (EU),[5] and comprehensive proposals have been put forward in a number of other jurisdictions including Australia, [6] Canada, [7] New Zealand[8] and the

---

2. *See, e.g.*, Privacy Rights Clearinghouse, *Chronology of Data Breaches*, http://www.privacyrights.org/data-breach#2 (last visited Sept. 10, 2010) (suggesting that hundreds of millions of US citizens may have been affected by a data breach).

3. Currently, only four states do not have a data breach notification law: Alabama, Kentucky, New Mexico and South Dakota. *See* National Conference of State Legislatures, State Security Breach Notification Laws, Apr. 12, 2010, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last visited October 6, 2010).

4. The Data Accountability and Trust Act of 2009, H.R. 2221, 111th Cong. (2009) is the first bill to have passed a vote from one of the Houses of Congress. *See* David Navetta, *House Passes Data Accountability and Trust Act (DATA)*, INFORMATION LAW GROUP, Dec. 10, 2009, http://www.infolawgroup.com/2009/12/articles/data-privacy-law-or-regulation/house-passes-data-accountability-and-trust-act-data/. It should also be noted that the Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009) has also been referred from the Senate Judiciary Committee to a full vote on the Senate floor. *See* Jaikumar Vijayan, *Federal Data-protection Law Inches Forward*, COMPUTERWORLD, Nov. 5, 2009, http://www.computerworld.com/s/article/9140408/Federal_data_protection_law_inches_forward.

5. *See* Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC), Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (2009) [hereinafter e-Privacy Directive]. *See also* Mark Burdon, et al., *The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments*, 26 COMPUTER L. & SECURITY REV. 115, 120-23 (2010) (regarding an overview of the notification provisions of the new Directive) [hereinafter Burdon et al., *Mandatory Notification of Data Breaches*].

6. *See* AUSTRALIAN LAW REFORM COMMISSION, FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE (2008) [hereinafter AUSTRALIAN PRIVACY LAW AND PRACTICE] (regarding the Australian Law Reform Commission's proposal for an Australian data breach notification scheme).

7. *See* Stikeman Elliot, *Bill C-29 proposes to enhance current private-sector privacy legislation*, Aug. 13, 2010, http://www.canadiantechnologyiplaw.com/2010/08/articles/privacy/bill-c29-proposes-to-enhance-current-privatesector-privacy-legislation/ (regarding a recent bill put before the Canadian House of Commons to implement a data breach notification scheme via the Personal

United Kingdom (UK).[9]

At face value, there are apparent similarities between data breach notification laws and information privacy laws as they both involve legal obligations relating to the protection of personal information.[10] Both laws seek to foster better security practices and have an information dissemination role that provides an individual with greater knowledge about how his or her information is stored and used. However, the development of data breach notification laws relates to a fundamental difference within information privacy legal regimes that is typically highlighted by distinctions between the sectoral approach to information privacy adopted by the US and the comprehensive approach to data protection adopted by the EU and other countries.[11] These distinctions manifest in different ways and this article identifies vertical tensions between both laws and shared horizontal weaknesses within both laws.

Data breach notification laws were developed in the absence of a comprehensive data protection framework as a specific law for a particular problem,[12] whereas they are now being implemented within

---

Information Protection and Electronic Documents Act 2000 (Can)). *See also* Industry Canada, *Government of Canada Moves to Enhance Safety and Security in the Online Marketplace*, MARKETWIRE, May 25, 2010, http://www.marketwire.com/press-release/Government-of-Canada-Moves-to-Enhance-Safety-and-Security-in-the-Online-Marketplace-1265966.htm (regarding an overview of the proposed amendments); CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, APPROACHES TO SECURITY BREACH NOTIFICATION: A WHITE PAPER, 36 (2007) (regarding a review of data breach notification in Canada).

8. *See* LAW COMMISSION OF NEW ZEALAND, REVIEW OF THE PRIVACY ACT 1993: ISSUES PAPER 17 (2010) (regarding a recent review of the New Zealand Privacy Act and the possible introduction of a data breach notification scheme).

9. The United Kingdom has taken a different track to data breach notification compared to other countries. A formal data breach notification scheme has been rejected by the Information Commissioner as notification of problems to the Commissioner was deemed to be a matter of existing good practice. *See* The News, *The UK Does Not Need a Data Breach Notification Law, Says Government*, OUT-LAW NEWS, Nov. 25, 2008, http://www.out-law.com/page-9619. However, the Commissioner has been granted extra powers to award penalties of £STG500,000 against organizations in breach of the Data Protection Act 1998 (UK), which includes data breaches. *See* Dan Raywood, *Half a Million Pound Penalty Introduced for Personal Data Security Breaches by the Information Commissioner's Office*, SC MAGAZINE, Jan. 13, 2010, http://www.scmagazineuk.com/half-a-million-pound-penalty-introduced-for-personal-data-security-breaches-by-the-information-commissioners-office/article/161159/ (providing an overview of the introduction of the fine).

10. *See, e.g.*, Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1106 (2009) (regarding data breach notification as a concern of sectoral information privacy law in the US).

11. It should be noted that the concepts of information privacy and data protection are used interchangeably in this article although the author acknowledges differences between them.

12. *See* Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467, 471 (2010) (explaining

the generic rights-based frameworks founded on comprehensive approaches to data protection or information privacy.[13] Data breach notification laws consequently not only attempt to fulfill a specific purpose, the mitigation of identity theft, but also have expansive conceptual aims originating from the conflicting goals of consumer protection and corporate compliance cost minimization. Comprehensive information privacy legal frameworks, on the other hand, have an expansive purpose, namely, to ensure legal protections related to the protection of personal information. Information privacy laws set minimum standards that relate to fair information practices and provide individuals with a series of limited rights of involvement in the process of personal information exchange.[14] The different developmental rationales behind encryption safe harbors for data breach notification demonstrate differences in the types of regulatory responses adopted by both laws. Data breach notification laws adopt market-based initiatives that are cognizant of corporate compliance cost burdens, whereas comprehensive information privacy laws adopt rights-based protections that favor individual interests over corporate requirements.[15]

Combined with vertical tensions, there are also shared horizontal weaknesses because both laws are predicated on overt information-based foundations.[16] Both laws focus too much on the type of information regulated rather than the social contexts and relationships that are involved in the personal information generation and exchange processes. Regulatory responses are formed upon the creation of chains of accountability and "one size fits all" remedies. These chains are founded upon binary relationships involving three parties: a personal information provider, a personal information collector, and a personal information re-user.[17] Problems occur in the application of

---

California enacted the country's first data breach notification law on July 1, 2003).

13. *Id.* at 473 (explaining that other states use similar frameworks but alter them). *See generally* Burdon et al., *supra* note 5 (regarding the implementation of data breach notification in the comprehensive frameworks of the EU and Australia).

14. *See* Privacy Rights Clearinghouse, Why Privacy, http://www.privacy rights.org/why-privacy (last visited Sept. 10, 2010).

15. *See, e.g.*, Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 280-281 (2009) (regarding the distinction between data protection and data security perspectives and different emphases at the heart of data breach notification laws).

16. *See* discussion at Part IV.C.

17. Mark Burdon, *Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws*, 2010 U. ILL. J.L. TECH. & POL'Y 101, 32 (2010) [hereinafter Burdon, *First Generation Laws*].

both laws because the social process of information exchange can now involve more parties than envisaged by one-dimensional and largely static chains of accountability. Data breaches themselves provide illumination on this point as they typically involve the insertion of a third party auxiliary to the accountability framework created by both laws, as demonstrated by an overview of three illustrative data breaches.

Part II of this article provides a brief overview of the conceptual foundations and development of both information privacy and data breach notification law. Part III examines the conflicting vertical tensions and Part IV identifies the shared horizontal weaknesses of both laws. The purpose of this examination is to demonstrate underlying conceptual weaknesses of data breach notification and information privacy laws that are founded on an insufficient regard for the crucial role of social context and social relationships as the foundation of information exchange processes. Part V introduces notions of contextualization that promote legal attention towards social relationships rather than specific types of information, which in turn, suggest a different approach to the conceptualization and application of both laws.

II. CONCEPTUAL FOUNDATIONS & LEGISLATIVE DEVELOPMENT

Later sections of this article will examine the conflicting tensions and shared weaknesses of both laws. Before that analysis can take place, however, it is necessary to briefly overview the conceptual foundations and legislative development of information privacy and data breach notification laws.

A. Information Privacy Law

The legal concept of information privacy is generally considered a sub-set of the many and multi-faceted theories of privacy that has been generated through the kaleidoscopic lens of different authors and different academic disciplines.[18] Attempts to answer the question "What is privacy?" in a meaningfully legal sense have generated literature that is immense in its intellectual breadth, intense in its scholarly conviction, and ingenious in its development of analytical

18. *See* Philip Leith, *The Socio-Legal Context of Privacy*, 2 INT'L. J.L. CONTEXT 105, 108 (2006) (regarding the socio-legal implications of privacy and the limits of information privacy); Herman T. Tavani, *Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy*, 38 METAPHILOSOPHY 1, 2, 3-9 (2007) (reviewing the basis of different theories of privacy).

frameworks. An answer to the question sought has not been forthcoming, thus leading to a degree of despair about whether such an answer can ever be found.[19] Conversely, attempts to answer the question "What is information privacy?" are much more coherent from a conceptual sense to the extent that information privacy laws have been implemented in many different legal jurisdictions.[20]

> The concept of information privacy is generally associated with control theories of privacy that relate to an individual's choice regarding the disclosure of his or her personal information.[21] One of the first and most influential representations of the control theory is Westin's "Privacy and Freedom."[22] Westin did not use either the term "right" or "control" or even "information privacy" in his description of an individual's required claim for information privacy,[23] but his work has nonetheless been perceived as addressing information privacy that provides individual rights of control over personal information.[24] In Privacy and Freedom,

---

19. *See generally* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1-2 (Harvard University Press. 2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY] (providing an overview of commentaries). *See also* William M. Beaney, *The Right to Privacy and American Law*, 31 LAW & CONTEMP. PROBS. 253, 255 (1966) (doubting whether it is possible to define a "right to privacy"); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) (commenting that the notion of privacy is so complex that it cannot be usefully conceptualized because it is so entangled with competing and contradictory dimensions); Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 310 (1975) (contending that ideas about the right of privacy are so overlapped by other rights that it is indeterminable).

20. COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE, 8 (MIT Press 2nd and updated ed. 2006) [hereinafter BENNETT & RAAB, GOVERNANCE OF PRIVACY] (regarding the policy goals of different jurisdictions "to give individuals greater control of the information that is collected, stored, processed, and disseminated about them" by organizations).

21. *See* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 14 (1992) (regarding the analogous links between "data protection" and Westin's information privacy); Tavani, *supra* note 18, at 7 (regarding an overview of key authors and theoretical applications); *See, e.g.*, Lisa Austin, *Privacy and the Question of Technology*, 22 L. & PHIL. 119, 125 (2003) (stating that individual control of personal information has been a key tenet of information privacy laws and has been a significant driver of conceptual development).

22. ALAN F. WESTIN, PRIVACY AND FREEDOM (Atheneum 1970) (1967).

23. *But see id.* at 42 (regarding Westin's "right of individual privacy" which is defined as "the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public").

24. *See, e.g.*, JAMES B. RULE, PRIVACY IN PERIL 22-23 (2007) (regarding the influence of Westin's work and the need to regulate organizational data systems in the late 1960s and early 1970s); RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 14 (1993) (noting the influence of *Privacy and Freedom* in relation to privacy as control definitions of privacy); JAMES WALDO ET AL., NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 59-60 (2007) (highlighting Westin's role in the development of the concept of information privacy).

> Westin determined four basic states of individual privacy: solitude, intimacy, anonymity, and reserve.[25] The latter state, reserve, is of the most interest regarding information privacy as it requires the creation of a psychological barrier against unwanted intrusion; this occurs when the individual's need to limit communication about himself is protected by the willing discretion of those surrounding him.[26]

The need for barriers is necessary as communication of the self is always incomplete. The requirements of societal involvement mean individuals are required to retain some information about them which is too personal for other persons or organizations to possess.[27] This mental distance, the space generated by choosing not to declare everything about one's self, requires an individual to have the ability and control to withhold or to disclose personal information. The ability of choice over our own information is consequently the "dynamic aspect of privacy in daily interpersonal relations."[28]

Westin also adduced four specific functions of privacy that reflect the value or purpose of privacy within society.[29] They are: *personal autonomy, emotional release, self-evaluation,* and *limited and protected communication.*[30] Again, the latter function is of relevance and it has two facets. The first, limited communication, sets interpersonal boundaries for the exchange of personal information. The second, protected communication, "provides for sharing personal information with trusted others."[31] It is the state of reserve in conjunction with limited and protected communication that is inherent in Westin's definition of information privacy: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [32]

Information privacy law is consequently based on the notion that individuals have rights relating to control over their personal information,[33] or at least, have rights pertaining to who can access

---

25. WESTIN, *supra* note 22, at 31-32.

26. *Id.* at 32.

27. *Id.*

28. *Id.*

29. *Id.*

30. *Id.*

31. *See* Stephen Margulis, T., *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, 59 J. SOC. ISSUES 411, 413 (2003).

32. WESTIN, *supra* note 22, at 7.

33. *See, e.g.*, Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (stating that privacy regards "the control we have over information about ourselves"); Arthur R Miller, *Personal*

their personal information[34] or a combination of both.[35] However, the "privacy as control paradigm"[36] is not without its critics. Schwartz highlights that while the control model has benefits because it seeks "to place the individual at the centre of decision-making about personal information use,"[37] it nonetheless suffers from several major flaws because it pays little consideration to information asymmetries,[38] and it is founded on the idea that personal information can mistakenly be construed as property.[39] Regan also states that

---

Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, 67 MICH. L. REV. 1091, 1107 (1968) ("the basic attribute of an effective right to privacy is the individual's ability to control the flow of information concerning or describing him"); Randall P Bezanson, *The Right to Privacy Revisited: Privacy, News and Social Change, 1890-1990*, 80 CAL. L. REV. 1133, 1135 (1992) (advancing a "concept of privacy based on the individual's control of information"); JERRY KANG, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1203 (1998) (referring to an individual's control over the processing of personal information); PRISCILLA M. REGAN, LEGISLATING PIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY, 9 (University of North Carolina Press 1995) [hereinafter REGAN, LEGISLATING PRIVACY] (commenting that privacy, in regard to US governmental collection of personal data, was defined as the "right of individuals to exercise some control over the use of information about themselves").

34. *See, e.g.*, Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980) (contending that privacy is a concern of accessibility that includes physical access by and the attention of other individuals); RULE, *supra* note 24, at 3 ("Let me define privacy as the exercise of an authentic option to withhold information on one's self"); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1110 (2002) (stating that information privacy as the right to "control-over-information can be viewed as a subset of the limited access conception"); David Archard, *The Value of Privacy*, *in* PRIVACY AND THE CRIMINAL LAW 16 (Erik Claes, et al. eds., 2006) (stating that the concept of limited access to a specified personal domain is the most plausible notion of privacy).

35. *See, e.g.*, James H. Moor, *Towards a Theory of Privacy in the Information Age*, 27 COMP. & SOC. 27, 31 (outlining the restricted access/limited control approach to privacy).

36. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000).

37. *Id.*

38. *Id.* at 830 (regarding privacy as control as the "commodification illusion").

39. The notion of personal information as property has been a controversial aspect of the information privacy law literature. *See, e.g.*, WESTIN, *supra* note 22, at 324-25 (introducing the notion that personal information can be classed as property). *See also* Lawrence Lessig, *Privacy as Property*, 69 SOC. RES. 261 (2002) (comparing privacy protection to intellectual property protection and the propertization of privacy "to allow individuals to differently value their privacy"); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383 (1996) (outlining an economic theory of personal information as property). *Contra* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1390 (2000) ("Juxtaposing the data privacy debate with the politics of intellectual property thus exposes an ideological fault line within the transaction costs approach to designating property interests"); Corien Prins, *Property and Privacy: European Perspectives and the Commodification of our Identity*, *in* THE FUTURE OF THE PUBLIC DOMAIN 249 (Lucie M. C. R. Guibault & P. B. Hugenholtz eds., 2006) (regarding the difficulties in assigning value to personal information); Sonia Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222, 242 (2004) (stating a weakness of the propertization of privacy concept is that it is grounded in notions of real property which do not extend to cyberspace).

Westin's work is too individualistic, which leads to the conclusion that Westin regarded "privacy as fundamentally at odds with social interests"[40] when that is clearly not the case.[41] Moreover, criticism is leveled at privacy as control from the seemingly tautological perspective that privacy as control is either too broad or too narrow.[42]

The conceptual reach of privacy as control has also been subject to criticism particularly regarding issues of individual consent. Allen contends there is a fundamental disconnect between what can be considered as having control over personal information and the requirements of a sufficient state of privacy because the former is not necessarily a constituent element of the latter.[43] Instead, privacy as control directs attention to issues of consent and choice about uses of personal information that connote an element of inaccessibility separate from privacy considerations.[44] Finally, the control aspect of information privacy has also been subject to criticism.[45] Simitis contends that privacy considerations no longer arise out of individual problems, but instead express conflicts that affect everyone.[46] Information privacy is thus not simply a problem of individual control over information.[47]

Despite these trenchant criticisms, the concept of privacy as control was the basis for information privacy legislation[48] and the

40. REGAN, LEGISLATING PIVACY, *supra* note 33, at 28. *See also* BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 50 (contending that Westin undertook a functional view regarding his investigation of privacy for an individual); Margulis, *supra* note 31, at 413 (stating that Westin's work takes an individualistic perspective about the societal role of information privacy).

41. REGAN, LEGISLATING PIVACY, *supra* note 33, at 220 ("I argue that privacy's importance does not stop with the individual and that recognition of the social importance of privacy will clear a path for more serious policy discourse about privacy and for the formulation of more effective public policy to protect privacy").

42. *See* Solove, *supra* note 34, at 1115 (contending that privacy as control is too vague due to the failure to define the types of information that individuals should control whilst other theories overcompensate and becoming too limiting).

43. *See* Anita L Allen, *Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 867-68 (2000) (regarding the differences between physical and informational privacy).

44. *Id.* at 869 (stating that informational privacy involves information in a state of inaccessibility).

45. *See* Austin, *supra* note 21, at 125-26.

46. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. Pa. L. Rev. 707, 709 (1987).

47. *Id.*

48. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 8 (commenting that the policy problem of "privacy" settled on the concept of information privacy).

development of what we recognize as "data protection"[49] or "information privacy"[50] or even "privacy"[51] laws. Three legal instruments developed in the 1970s and 1980s have been integral to the development of information privacy law as we know it today.[52] In Europe, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data by Council of Europe[53] was a cornerstone for the European Union's subsequent Data Protection Directive.[54] In the US, an influential report produced by the US Department of Health, Education, and Welfare[55] led to the implementation of the Privacy Act of 1974 and the Code of Fair Information Practice for Federal Government Agencies.[56] Finally, The Organization for Economic Cooperation and Development's (OECD) developed guidelines[57] for member countries relating to the transfer of personal information between member states which is a significant driver regarding the formulation of member state national legislation.[58]

The originating legal instruments and subsequent laws have many common features.[59] They are imbued on a principle of fairness

---

49. *See, e.g.*, Council Directive 95/46/EC, 1995 O.J. (L281) 31 (EU) [hereinafter Council Directive 95/46]; Data Protection Act, 1998, c. 29 (UK).

50. *See, e.g.*, Information Privacy Act, 2000 (Vict. Acts); Information Privacy Act, 2009 (Queensl. Stat.).

51. *See, e.g.*, Privacy Act, 1988 (Austl.); 5 U.S.C. § 552a (1974).

52. RULE, *supra* note 24, at 25, 29 (regarding the effect of the three instruments on the overall development of information privacy law); BENNETT *supra* note 21, at 95-101 (regarding the development of fair information principles through different international legal instruments).

53. Eur. *Consult. Assoc.*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data *(1981)*, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

54. Council Directive 95/46.

55. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm [hereinafter HEW REPORT].

56. *See* DANIEL J. SOLOVE, ET AL., INFORMATION PRIVACY LAW (2d ed. 2006) (citing HEW REPORT at 23–30, 41–42).

57. ORG. FOR ECON. CO-OPERATION AND DEV. [OECD], GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html.

58. *See* Michael Kirby, *Twenty-five Years of Evolving Information Privacy Law--Where Have We Come From and Where Are We Going?*, 21 PROMETHEUS 467 (2003) (regarding implementation of the Guidelines in Australia and New Zealand); LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 32 (Kluwer Law International 2002) (noting that the treaty has been ratified by twenty-seven member states).

59. *See* BYGRAVE, *supra* note 58, at 32; REBECCA A. GRANT & COLIN J. BENNETT,

and they adopt organizational-oriented controls relating to the process of personal information processing.[60] A series of "fair information practices"[61] or "information privacy principles"[62] stipulate minimum standards regarding the collection, storage, and use of personal information by data collecting organizations have thus emerged to regulate the process of personal information exchange.[63] While the genesis of information privacy laws can be traced back to these three roots causing subsequent laws to share similar features, a fundamental divergence has occurred. This divergence has caused the US to adopt the sectoral approach and the EU and non-EU states of the OECD to adopt the comprehensive approach, as outlined in Part III.A.

B. Data Breach Notification Law

Although forms of mandatory data breach notification existed prior to the development of US state-based laws,[64] the inception of these laws are normally associated with US state-based legislatures, particularly the California data breach notification law that was enacted in 2003.[65] That law requires any California business to notify California residents an existing or potential data breach that includes an unauthorized acquisition of unencrypted and computerized personal information,.[66] Individuals are to be notified within a

---

VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 6 (University of Toronto Press 1999).

60. *See, e.g.*, RULE, *supra* note 24, at 27 ("the workings of personal data systems [are] open, accountable, and subject to known rules of due process"). *See also* Viktor Mayer-Schonberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 221 (Philip Agre & Marc Rotenberg eds., 1997) (describing the European advances in data storage and protection).

61. *See, e.g.*, Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 195-202 (Philip Agre & Marc Rotenberg eds., 1997) (regarding the development of fair information practices arising out of the HEW Report and subsequent implementation through the Privacy Act of 1974).

62. *See, e.g.*, GRAHAM GREENLEAF, ET AL., STRENGTHENING UNIFORM PRIVACY PRINCIPLES: AN ANALYSIS OF THE ALRC'S PROPOSED PRINCIPLES, *available at* http://www.bakercyberlawcentre.org/ipp/publications/papers/ALRC_DP72_UPPs_final.pdf (regarding the application of Australia's privacy principles).

63. *See, e.g.*, BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 12 (outlining the impact of fair information practices on the jurisdictional development of information privacy law).

64. *See, e.g.*, Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457, 465 (2004) (regarding security breach notification under the EU's e-Privacy Directive which came into force in 2002).

65. CAL. CIV. CODE § 1798.29 (West 2003).

66. *Id.*

timeframe that is expedient and without reasonable delay.[67] Notification can take different forms including by letter, electronic notification, or substitute notice[68] which entails "conspicuous posting"[69] on the organization's website or via state media sources. However, some data breaches are exempt from notification. These include "good faith acquisitions"[70] of personal information by an employee or agent of the breached entity[71] and encrypted personal information.[72] The type of personal information required to be notified also provides a limiting factor. Unlike information privacy laws, data breach notification laws have specific requirements as to what constitutes information to be regulated.[73]

The purpose of the California law and most other subsequent data breach notification laws is directly linked to the mitigation of identity theft.[74] The law was introduced to the California legislature

---

67. However, law enforcement agencies can request a delay if notification would impede a criminal investigation. *See* CAL. CIV. CODE § 1798.29 (West 2003). Time frames also vary between different states. *See, e.g.*, FLA. STAT. § 817.5681 (2005) (within 45 days); OHIO REV. CODE ANN. § 1349.19 (West 2005); WIS. STAT. § 134.98 (2006); COLO. REV. STAT. § 6-1-716 (2006) (as quickly as possible); DEL. CODE ANN. tit. 6, § 12B-102 (2005); IDAHO CODE § 28-51-104 (Michie 2006).

68. Under the Californian law, substitute notice is only available if the data breach involved more than half a million individuals or would exceed a cost of over $250,000. *Id.* Other states vary on this point. *See, e.g.*, HAW. REV. STAT. § 487N-1 (2007) (breach involves over 200,000 persons and cost exceeds more than $100,000) and N.H. REV. STAT. ANN. § 359-C:20 (2007) (breach involves over 1,000 persons and cost exceeds $5,000).

69. CAL. CIV. CODE § 1798.29 (West 2003).

70. *Id.*

71. *See, e.g.*, CAL. CIV. CODE § 1798.29 (West 2003); FLA. STAT. § 817.5681 (2005); OHIO REV. CODE ANN. § 1349.19 (West 2005); WIS. STAT. § 134.97 (2006); COLO. REV. STAT. § 6-1-716 (2006); DEL. CODE ANN. tit. 6, § 12B-102 (2005); ALASKA STAT. § 45.48.010 (2009); ARIZ. REV. STAT. § 44-7501 (2007); ARK. STAT. § 45.48.010 (Michie 2009); D.C. CODE ANN. § 28-3851 (2007); GA. CODE ANN. §§ 10-1-911 (2005); 815 ILL. COMP. STAT. 530/5 (2005); IND. CODE § 24-4.9-2-2 (2006); MD. CODE ANN., COM. LAW § 14-3504 (2008); MASS. GEN. LAWS ch.93H, §1 (2007); NEB. REV. STAT. §§ 87-802 (2006); NEV. REV. STAT. § 603A.220 (2006); N.J. STAT. ANN. § 56:8-163 (West 2006); N.Y. GEN. BUS. LAWS §§ 899-aa (2005); N.D. CENT. CODE §§ 51-30-02 (2005); OKLA. STAT. tit. 74, § 3113.1 (2006); OR. REV. STAT. § 646A.602 (2007); S.C. CODE ANN. § 39-1-90 (2009); TENN. CODE ANN. § 47-18-2107 (2005); TEX. BUS. & COM. CODE. § 521.053 (Vernon 2005); WASH. REV. CODE § 19.255.010 (2005); W. VA. CODE § 46A-2A-101 (2008).

72. *See, e.g.*, Mark Burdon, Jason Reid & Rouhshi Low, *Encryption Safe Harbours and Data Breach Notification Laws*, 26 COMPUTER L. & SECURITY REV. 520 (2010) [hereinafter Burdon et al., *Encryption Safe Harbors*].

73. This point is covered in depth below at Part IV.A.

74. *See, e.g.*, CAL. OFFICE OF PRIVACY PROTECTION, RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION, at 6 (2009) ("One of the most significant privacy laws in recent years is the California law intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the

as Senate Bill 1386 (hereafter "SB1386"), but at its point of introduction SB1386 bore no resemblance to the data breach notification law into which it would eventually evolve.[75] A radical re-write was undertaken following a computer hacking incident at a data processing warehouse that the California State Government maintains.[76] An unidentified intruder gained access to the Government's information systems and retrieved the personal information of approximately 265,000 California public servants.[77] The state held an informational hearing into the incident, and it became apparent that the state government delayed notification to its employees.[78] Evidence presented during the hearing attributed several attempts of identity theft to the data breach.[79] As a consequence of the breach, SB1386 was therefore radically re-drafted and redesigned to

---

crime's impact."); Amanda Draper, Comment, *Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-notification Law*, 40 J. MARSHALL L. REV. 681, 686 (2007) (noting that high profile data breaches in credit card processing corporations have been an incentive for the development of new laws); Kenneth M Siegel, Comment, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 PENN ST. L. REV. 779, 781 (2007) (highlighting the identity theft risks that can arise from a single data breach); Regan, *supra* note 10, at 1105-06 (regarding the impact that major data breaches had on Congressional developments relating to a national data breach notification law); Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUS. L. REV. 1597, 1621 (2007) ("California's Notification Act has an admirable goal to curb identity theft."); Sara A. Needles, Comment, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 281 (2009) ("Much of data breach law has been enacted to deal with the threat of identity theft resulting from unauthorized access of computerized records."); Jennifer A. Chandler, *Negligence Liability for Breaches of Data Security*, 23 REV. BANKING & FIN. L. 223, 229 (2008) (highlighting potential mitigation benefits in relation to identity theft).

75. *See* S.B. 1386 (*Introduced*), 2002 Leg., Reg. Sess. (Cal. 2002), *available at* http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020212_introduced.pdf (a bill concerned with exempting the disclosure of personal information under the auspices of Californian freedom of information law). *See also* Joseph Simitian, *How a Bill Becomes Law, Really*, 24 BERKELEY TECH. L.J. 1009 (2009) (regarding the background development of some of the key issues relating to notification under the Californian law).

76. *Personal Information: Disclosure; Breach Of Security: Before the Assem. Comm. on Judiciary* (Cal. 2002), *availible at* http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_cfa_20020617_141710_asm_comm.html. *See also* Preston & Turner, *supra* note 64, at 459 (regarding the effect on the attack on the development of the law); Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J. L. & TECH. 4 (2003) (confirming the impact of the breach on the law's development); Jane Winn, *Are 'Better' Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1142-43 (2009) (providing a brief outline of the background development to California's law).

77. S.B. 1386 (*Introduced*), 2002 Leg., Reg. Sess. (Cal. 2002).

78. *See* Skinner, *supra* note 76, at 4 (regarding details of the delay).

79. *See id.* at 5 (providing details of the hearing in which attempts at identity theft were examined but could not be conclusively tied to the data breach).

provide immediate notification for the purposes of identity theft mitigation.[80] Despite the fact that data breach notification laws are designed to mitigate identity theft, subsequent research critically questions whether the link between data breaches and identity theft is as strong as initially indicated.[81]

The California law dramatically impacted the uptake of data breach notification laws in other state legislatures..[82] A majority of state-based laws are largely based on the California model,[83] but some state laws have adopted different notification triggers.[84] Acquisition

---

80. *See, e.g.*, Simitian, *supra* note 75, at 1011 (regarding the impetus for legislative action following the data breach).

81. *See, e.g.*, JAVELIN STRATEGY AND RESEARCH, DATA BREACHES AND IDENTITY FRAUD: MISUNDERSTANDING COULD FAIL CONSUMERS AND BURDEN BUSINESSES (2006) (conducting a study of identity theft victims which demonstrated that a small percentage was linked to data breaches); U.S. GOV'T ACCOUNTABILITY OFFICE, NO. GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) (reviewing twenty-four large data breaches to find little evidence of concomitant identity theft incidents); Sasha Romanosky, et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?* (Carnegie Mellon University), 30 J. OF POL'Y ANALYSIS & MGMT. (forthcoming 2011), *available at* http://ssrn.com/abstract=1268926 (analyzing identity theft complaints from victims and finding little evidence that data breach notification laws reduce the frequency of identity theft incidents); Brendan St. Amant, *Recent Development, Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 Harv. J. on Legis. 527 (2007) ("The currently favored cost-benefit analysis that links security breaches to identity theft obscures the central policy issue of what actual rights citizens should have over the whereabouts and release of their personal information."); FRED H. CATE, INFORMATION SECURITY BREACHES: LOOKING BACK AND THINKING AHEAD (2008), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf ("Identity fraud and security breaches are both certainly important issues, but there is little evidence connecting the two, especially in the case of true identity theft.").

82. *See* Burdon, et al., *Mandatory Notification of Data Breaches, supra* note 5, at 117 (chronicling the uptake of data breach notification laws post the inception of the Californian law). *See also* Flora J. Garcia, Comment, *Data Protection, Breach Notification, and the Interplay between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTEL. PROP. MEDIA & ENT. L.J. 693, 707-08 (2007) (regarding the rapid proliferation of state-based data breach notification laws).

83. CAL. CIV. CODE § 1798.29(A) (West 2003); FLA. STAT. § 817.5681 (2005); WIS. STAT. § 134.98 (2008); COLO. REV. STAT. § 6-1-716 (2006); 6 DEL. CODE ANN. tit. 12B § 102 (2005); IDAHO CODE ANN. § 28-51-105 (2006); ALASKA STAT. § 45.48.010 (2009); ARK. CODE ANN. § 4-110-105 (2005); GA. CODE ANN. §§ 10-1-911 (2005); 815 ILL. COMP. STAT. 530/5 (2005); NEV. REV. STAT. §§ 603A.220 (2006); N.J. STAT. ANN. § 56:8-163 (WEST 2006); N.Y. GEN. BUS. LAW §§ 899-AA (MCKINNEY 2005); N.D. CENT. CODE §§ 51-30-02 (2005); OKLA. STAT. tit. 74 § 3113.1 (2006); S.C. CODE ANN. § 39-1-90 (2009); TENN. CODE ANN. § 47-18-2107 (2005); TEX. BUS. & COM. CODE. ANN. § 521.053 (VERNON 2007); WASH. REV. CODE § 19.255.010 (2005); CONN. GEN. STAT. § 36A-701B (SUPP. 2006); LA. REV. STAT. ANN. § 51:3074 (2005); MINN. STAT. § 325E.61 (2006); MO. REV. STAT. § 407.1500 (2009); R.I. GEN. LAWS § 11-49.2-3 (2005); UTAH CODE ANN. §§ 13-44-202 (2006).

84. *See* Kathryn E. Picanso, Comment, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 383 (2006) (outlining states with a

based triggers, such as the California law, have a relatively low triggering threshold[85] that triggers an obligation to notify when an organization has suffered, or believes it has suffered a breach.[86] Risk based triggers, on the other hand, attempt to raise the triggering threshold to minimize the threat of unnecessary notification.[87] These triggers have a range of different standards that include: a reasonable likelihood of harm or material harm,[88] a reasonable likelihood of substantial economic loss,[89] a significant or material risk of identity theft or other frauds,[90] and whether a data breach has or is reasonably likely to cause loss or injury.[91]

In the US, laws have been enacted at the state level, and the situation at the federal level has some parallels to state-based law. First, there was an explosion of interest in data breach notification law leading to a proliferation of legal proposals in 2005 that has continued until the present time.[92] None of these bills have been enacted yet

---

reasonable risk of harm trigger); Michael E. Jones, Comment, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 555, 571-72 (2007) (detailing the use of risk based triggers in federal data breach proposals).

85. *See* Garcia, *supra* note 82, at 704 (triggering notification even if only reasonably believed acquired without actual use).

86. *See* Jones, *supra* note 84, at 562 (regarding the elements of acquisition based triggers that are deemed to favor consumer protection because notification is not left to the breached entity); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 933 (2007) (commenting the California law "is marked by a low threshold for notification").

87. *See* CATE, *supra* note 81, at 13 ("Requiring breach notices in situations other than those in which they are realistically likely to prevent or mitigate harm or serve some other clearly articulated valuable function threatens to exacerbate the existing tendency of recipients to ignore those notices"); MICHAEL TURNER, TOWARDS A RATIONAL PERSONAL DATA BREACH NOTIFICATION REGIME (2006), http://perc.net/files/downloads/data_breach.pdf ("At some point, consumers begin to discount notices if the average likelihood that a breach will result in damage is very low"); Jones, *supra* note 84, at 562 (regarding risk based triggers that are deemed to favor corporate interests because the decision to notify or not is left squarely with the breached organization).

88. *See, e.g.*, FLA STAT. § 817.5681 (2005); ALASKA STAT. § 45.48.010 (2009); ARK. CODE ANN. § 4-110-105 (2005); OR. REV. STAT. § 646A.600 (2007); CONN. GEN. STAT. § 36a-701b (2006); LA. REV. STAT. ANN. §§ 51:3071 (2005); IOWA CODE § 715C.1 (2008); N.C. GEN. STAT. §§ 75-60 (2005).

89. *See* ARIZ. REV. STAT. § 44-7501 (2007).

90. *See* OHIO REV. CODE ANN. § 1349.19 (West 2005); WIS. STAT. § 134.98 (2006); MD. CODE. ANN. COM. LAW §§ 14-3501 (2008); MASS GEN. LAW ch. 93H §1 (2007); R.I. GEN. LAWS § 11-49.2-1 (2005); UTAH CODE ANN. §§ 13-42-101 (2006); KAN. STAT. ANN. §§ 50-7a01 (2006); MICH. COMP. LAWS § 445.72 (2007).

91. *See* 73 PA. CONS. STAT. § 2303 (2006); MICH. COMP. LAWS § 445.72 (2007); MONT. CODE ANN. § 30-14-1704 (2006); VA. CODE ANN. § 18.2-186.6 (2008).

92. *See* Regan, *supra* note 10, at 1109-110 (outlining bills placed before both Houses of Congress).

although this may be about to change.[93]

The purposes of the bills varied. For example, some bills sought to develop a national, federal-based data breach notification law to supplant state-based laws.[94] Other bills responded to specific data breach incidents[95] and further bills covered certain industrial sectors such as the data brokerage industry[96] or Federal government agencies.[97] Second, the proposed federal bills share the same underlying rationale of state-based laws that the primary function of data breach notification was to provide individuals with an opportunity to mitigate any potential adverse outcomes, thus assisting with the prevention of identity theft-related crimes.[98]

Accordingly, data breach notification laws attempt to fulfill two differing conceptual aims. First, the law primarily seeks to formally recognize that an individual has a "right to know" about unauthorized misuse of his or her personal information and notice of the incident enables mitigation of subsequent identity theft.[99] Smedinghoff contends that the reporting of personal information data breaches is akin to the common law duty to warn of dangers.[100] The duty requires

---

93. *See* Data Accountability and Trust Act of 2009, H.R. 2221, 111th Cong. (2009).

94. *See, e.g., id.*; Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009); Data Breach Notification Act of 2009, S. 139, 111th Cong. (2009).

95. *See, e.g.*, Veterans' ID Theft Protection Act of 2006, H.R. 5487, 109th Cong. (2006); Comprehensive Credit Services for Veterans Act of 2006, H.R. 5783, 109th Cong. (2006); Comprehensive Veterans' Data Protection and Identity Theft Protection Act of 2006, H.R. 5577, 109th Cong. (2006) (following the aftermath of a major data breach involving the US Government's Department of Veterans Affairs). *See also* DEPARTMENT OF VETERANS AFFAIRS OFFICE OF INSPECTOR GENERAL, REVIEW OF ISSUES RELATED TO THE LOSS OF VA INFORMATION INVOLVING THE IDENTITY OF MILLIONS OF VETERANS (2006) (for extensive details of the breach).

96. *See, e.g.*, Identity Theft Bill, H.R. 3140, 109th Cong. (2005).

97. *See, e.g.*, Federal Agency Data Breach Notification Act of 2006, H.R. 5838, 109th Cong. (2006); Federal Agency Data Breach Protection Act of 2007, H.R. 2124, 110th Cong. (2007).

98. *See, e.g.*, Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009) ("To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information").

99. *See, e.g.*, Rode, *supra* note 74, at 1621 (commenting that the purpose of the Californian law was to provide consumers with greater knowledge in order they could take action); Thomas J. Smedinghoff, *Trends in the Law of Information Security*, 17 INTEL. PROP. & TECH. L. J. 1, 4 (2005) (stating that data breach notification laws are designed as a way to protect persons who may be adversely affected by a security breach); Needles, *supra* note 74, at 380 (stating "Breach notification laws let individuals know that their data has slipped into unauthorized hands"); Schwartz & Janger, *supra* note 86, at 917 (stating that breach notification can assist individuals and organizations to mitigate harm caused by a breach).

100. Thomas J. Smedinghoff, The State of Information Security Law: A Focus on the Key Legal Trends (May 2008) (unpublished manuscript), *available at*

a party who has a superior knowledge of a potential danger of injury or damage that could be inflicted upon another person, by a specific hazard, to warn persons who lack such knowledge.[101] Data breach notification law was thus intended to provide an *ex post* protection for individuals and mandatory notification was deemed the regulatory tool to complete that task.[102]

Second, the auxiliary aim of the law is to encourage organizations to adopt better security practices.[103] Encryption safe harbors are a case point as they seek to encourage the wider adoption of encryption technologies for the storage and use of personal information.[104] However, notification also acts as a regulatory threat through the tool of reputational sanction as breached organizations have to confess the incident to their customers.[105] Both encouragement and threat elements are designed to ensure that sound information management procedures and practices become a

---

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1114246.

101. *Id.* By requiring notice to persons who may be adversely affected by a security breach (e.g., persons whose compromised personal information may be used to facilitate identity theft), these laws seek to provide such persons with a warning that their personal information has been compromised, and an opportunity to take steps to protect themselves against the consequences of identity theft.

102. *See* Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1072-74 (2009) (regarding an overview of information disclosure measures as an *ex post* mechanism in data breach notification laws).

103. *See, e.g., id.* at 1075 (notification as an information disclosure mechanism is used to improve organizational security controls); Winn, *supra* note 76, at 1147-48 (regarding the incentives for database owners to implement security measures); Rode, *supra* note 74, at 1624 ("notification statutes . . . serve as powerful incentives for businesses to attack identity theft at the front lines"); Skinner, *supra* note 76, at 7 (quoting Benjamin Wright "they [data breach notification laws] have powerful incentive (sic) to secure data from the beginning"); Schwartz & Janger, *supra* note 86, at 953-55 (regarding "reasonable security" measures that the "ideal data processing entity" would put in place from a data breach notification act).

104. *See generally* Burdon et al., *Encryption Safe Harbours*, *supra* note 72 (providing a detailed critique of encryption safe harbors in data breach notification laws); MARK BURDON, ET AL., IF IT'S ENCRYPTED IT'S SECURE! THE VIABILITY OF US STATE-BASED ENCRYPTION EXEMPTIONS (IEEE 2010) [hereinafter BURDON, ET AL., VIABILITY], *available at* http://eprints.qut.edu.au/32781/1/c32781.pdf (analyzing encryption exemptions found in US state-based data breach notification laws against a factor-based safe harbor proposed in Australia and the EU); Winn, *supra* note 76, at 1145-46 (critiquing the California law's encryption safe harbor). *See also* Part III.B below.

105. *See, e.g.*, Winn, *supra* note 76, at 1143 (stating that the "shaming function" of data breach notification laws is a "direct and concrete" element); Schwartz & Janger, *supra* note 86, at 929-31 (detailing in depth the role of "reputational sanction" in data breach notification laws); Rode, *supra* note 74, at 1628 (regarding the disclosure of a security breach which can tarnish a company's public image).

management priority.[106] This reflects the fact that there was little market incentive for private sector organizations to behave responsibly and to report a data breach due to the negative publicity that would arise.[107] As such, the second aim of data breach notification law also has an *ex ante* element through the encouraged adoption of information security measures.[108] Nevertheless these are two very different aims that arise from data breach incidents.[109] Data breach notification laws therefore demand a delicate balancing act that requires gauging the risks of providing adequate notification to individuals while attempting to minimize corporate compliance cost burdens relating to unnecessary notification.[110]

C. Summary

This brief overview of the conceptual background and legislative development of both information privacy and data breach notification laws reveal similarities and differences between both legal concepts. Both laws have an obvious interest relating to the protection of personal information and they both attempt to provide individuals with a greater knowledge about the use of their personal information

---

106. *See* Schwartz & Janger, *supra* note 86, at 926 (regarding the various forces that are formed under data breach notification law).

107. *See* COMPUTER SECURITY INSTITUTE, COMPUTER CRIME AND SECURITY SURVEY (2006), *available at* http://pdf.textfiles.com/security/fbi2006.pdf (detailing the reluctance of organizations to inform law enforcement agencies about a data breach); ALESSANDRO ACQUISTI, ET AL., IS THERE A COST TO PRIVACY BREACHES? AN EVENT STUDY 4 (2006), *available at* http://aisel.aisnet.org/icis2006/94/ ("a privacy incident is a negative externality that natural incentives cannot correct"); Chandler, *supra* note 74, at 228 (regarding the lack of consumer interest in data breaches and the limited effect on share price as an effective deterrent to implement security measures); Rode, *supra* note 74, at 1631 (regarding the ineffectiveness of market based provisions when businesses miscalculate the value placed by individuals on privacy). *See contra* Jacob W. Schneider, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 291 (2009) (stating that the ineffectiveness of data breach notification as a legal remedy because it provides little market incentive to strengthen data security).

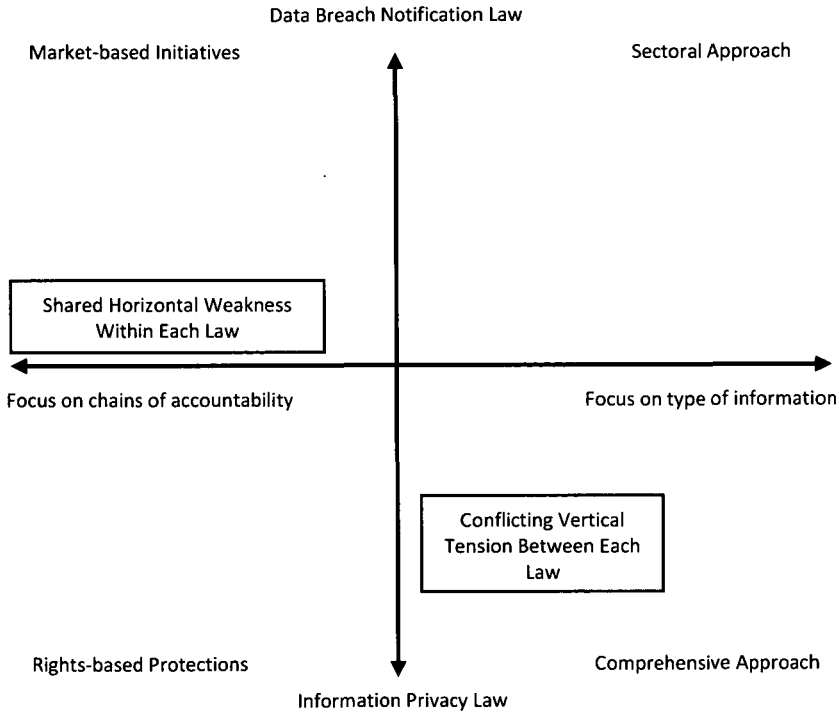
108. *See* Romanosky & Acquisti, *supra* note 102 (regarding the ex ante role of security protections to reduce the numbers of future data breaches).

109. *See* Needles, *supra* note 74, at 281 (noting the different purposes between data breach notification as "data control" and as a "privacy" concern); Turner, *supra* note 87 (regarding the conflicting notions of notification to individuals and the use of notification as an incentive to strengthen security).

110. *See* Schwartz & Janger, *supra* note 86, at 918 (regarding the "important function of breach notification" after a breach that requires a "multi-institutional, co-ordinated response"); Schwartz, *supra* note 36; Thomas J. Smedinghoff, *Security Breach Notification - Adapting to the Regulatory Framework*, 21 The Review of Banking & Financial Services 115 (2005); Turner, *supra* note 87 (regarding the risks that organizations face in decision to notify or not to notify).

by organizations. Despite these obvious similarities, there are also significant differences between the two laws that go to the heart of both concepts and different legal frameworks. To outline these distinctions, the metaphor of vertical and horizontal is employed to determine tensions shared weaknesses.[111] These issues are explored further in the next parts of this article and represented by figure 1 below.

Fig.1 – Vertical Tensions and Horizontal Weaknesses



111. *See, e.g.*, Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 872-73 (2009) (regarding the classification of dimensions relating to US information privacy law as vertical issues, such as the desirability of a comprehensive federal law over state-based laws and horizontal issues which regard "the interplay of any federal information privacy law with other sector-Specific federal rules").

III. CONFLICTING VERTICAL TENSIONS

Vertical tensions emanate due to the differing conceptual and developmental origins of both laws that ultimately represent the distinction between sectoral and comprehensive approaches to the regulation of information privacy.[112] The author asserts that the sectoral/comprehensive distinction also determines the form of regulatory remedy that is deemed appropriate which further highlight distinctions between market-based initiatives and rights-based protections that result in contradictory emphases over the minimization of corporate compliance costs.

A. Sectoral Versus Comprehensive Approaches

The implementations of information privacy laws have taken essentially different tracks despite their similar origins.[113] That in itself is not surprising as a right to privacy is not perceived as an absolute right and thus the interpretation of the emphasis given to an individual's right to control his or her personal information is in competition with other social rights and interests. The application of information privacy legal regimes is likely to be a matter of contestable discussion amongst different legislative jurisdictions.[114] As such, information privacy laws are manifestations of political processes which have implications for the implementable scope of such laws.[115] Jurisdictional information privacy laws therefore reflect

---

112. The author acknowledges that the distinction between sectoral and comprehensive frameworks is a broad categorization only and notes that some comprehensive laws also have aspects of sectoral regulation. *See* BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 132-33 (highlighting that the sectoral/comprehensive distinction is broad in its conceptual reach and that in practice several countries encompass aspects of both approaches within their legal systems). However, this broad distinction is sufficient for the purposes of this article because it demonstrates the different conceptual, normative and regulatory foundations of US data breach notification law when examined in conjunction with comprehensive information privacy regimes.

113. *See* BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 3-6 (stating that human need for privacy is "manifested to different degrees and in different ways from culture to culture").

114. *See, e.g.*, Charles Raab, *From Balancing to Steering: New Directions for Data Protection*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 68 (Colin J. Bennett & Rebecca Grant eds., 1999) (regarding the limited role of a right to privacy which does not take precedence over all uses of personal information); REGAN, LEGISLATING PRIVACY, *supra* note 33, at 16 (regarding privacy protection in the US as the balancing of individual and political interests); BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 13 (stating that privacy is not an absolute right and is balanced against other community rights and obligations).

115. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 125 (contending that information privacy law is "an exercise of the power of the state in regulating the processing of

the wider social, legal and policy values of individual jurisdictions.[116] The US attitude towards information privacy law and the developmental purpose of data breach notification laws reflect this point.

The sectoral approach[117] to information privacy in the US has been characterized as "sporadic"[118] and "reactive."[119] The regulatory focus of US information privacy law is the general curtailment of government powers in combination with laws that govern industry-specific practices or various types of sensitive information.[120] The existence or non-existence of information privacy regulation at the federal level is specific to particular circumstances or sectors. For example, the Privacy Act[121] provides a range of fair information practices that US Government agencies must comply with regarding the handling of personal information. The Gramm Leach Bliley Act[122] (GLBA) creates privacy protections for personal financial information within the specific remit of the financial services sector. The Health Insurance Portability and Accountability Act (HIPAA)[123] consigns

---

personal data").

116. *See* BENNETT, *supra* note 21, at 242-43 (regarding the effect of different political philosophies on the implementation of information privacy legislation); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 153 (1998) (contending that different approaches to privacy protection reflect unique jurisdictional approaches).

117. *See* Gellman, *supra* note 61, at 195 (describing sectoral as "no general privacy laws, just specific laws covering specific records or record keepers"); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 910 (2009) (US information privacy laws "regulate information use exclusively on a sector-by-sector basis").

118. *See* Joel R. Reidenberg, *The Globalization of Privacy Solutions: The Movement Towards Obligatory Standards for Fair Information Practices, in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE, 217 (Colin J. Bennett & Rebecca Grant eds., 1999); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 236 (1992) (stating that the lack of a coherent and systematic approach to information privacy protection in the US "presents an undesirable policy void"); John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 25 RICH. J.L. & TECH. 1, 15 (2009) (stating that US privacy regulation is best described as "a haphazard set of industry specific regulations...which frequently overlap and are often contradictory"); Gellman, *supra* note 61, at 195 (describing the legal structure for US privacy protection as a "patchwork quilt").

119. *See* BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 37 (regarding reactivity as a weakness of sectoral regimes).

120. *See, e.g.*, Reidenberg, *supra* note 118, at 209 (stating that US federal and state information privacy laws target individual protection in relation to defined problems that arise from fear of government intervention and a reluctance to regulate industry).

121. The Privacy Act of 1974, 5 U.S.C. § 552a (2006).

122. Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999, 15 U.S.C. §§ 6801-6809 (2006).

123. Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. §§ 160, 162,

legal protections in relation to identifiable health information held in the medical and health insurance sectors. In a different vein, the Children's Online Privacy Protection Act (COPPA)[124] governs restrictions on the collection of online personal information from children under the age of thirteen.

Alongside these sector-based laws, there are a collection of other laws that provide legal remedies for specific issues that have become sufficiently politicized to warrant legislative action.[125] For example, the Drivers Privacy Protection Act (DPPA) restricts the disclosure of driver license information by state authorities.[126] The DPPA was a legislative response to the murder of actress Rebecca Schaeffer where an assailant used publicly available driver license information to stalk and then murder the victim.[127] The DPPA has also been instrumental in restricting the sale of driver license information by state agencies to commercial entities.[128] The Video Privacy Protection Act[129] protects personal information provided to video rental stores following a controversy involving Supreme Court nominee Robert Bork and the media's publication of his video watching habits.[130]

The myriad of information privacy legislation has also been replicated at the state level.[131] Some states implement laws that provide general statutory rights of privacy that are akin to tort law

---

164 (2006).

124. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006).

125. *See* BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 37; REGAN, LEGISLATING PRIVACY, *supra* note 33, at 199 (stating that congressional privacy legislation was based on various critical events which opened up a policy window); Priscilla Regan, *The United States*, *in* GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION 51 (James B. Rule & Graham Greenleaf eds., 2008) ("Generally it takes an incident to focus attention on the issue of information privacy – and such incidents tend to focus on one type of record system at a time.").

126. Drivers Privacy Protection Act of 1994, 18 U.S.C. § 2725 (2006).

127. *See, e.g.*, SOLOVE, UNDERSTANDING PRIVACY *supra* note 19, at 69 (regarding the distinction between public and private data in the Schaeffer case); Garcia, *supra* note 82, at 715 (stating the "Schaeffer case is credited with sparking the passage of the Drivers' Privacy Protection Act"). *See also* REGAN, LEGISLATING PRIVACY, *supra* note 33, at 207 (regarding the use of state driver license information to harass pregnant mothers who visited abortion clinics).

128. *See, e.g.*, Michael A. Froomkin, *Government Data Breaches*, 24 BERKELEY TECH. L.J. 1019, 1029 (2009) (noting the importance of the DPPA to state agencie).; Garcia, *supra* note 82, at 715 (highlighting state revenues based from the sale of driver license information); Regan, *supra* note 125, at 50 (summarizing the development of the DPPA).

129. Video Privacy Protection Act of 1998, 18 U.S.C. § 2710 (2006).

130. *See* Schwartz, *supra* note 117, at 935-36 (providing a comprehensive overview to the development of the law including details of congressional outrage).

131. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 221 (1992) (commenting that state-based protections suffer from incompleteness and that state-based protections vary from state to state).

protections and thus govern areas such as common law invasions of privacy.[132] Other states, like their federal counterpart, have enacted a number of sectoral based laws that are aimed at certain industry practices. For example, in addition to federal laws, some states have specifically legislated laws relating to the use of personal information in relation to certain information, such as video rental records, as highlighted above.[133] Accordingly, Schwartz contends that a duopoly exists between federal and state laws in which federal laws deliver specified benchmarks that allow state laws further room for experimental development.[134]

Comprehensive legal frameworks, on the other hand, adopt a different approach to sectoral regimes. They establish information privacy rights for individuals and define obligations for data collecting organizations regardless of industrial sector.[135] Comprehensive frameworks have universal notions of the type of information that is covered by information privacy laws, typically defined as "personal data"[136] or "personal information."[137] Moreover, the type of data covered by these laws is generally context dependent which means that different types of information can be personal information at different times depending upon the context upon which it is used.[138] The context dependent approach is a significant difference to sectoral laws that have a restrictive outlook of the type of information that will constitute personal information. Hence, sectoral information privacy laws have developed context-independent approaches related to the classification of personal information that reflect the restricted aims of industry or information specific legislation.

Enforcement mechanisms operated by comprehensive information privacy regimes are also different to those found in sectoral regimes. Most comprehensive frameworks employ specific

132. *Id.* at 228.

133. *See* Schwartz, *supra* note 117, at 919 (regarding state variants on the VPPA).

134. *Id.*; *but see* Bellia, *supra* note 111, at 873.

135. *See, e.g.*, Council Directive 95/46, Art 7, 1995 O.J. (L281) (EC).

136. Council Directive 95/46, Art 2(a), 1995 O.J. (L 281) (EC).

137. S6(1) PRIVACY ACT 1988 (Cth) (Austrl.).

138. *See, e.g.*, Mark Burdon & Paul Telford, *The Conceptual Basis of Personal Information in Australian Privacy Law*, 17 Murdoch Elaw Journal 1 (2010) [hereinafter Burdon & Telford, *Conceptual Basis*] (regarding an overview of context independent and context dependent approaches in Australian privacy law); *See also* SHARON BOOTH ET AL., WHAT ARE 'PERSONAL DATA'? A STUDY CONDUCTED FOR THE UK INFORMATION COMMISSIONER 6 (2004) (regarding a survey of data protection authorities and their conceptual construction of personal information).

supervisory authorities with given sets of legislative powers to protect the rights of individuals and impose compliance obligations upon organizations and are seen as a necessary condition of an effective information privacy regime.[139] Contrast that with the situation in the US, which does not have a dedicated supervisory authority for the enforcement of information privacy. Instead, governance obligations are dispersed amongst different public sector organizations that mirror the fragmented legislative focus of the US approach.[140] Moreover, the lack of a unified commission is now seen as a detriment to the US approach to information privacy.[141]

Data breach notification laws have thus been developed within the sectoral environment of the US to provide a remedial fix to a given problem, namely, the mitigation of identity theft arising from data breaches of personal information.[142] However, a law that has a primary purpose of mitigating identity theft is fundamentally different from a law that is purposely designed to ensure the protection of personal information as found in comprehensive information privacy regimes.[143] The former is designed to provide a particular remedy to a specific problem while the latter consigns broad rights to individuals regarding the personal information exchange process. The question consequently arises whether data breach notification laws *should* regard the protection of personal information *per se,* as information privacy laws do, rather than focusing on the specified remit of mitigating identity theft?

These are weighty normative distinctions for to do so require a major change in perspective, from both sectoral and comprehensive approaches, regarding the purpose of data breach notification. There is a clear conceptual foundation for a narrower approach to the protection of personal information in data breach notification laws

---

139. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 113 (noting the European Union's approach to privacy laws).

140. E.g., eight federal agencies have supervisory powers to enforce elements of the GLBA. They are the Federal Trade Commission; The Office of the Comptroller of the Currency; The Federal Reserve Board; The Federal Deposit Insurance Corporation; The Office of the Thrift Supervision; The National Credit Union Administration; The Security and Exchange Commission and the Commodity Futures Trading Commission. OFFICE OF THE COMPTROLLER OF THE CURRENCY ET AL., INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE (2005), http://www.ots.treas.gov/docs/2/25231.pdf.

141. *See* Schwartz, *supra* note 117, at 927 (regarding one of the positive effects of a comprehensive law in the US).

142. *Id.* at 929-31.

143. *See, e.g.*, Winn, *supra* note 76, at 1134 (regarding the potential limiting implications of data breach notification laws that predominantly focus on the mitigation of identity theft).

that goes back to the first data breach notification law, California Civil Code 1729(a), and flows through to recent US state and federal developments. However, even in comprehensive jurisdictions, there has been a degree of reluctance to enmesh data breach notification completely within established legal frameworks.[144] This has resulted in the EU's data breach notification scheme being developed within the reduced scope of the e-Privacy Directive and the Australian Law Reform Commission's proposal that has not only developed an ancillary definition of personal information for the specific purpose of data breach notification,[145] but has recommended that data breach notification not be formalized as a privacy principle. [146]

Data breach notification law, viewed from the perspective of the type of information privacy legal framework within which it operates, provides a contradictory picture about how it has been applied. In the US, data breach notification law is a comprehensive measure to remedy deficiencies arising from the sectoral approach to information privacy.[147] The comprehensiveness of the law is evident because it generally applies to all types of organization regardless of industrial sector.[148] However, the application of this comprehensive approach is nevertheless constrained by focusing notification to specified circumstances that could give rise to identity theft which involve certain types of combined personal information. Conversely, data breach notification law in comprehensive regimes is a sectoral measure to remedy deficiencies in the application of fair information practices or information privacy principles that regard corporate obligations to secure personal information.[149] In effect, the notifications resulting from the advent of data breach notification laws demonstrate that the application of security-related principles and practices simply are not working both in terms of the volume of

144. *See, e.g.*, Burdon, et al., *Mandatory Notification of Data Breaches*, *supra* note 5, at 127 (regarding the reluctance of Australian and EU legislators to fully enmesh data breach notification within existing legal frameworks).

145. *See* AUSTRALIAN PRIVACY LAW AND PRACTICE, *supra* note 6, at 1693 (Specifying personal information under the proposal, "should draw on the existing definitions of 'personal information' and 'sensitive information' in the Privacy Act and should prescribe what combinations of these types of information would, when acquired without authorization, give rise to a real risk of serious harm requiring notification").

146. *See* Nigel Waters, et al., *Intepreting the Security Principle* (Cyberspace Law and Policy Centre, University of New South Wales, Working Paper No. 1, 2007), *available at* http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf.

147. *Id.* at 34-35.

148. *See* Needles, *supra* note 74, at 277.

149. *Id.* at 283.

incidents and the number of persons affected. Accordingly, data breach notification is either a comprehensive facet to a sectoral approach or a sectoral adjunct to a comprehensive regime.[150] These differences in application are manifested in the scope of protections provided in sectoral and comprehensive regimes which place different priorities relating to the provision of individual protections and the minimization of corporate compliance costs.

B. Market-Based Initiatives Versus Rights-Based Protections

The manifestations of sectoral and comprehensive approaches highlight differences between both laws as they place alternate priorities about the role of organizational compliance cost mitigation. Data breach notification laws tend to adopt market-based remedies that are conscious of the compliance requirements of data collecting organizations whereas those information privacy regimes that adopt data breach notification laws tend to focus more on the preservation of individual protections. The development of encryption safe harbors for data breach notification in the US and other jurisdictions is relevant in this regard.

The use of an encryption safe harbor has been an integral element of data breach notification laws because legislators use encryption to define notification parameters for organizations. As applied in most data breach notification laws, encrypted personal information does not trigger an obligation to notify because the information that has been acquired without authorization is secure, and therefore does not pose an identity theft risk.[151] In a review of 2007 US developments, Jones identified three types of encryption safe harbors. [152] *Exemptions* exempt notification based on the notion that encrypted data is secure and does not pose a risk.[153] *Rebuttable presumptions* create a presumption that encrypted data is secure and unauthorized acquisitions do not have to be notified.[154] However, this presumption can be rebutted by facts to the contrary. *Factor-based analysis* requires breached organizations to demonstrate that the encryption adopted was effective before notification is exempted.[155]

---

150. *See, e.g., id.* at 303 (regarding the application of data breach notification in US and other jurisdictions).

151. *Id.* at 278-79.

152. Michael Jones, *Data Breaches: Recent Developments in the Public and Private Sector*, 3 ISJLP 555, 573 (2007).

153. *Id.* at 565.

154. *Id.* at 573.

155. BURDON, ET AL., VIABILITY, *supra* note 104.

The use of these different types of safe harbors reveals underlying contestations that take place in sectoral and comprehensive regimes regarding the use of encrypted personal information as a means to minimize corporate compliance costs. Recent research shows that the use of exemptions and rebuttable presumptions are favored by the sectoral approach of the US while factor-based analysis is favored in comprehensive regimes such as the EU and Australia.[156]

At the US state legislature level, the use of encryption exemptions is directly linked to corporate compliance cost reduction and the development of market incentives to enhance corporate information security measures. For example, the controversial encryption exemption adopted in the California law appears to have been developed as a means of reducing corporate fears relating to compliance costs and to ensure that the law was compliant with related federal legislation and regulation.[157] The legislative intent of the California encryption exemption was thus a relatively simple solution to the complex balancing act of enhancing information security practices, while at the same time, minimizing compliance burdens. Similar outcomes are also evident in other states. Following the implementation of Indiana's initial data breach notification law in 2006, a second data breach notification bill was introduced in 2008[158] that sought to alter the statute's definition of encryption. The provisions of the second bill would have had the effect of benchmarking adopted encryption processes and technologies to ensure they meet existing industry best practices, including the move away from password protection to encryption. However, the vast majority of the bill was rejected following intensive lobbying by major corporations who feared an increase in compliance requirements.[159]

The development of the Massachusetts encryption exemption has

156. *See generally* Burdon et al., *Encryption Safe Harbors*, *supra* note 72.

157. *Personal Information Privacy: Hearing on SB1386 Before the Assembly Committee on Buisness and Professions, (need leg. session info) (2002)* (statement by Lou Correa, Chairman, Assembly Committee on Business and Professions) ("[I]n practice, this bill will create incentives for organizations seeking to simplify their legal requirements to encrypt their personal information data and develop privacy policies with similar notification procedures.").

158. H.B. 1197, 2008 115th Gen. Assemb., Second Reg. Sess. (Ind. 2008) (sought additions to the existing encryption definition that would require adopted encryption processes to be "consistent with best practices common in the industry" including the security management arrangements of the encryption key).

159. *See* Chris Soghoian, *At&T, Microsoft Win as ID Theft Bill Eviscorated*, CNET NEWS, February 13, 2008), http://news.cnet.com/8301-13739_3-9870992-46.html (regarding the contentious discussions involved in the development of the second bill).

also been fraught with contention. The Massachusetts definition of encryption is unique[160] and has been the subject to much controversy particularly relating to the use of further regulations developed by the Office of Consumer Affairs and Business Regulation (OCABR). The first version of the OCABR regulations was released in early 2008 to voluble criticism from private sector organizations regarding potential compliance requirements.[161] The criticism was such that a public hearing was held and a further senate bill (SB173) was put forward to revise the encryption requirements of the OCABR regulations.[162] Senate Chairman Morrissey introduced SB173, stating at the hearing that the regulations went "beyond its intent"[163] in relation to technical requirements and other factors. Moreover, SB173 removed the specific requirement for a type of encryption and stated that a specified form of encryption was not to be applied.[164] The primary reason for the removal of the specified encryption exemption was to protect small and medium size businesses as specified by section one of SB173.[165] In February 2009, OCABR released amended

160. *See* MASS. GEN. LAWS ch. 93H, §1 (2007). (The full definition of encryption reads: encryption "is the transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation." It is the second element of the definition, in conjunction with the 128 bit requirement that has led to controversy).

161. *See* Mark E. Schreiber & Robert G. Young, *Aggressive New Massachusetts Data Breach Law and Proposed Security Rules Require Company Action*, 3 PRIVACY & DATA SECURITY L.J. 140, 144 (2008), *available at* http://www.eapdlaw.com/files/News/4322f87f-a398-4342-8c0b-33c977a22c54/Presentation/NewsAttachment/eb517cbf-4b50-4d70-a250-399e9596f7da/aggressive%20new%20massachusetts%20data%20law.pdf (regarding private sector concerns); *see also* Anne Doherty Johnson, *AeA Update: Massachusetts Data Breach Regulations*, AEA NEW ENGLAND COUNCIL, Nov. 17, 2008, http://www.aeanet.org/AeACouncils/zpUnYyihJjBdaJkdVziIPsEPkNrmnYWy.pdf (particularly in relation to technical issues such as the definition of encryption, the requirement to encrypt personal information and the requirement to encrypt information transmitted wirelessly).

162. *See* Alexander B. Howard, *Mass. Senate Seeks to Amend, Weaken Data Breach Notification Law*, SEARCH COMPLIANCE, May 14, 2009, http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1356356,00.html# (regarding the claim that the Massachusetts Legislature had the power to change 93(H) but not the regulations). *See also* Jason Lefferts, *Office of Consumer Affairs Files Revised ID Theft Regulations*, OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, Feb. 12, 2009, http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090212_idtheft&csid=Eoca (regarding the regulatory change of approach).

163. *See* Alexander B. Howard, *Mass. Senate Seeks to Amend, Weaken Data Breach Notification Law*, SEARCH COMPLIANCE, May 14, 2009, http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1356356,00.html#.

164. *Id.*

165. *See* S.B. 173, 186th General Court (Mass. 2009), *available at* http://www.mass.gov/legis/bills/senate/186/st00pdf/st00173.pdf. S1(A), SB173 (stating "The

regulations and the definition of encryption was changed.[166] At present, SB173 has not been enacted but the new regulations have now come into force.[167]

At the US federal level, the two bills that have passed a vote in Congress contain rebuttable presumptions rather than exemptions. However, the use of rebuttable presumptions still indicates a desire to reduce corporate compliance obligations. Testimony heard by the House of Representative Subcommittee on Commerce, Trade and Consumer Protection, in relation to the DATA 2009 bill is clear on this point. The threat of over-regulation was clearly articulated in line with the adoption of a risk-based approach that focused on the implementation of reasonable and appropriate security measures rather than specific technologies.[168] A similar point is echoed by California Senator Diane Feinstein regarding her efforts to introduce a number of data breach notification bills including the Notification of Risk to Personal Data Act of 2005. Senator Feinstein did not believe an encryption exemption was warranted because "[c]onsumers must have the tools they need to protect themselves against the risk of identity theft"[169] even though it was against the interests of the

---

department shall not in its regulations, however, require covered persons to use a specific technology or technologies, or a specific method or methods for protecting personal information.").

166. OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, 201 CMR 17.00: STANDARDS FOR THE PRTOECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH, http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf (last visited Sept. 7, 2010) ("the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key").

167. *Id.* (regarding the new regulations).

168. *See Testimony of Robert Holleyman: Hearing on H.R. 2221 "the Data Accountability and Protection Act" and H.R. 1319 "Informed P2P User Act" Before the Subcommittee on Commerce, Trade and Consumer Protection House Committee on Energy and Commerce,* 111th Cong. 5 (May 5, 2009) (statement of Robert Holleyman President and CEO of Business Software Alliance) (regarding testimony provided by Robert Holleyman, the president of the Business Software Alliance (BSA) and stating "The potential is high to turn data custody – an activity that is for most companies, whether large or small, only incidental to their core business – into a stifling compliance burden, with little to gain in terms of increased data security"). *See also* Business Software Alliance, *About BSA and Members*, BSA, http://www.bsa.org/country/BSA%20and%20Members.aspx (last visited Sept. 8, 2010) (stating "BSA is the voice of the world's commercial software industry and its hardware partners on a wide range of business and policy affairs").

169. Press Release, Senator Diane Feinstein, Press Release: Senator Feinstein Calls for Passage of Legislation to Require Prompt Notification When Personal Information Has Been Compromised by Data Breach (June 6, 2006) (on file with author), *available at* http://feinstein.senate.gov/public/index.cfm?FuseAction=NewsRoom.PressReleases&ContentRecord_id=7929faac-7e9c-9af9-71f4-d3142e230015&Region_id=&Issue_id=5b8dc16b-7e9c-9af9-7de7-22b24a491232).

financial sector.[170] The bill did not succeed, but Senator Feinstein clearly indicates corporate interests in the reduction of compliance requirements related to data breach notification.

These examples highlight that the use of encryption safe harbors in US data breach notification laws and proposals prioritize the reduction of corporate compliance cost burdens by minimizing the scope of notification. The encryption safe harbor has been an adjunct to the primary aim of the laws, the mitigation of identity theft crimes, and has been developed as a counterbalance to corporate fears of the compliance implications of over-notification that potentially conflict with the consumer protection aims of data breach notification laws.

Contrast that with similar discussion within the EU where encryption safe harbors have also been a bone of contention but for different reasons. The Article 29 Data Protection Working Party issued an opinion on the proposed amendments to the e-Privacy Directive and stated that the appropriate technological protection measures exemption should not be implemented.[171] The Working Party feared that the enactment of an exemption would significantly reduce the quality and usefulness of notifications delivered to affected persons.[172] In essence, the only way a person can take action to protect themselves is if they have received adequate information about the risk. The content of notification format is an essential component of notification and organizational decisions to notify should only be based on the principle of risk assessment rather than exemptions based on technical measures to protect personal data.[173] The European Data Protection Supervisor (EDPS) voiced a similar concern by broadly stating that Article 4 of the amended e-Privacy Directive "should not contain any exception to the obligation to notify".[174] Instead, the issue of safe harbors to notification should be

170. Press Release, Senator Diane Feinstein, Press Release: Senator Feinstein Reiterates Call for Passage of Strong ID Theft Legislation (June 7, 2006) (on file with the author), *available at* http://www.feinstein.senate.gov/public/index.cfm?FuseAction=NewsRoom.PressReleases&ContentRecord_id=792a0134-7e9c-9af9-75ef-07abbb67d740&Region_id=&Issue_id=5b8dc16b-7e9c-9af9-7de7-22b24a491232).

171. *See* Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) at 6, Article 29 Data Protection Working Party (2009).

172. *Id.* at 6.

173. *Id.*

174. Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) at 8 (2008).

addressed through extensive debate relating to the issues at stake which would be reflected in implementing legislation.[175]

Significant differences exist between sectoral and comprehensive approaches regarding the choice of encryption safe harbors in data breach notification laws. The use of encryption safe harbors highlights the different prioritization between sectoral and comprehensive approaches regarding conflicting interests of corporate compliance and consumer protection.[176] The use encryption safe harbors again highlights the *ex ante* and an *ex post* purposes[177] that are inherent to data breach notification. Comprehensive approaches focus on the *ex ante* purpose through the encouraged adoption of encryption and other technologies to protect personal information.[178] The sectoral approach, on the other hand, focuses on the *ex post* aim that regards a greater importance to the minimization of compliance cost burdens by not requiring notification for data breaches that involve the unauthorized acquisition of encrypted personal information. As such, the use of encryption safe harbors for data breach notification purposes in comprehensive legal frameworks encourage the use of encryption as a means to secure personal data *per se* thus ensuring the protection of individual rights of control and access to personal information. However, encryption safe harbors in sectoral data breach notification laws use encryption as compliance cost reduction measure and a market-based incentive for encouraged adoption of information security procedures.[179] These are two different motivations for the use of encryption that reflect the expansive scope of rights-based protections of information privacy laws and the narrow approach of market-based initiatives found in data breach notification laws. These fundamental differences explain why the sectoral approach of data breach notification sits rather

175. *Id.* at 8.

176. *See, e.g.*, Winn, *supra* note 76, at 1161 (regarding the development of the Californian law, "Confronted with the complex, multi-polar institutional framework of business information systems, the California legislature asserted jurisdiction over only two parties and crafted a bi-polar solution that resembles the holding of a case more than it resembles modern regulation: California citizens were given a right of notice of problems occurring at businesses serving them.").

177. Romanosky & Acquisti, *supra* note 102, at 1061.

178. *See, e.g.*, The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data at 15-16, Article 29 Data Protection Working Party (2009); Plain English Guidelines to Information Privacy Principles 4-7 at 7, Office of the Privacy Commissioner (Austrl.) (1998).

179. *See, e.g.*, Reidenberg, *supra* note 118, at 239-40.

uncomfortably in comprehensive frameworks and the comprehensive element of universal coverage generates such compliance cost-related concerns.

IV. SHARED HORIZONTAL WEAKNESSES

Along with fundamental differences, both information privacy and data breach notification laws share similar weaknesses which come more clearly into focus when the conceptual reach of the information covered by the laws is examined. Regulatory action under both laws is derived under chains of accountability that seek to link providers, collectors and users of personal information. Moreover, both laws have an overt focus on the regulation of specific types of information albeit from different conceptual and contextual approaches. These shared weaknesses are illustrated within the context of three major data breaches.

A. Three Illustrative Data Breaches

Three data breaches are examined to demonstrate that individual breaches have different causes and ramifications that require alternative regulatory responses. The introduction of Bennett and Raab's Fallibility Matrix reveals the different causes behind the three breaches that involve both human and technological errors. However, both data breach notification and information privacy laws have restricted accountability frameworks which results in limited remedies.

The first example involves the British National Party (BNP) and the leaking of their membership list. The BNP is a right-wing, nationalist political party based in the United Kingdom, and membership of the party is a sensitive issue as some professions preclude membership of the party.[180] In 2008, a disgruntled former BNP employee obtained the BNP's membership list without authorization and published the roughly 13,500 party membership list on the Internet.[181] The published details included names, addresses,

180. *See ACPO Bans Police from Joining BNP*, BBC NEWS, May 19, 2004, http://news.bbc.co.uk/2/hi/uk_news/3930175.stm (regarding the Association of Chief Police Officers (ACPO) ban on membership of the BNP in UK police forces); Christopher Hope, *How Many BNP activists Live in Your Town? Now You Can Find Out*, THE DAILY TELEGRAPH, Nov. 20, 2008, http://www.telegraph.co.uk/news/newstopics/politics/3484489/How-many-BNP-activists-live-in-your-town-Now-you-can-find-out.html.

181. *See generally* Ian Cobain, Esther Addley & Haroon Siddique, *BNP Membership List Posted Online by Former 'Hardliner'*, GUARDIAN, Nov. 19, 2008, http://www.guardian.co.uk/politics/2008/nov/19/bnp-list; *BNP Activists' Details Published,*

telephone numbers, email addresses, and, in some cases, employment details. The list also included the names and ages of children who have become members of the party after a parent had taken out a family membership, and several people who had joined the party at the age of sixteen.[182] The BNP subsequently admitted that the list was inaccurate as it included the names of persons who had never been party members.[183]

Different organizations and individuals used bit torrent and social networking websites[184] to copy and disseminate the membership list further. Moreover, media organizations and individuals used the membership list to create geo-mashups based on its content. The unauthorized release of the BNP membership list had some serious consequences. Some BNP members lost their jobs[185] or received death threats[186] and in one instance, a car belonging to the

---

BBC NEWS, May 19, 2008, http://news.bbc.co.uk/2/hi/7736405.stm; Dominic Kennedy & Nico Hines, *Thousands in Fear after BNP Members List Leak*, THE TIMES, Nov. 19 2008, http://www.timesonline.co.uk/tol/news/politics/article5183833.ece; James Kirkup & Christopher Hope, *BNP Membership List Leaked onto Internet*, THE DAILY TELEGRAPH, Nov. 19 2008, http://www.telegraph.co.uk/news/newstopics/politics/3479612/BNP-membership-list-leaked-onto-internet.html; Ben Russell, *BNP Membership List Published on Internet*, THE INDEPENDENT, Nov. 19 2008, http://www.independent.co.uk/news/uk/politics/bnp-membership-list-published-on-internet-1024719.html; James Sturcke, et al., *BNP Membership List Leaked Online*, GUARDIAN, Nov. 18, 2008, http://www.guardian.co.uk/politics/2008/nov/18/bnp-membership-list-leak.

182. *See* Cobain, Addley & Siddique, *supra* note 181.

183. *See* Sturcke, et al., *supra* note 181 (reporting that data collected and published on the list was of a rather unconventional nature).

184. *See* Sam Leith, Comments, *What's 'Liberal' About Hacking into the BNP?*, DAILY TELEGRAPH (London), Nov. 22, 2008, at 30, *available at* http://www.telegraph.co.uk/comment/columnists/samleith/3563694/Whats-liberal-about-hacking-into-the-BNP.html (regarding publication of personal information from the BNP membership list on Facebook).

185. *See 'BNP Membership' Officer Sacked*, BBC NEWS, March 21, 2009, http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/england/merseyside/7956824.stm (regarding the sacking of a police officer for being a member of the BNP); *Radio Host Exposed in BNP Leak is Axed*, LONDON EVENING STANDARD, NOV. 19, 2008, http://www.thisislondon.co.uk/standard/article-23589438-radio-host-exposed-in-bnp-leak-is-axed.do (regarding the sacking of a national talk back radio presenter); *Church Asked to Ban BNP Members*, BBC NEWS, Jan. 19, 2009, http://news.bbc.co.uk/2/hi/uk_news/7838280.stm (highlighting the fact that the Church of England Synod is considering banning clergy from joining the BNP after it was revealed that clergymen were members of the BNP).

186. *See BNP Members 'Targeted by Threats,'* BBC NEWS, Nov. 19, 2008, http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/politics/7736794.stm (regarding details of threats received by callers to a BBC radio programme); Ian Watson, *Privacy Issues for BNP Members*, BBC NEWS, Nov. 19, 2008, http://news.bbc.co.uk/2/hi/uk_news/politics/7737651.stm (regarding the security of BNP members in Northern Ireland and the Irish Republic); Iain Robinson, *Death Threats Follow BNP List*, THE SENTINEL, Nov. 20, 2008, at 11, *available at* http://www.thisisstaffordshire.co.uk/news/Death-threats-follow-BNP-list/article-488115-

neighbor of a BNP member was mistakenly petrol bombed.[187] Media sources reported that two persons were arrested and prosecuted with criminal offences under the Data Protection Act 1998, in a joint investigation with the Information Commissioner's Office, regarding the publication of the list.[188]

The second example involves the pharmaceutical corporation Pfizer. In 2007, the spouse of a Pfizer employee accessed his partner's work-related laptop by using the employee's username and password.[189] After he had gained access, the spouse installed an unauthorized software program which enabled access to a peer-to-peer file sharing network.[190] The installation of the software was done without the knowledge or consent of the corporation and was against Pfizer's employee policies.[191] The laptop held details of 17,000 Pfizer employees and the unauthorized software was configured in such a way that other members of the peer-to-peer network were able to access files containing Pfizer employee details.[192] Pfizer was able to determine that the personal information of 15,700 Pfizer employees had been accessed or copied by unknown members of the peer-to-peer network.[193] Pfizer was also asked a number of critical questions by the Attorney General of Connecticut, Richard Blumenthal regarding Pfizer's knowledge of the data breach and the delay in notification to

---

detail/article.html (regarding death threats received by a BNP local councilor); *Death Threats as BNP Members are Named*, CORNISH GUARDIAN, Nov. 26, 2008, at 22, *available at* http://www.thisiscornwall.co.uk/news/Death-threats-BNP-members-named/article-499803-detail/article.html (regarding death threats to Cornish BNP members).

187. *Police Probe BNP Link to Car Fire*, BBC NEWS, Nov. 21, 2008, http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/england/bradford/7741270.stm; Nico Hines, *BNP Member Says Family Safety at Risk After Car Explodes Outside Home*, TIMES ONLINE, Nov. 21, 2008, http://www.timesonline.co.uk/tol/news/uk/crime/article5204727.ece.

188. *Two Arrests over Leaked BNP List*, BBC NEWS, Dec. 5, 2008, http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/england/nottinghamshire/7768142.stm; *BNP List Arrest Pair are Bailed*, BBC NEWS, Dec. 10, 2008, http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/england/nottinghamshire/7775631.stm; Ian Johnston, *Two Held over BNP Member List Leak*, THE INDEPENDENT, Dec. 6, 2008, http://license.icopyright.net/user/viewFreeUse.act?fuid=OTg1NDg4Mg.

189. Jaikumar Vijayan, *Pfizer Waited Six Weeks to Disclose Data Breach*, INFOWORLD, July 18, 2007, http://www.infoworld.com/d/security-central/pfizer-waitedsix-weeks-disclose-data-breach-268.

190. Martin H. Bosworth, *Pfizer Keeps Data Breach Quiet*, CONSUMERAFFAIRS.COM, July 17, 2007, http://www.consumeraffairs.com/news04/2007/07/pfizer_data.html.

191. Pfizer, FAQs Related to Pfizer Data Breach: Introduction (2007), http://www.pfizer.com/contact/pfizer_data_breach_introduction.jsp (last visited Sept. 10, 2010).

192. Vijayan, *supra* note 189; John Leyden, *Pfizer Worker Data Leaked via P2P*, THE REGISTER, June 14, 2007, http://www.theregister.co.uk/2007/06/14/pfizer_p2p_data_leak/.

193. Vijayan, *supra* note 189.

its employees.[194] Pfizer replied in depth about the circumstances of the breach but offered no indication as to the reason for the delay in notification.[195]

The final example regards one of the most important and influential data breaches, the ChoicePoint incident. ChoicePoint was a data collection and storage company that held information on USA households and persons totaling nineteen billion records on US citizens.[196] ChoicePoint provided access to its databases for legitimate businesses for a subscription fee. At the time of the breach, ChoicePoint had 50,000 subscribing companies that included insurance agencies, banks, landlords and private detectives.[197] In February 2005, criminals posing as a small business applied to ChoicePoint for subscription to their information services. Once the criminals subscribed to ChoicePoint's information services, they were allowed to acquire the personal information of 163,000 persons including date of birth, social security numbers, and credit reports to be used for identity theft crimes.

The application forms necessary to access ChoicePoint's data were completed using false information which the company failed to realize because it had not implemented procedures that confirmed and authorized the identities of potential subscribers.[198] ChoicePoint later admitted that fifty business clients to whom it was selling data were fraudulent entities.[199] ChoicePoint simply did not have processes in place to identify and monitor unlawful users despite the fact that they had been previously notified by law enforcement authorities of

194. Letter from Richard Blumenthal to Bernard Nash, Esq., Dickstein Shapiro LLP, re Pfizer Security Breach (June 6, 2007) (on file with the State of Connecticut), http://www.ct.gov/ag/lib/ag/consumers/pfizerdatabreachletter.pdf.

195. Vijayan, *supra* note 189.

196. *See Choicepoint*, EPIC.ORG (Electronic Privacy Information Center, Washington D.C.), http://epic.org/privacy/choicepoint/ (last visited Sept. 10, 2010) (regarding the role of ChoicePoint as a data broker); Garcia, *supra* note 82, at 716 (stating that ChoicePoint collected personal information of consumers, "including names, social security numbers, dates of birth, bank and credit card account numbers, and credit histories, much of which is sensitive and not publicly available").

197. *See, e.g.*, Derek A. Bishop, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 SHIDLER J. L. COM. & TECH. 7 (2006) (regarding class actions against ChoicePoint); *see generally* Martin G. Bingisser, *Data Privacy and Breach Reporting: Compliance with Varying State Laws*, 4 SHIDLER J. L. COM. & TECH. 9 (2008) (regarding the actions of state attorney general's).

198. *See* P. N. Otto, et al., *The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information*, 5 IEEE SECURITY & PRIVACY 15, 18. (2007) (providing a detailed and critical overview of the incident).

199. *See* Garcia, *supra* note 82, at 716-17.

fraudulent activities arising from some of their subscribers.[200] ChoicePoint notified consumers of the incident pursuant to the California law and were subsequently charged with offences relating to the failure to provide adequate security and for making false and misleading statements about its privacy policy.[201] In total, eight hundred incidents of identity theft have been attributed to the ChoicePoint data breach.[202] ChoicePoint agreed to pay $US10 million in civil penalties and $US5 million in consumer redress to reimburse consumers for expenses due to identity theft. [203]

B. One Size Fits All Chains of Accountability

The author contends that both laws have a shared weakness because they are predicated on process-based chains of accountability that seek to provide legislative remedies within the bounds of designated roles involving providers, collectors and re-users of personal information. However, limitations emerge due to the simplistic nature of these chains, which no longer account for the complexities of personal information exchange and because remedial responses treat different concerns within the same constrained rubric of the accountability framework. The limits of both laws are illustrated when the three data breaches highlighted are examined in greater depth using Bennett and Raab's fallibility matrix,[204] which underscores that different types of privacy problems are essentially addressed in the same manner by both laws.

Bennett and Raab developed a simple four cell matrix to examine the source of privacy problems that arise through human and technological fallibilities and infallibilities.[205] The authors use the matrix to demonstrate that different types of privacy problems can occur within different cells. For example, Cell I contains most privacy

200. United States of America (for the Federal Trade Commission) v. ChoicePoint Inc., FTC File No. 052-3069 p. 13, (Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, January 26, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

201. *See* Samuel Lee, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*. 1 ENTREPRENEURIAL BUS. L. J. 125, 130 (2006).

202. Press Release, Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

203. *Id.* (outlining details of the settlement); *see also* Garcia, *supra* note 82, at 716.

204. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 25 (regarding the conceptual basis of the matrix).

205. *Id.*

problems as they involve both human and technological fallibilities such as the excessive collection of personal information.[206] Cell II details a different type of situation, namely, where there are no technological or structural problems and the privacy problem occurs due solely to the "workings of human agency."[207] Cell III covers opposite situations to Cell II where a technological or structural issue, rather than a case of human error, gives rise to privacy problems, such as a deficient data processing system or a malicious hacking attack.[208] Finally, Cell IV refers to situations in which both human agents and technological structures perform adequately but this level of performance creates surveillance-related concerns.[209] The last cell is of less concern to this article as the focus on data breaches naturally requires an examination of personal information leakage. However, the remaining three cells are instructive because they highlight that data breaches and therefore information privacy problems arise in different contexts, as outlined in Figure 2 below.

Bennett and Raab also contend that each fallibility axis is a continuum and thus the positioning of privacy problems can be related to any part of each cell.[210] However, in practice, it is likely that most positions will be found nearer the meeting point of the axes rather than the corners of each cell because "few human agents, and few technical systems, are either perfect or imperfect."[211] The three example breaches show that, even though each breach can be separated into different cells, they nonetheless share overlapping features that make each breach relatively similar. For example, it could be argued that all data breaches involved issues of ineffective security which would tend to suggest a technological or structural failing. It is not surprising to find that each breach locates towards the center of the matrix rather than the periphery. Nevertheless, each data breach highlights that information privacy problems originate in different ways.

206. *Id.* at 26-27.

207. *Id.* (citing examples such as "wrong inferences or conclusions from outputs of data produced by the system, whether because of inadequate training, the biases inherent in the pursuit of certain organizational goals, the pressures of reward systems in the organization").

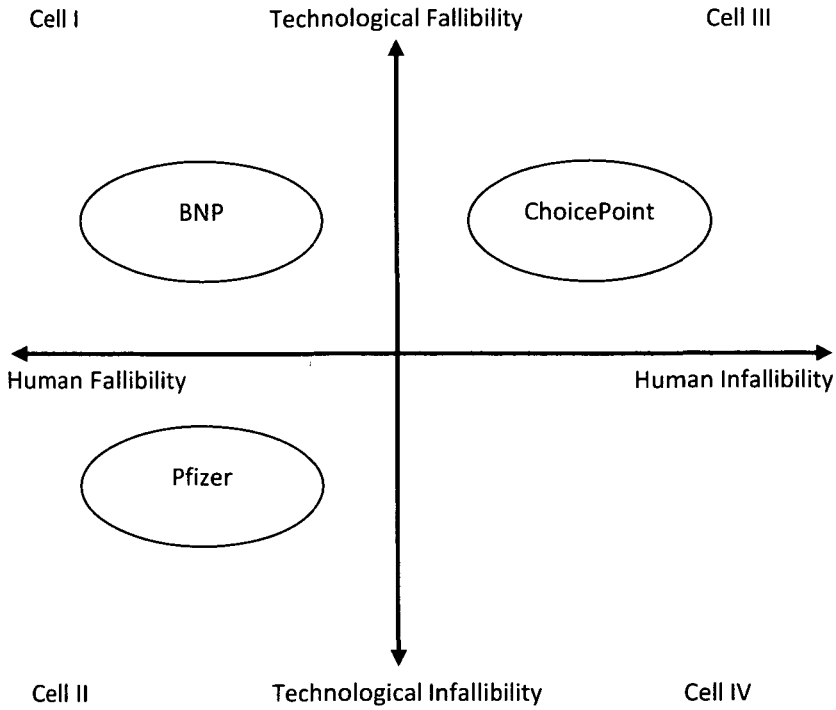
208. *Id.*

209. *Id.*

210. *Id.*

211. *Id.* at 26.

Fig. 2 – Application of Illustrative Data Breaches to Bennett and Raab's Fallibility Matrix



The BNP data breach can be located in Cell I because it entails both technological and human failings. First, human infallibilities arose because unnecessary and inaccurate personal information was collected from BNP members and even non-BNP members. Second, technological and structural fallibilities occurred because the disgruntled employee was able to easily acquire and copy the complete membership list without authorization and remove it from the confines of the BNP's organizational structure. The Pfizer data breach, on the other hand, gives rise to a different problem, which locates it in Cell II of Bennett and Raab's matrix. The initial data breach arose because the employee's spouse installed unauthorized software which enabled unknown third parties to access and acquire employee personal information without authorization. Accordingly, there was no technological or structural fallibility, and the problem

originated solely from the actions of the employee's spouse who was able to bypass technological protections. The ChoicePoint data breach is an example of a Cell III type privacy concern as it originated from a structural and technological problem rather than human fallibility. In this case, it was ChoicePoint's procedures which were at fault. In fact, if ChoicePoint had completed a background check on the criminals, it would have found a link between one of the applicants and previous frauds involving social security numbers according to its own records.[212]

The application of Bennett and Raab's matrix to these three data breaches is helpful because it demonstrates that data breaches, as information privacy problems, emerge in different ways and contain different contexts. For example, only one of the breaches, the ChoicePoint incident, is directly related to identity theft issues. The BNP data breach, while not giving rise to identity theft issues, clearly gave rise to different forms of harm such as the petrol bombing attack that took place. The Pfizer data breach did not materialize any actual identity theft or other related harms but certainly had the potential to do so.213 However, while the three data breaches have different contexts, all of them involve the insertion of outside third parties that are integral to the emergent privacy problems.

The BNP data breach occurred because of the disgruntled employee's initial unauthorized acquisition but the real 'privacy problem' was the subsequent re-use of the membership list and its publication on the internet by third parties ulterior to the breach. The Pfizer breach, like the BNP breach, demonstrates a layered, emergent problem. The installation of the peer-to-peer software by the employee's spouse gave rise to the initial privacy concern. However, it is the second unauthorized acquisition by third parties unknown to the breached organization that gave rise to the actual problem. The ChoicePoint data breach is somewhat different in character to the BNP and the Pfizer data breaches because there is less of an emergent problem involving stages of unauthorized access. There was not an initial unauthorized act that gave rise to a series of subsequent and

212. *See* United States of America (for the Federal Trade Commission) v. ChoicePoint Inc., FTC File No. 052-3069 p. 13, (Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, January 26, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

213. *Data Security Breach at Pfizer Affects Thousands*, TechTarget, Sep. 5, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1270736,00.html. *See, e.g.*, Blumenthal, *supra* note 194) (regarding proposed actions for Pfizer to take to mitigate the possibilities of identity theft).

more serious unauthorized acts. Instead, the data breach was mistakenly authorized by ChoicePoint due to the failings of its own security systems. As such, only one act of unauthorized acquisition took place that involved a different type of ulterior third party, identity theft criminals.

These three incidents show that data breaches involve different types of privacy problems. However, both information privacy and data breach notification laws deal with those problems in a 'one-size fits all' fashion founded upon narrow chains of accountability and one-dimensional remedies that provide limited help or real redress. For example, previous work has highlighted the limits of information privacy law in dealing with the BNP data breach.[214] The analysis of this data breach within the rubric of investigating privacy invasive geo-mashups highlighted the limits of information privacy law. The principle reason being is that information privacy law is predicated on predictable, binary chains of accountability between personal information providers, collectors, and re-users. However, in this incident the binary relationship between the data provider and the data re-users (Wikileaks and the geo-mashup creators) does not materialize, and thus there is no form of redress available against these parties for individual BNP members whose personal information has nonetheless been disclosed by them.

A similar concern arises with the Pfizer data breach where there is no relationship at all between the provider of personal information (Pfizer's employees) and the subsequent re-users (the peer-to-peer members) other than a tangential link via the errant spouse. However, it is clear that these re-users can give rise to serious potential threats even though there is no direct relationship. Information privacy law seems to operate more effectively with the ChoicePoint data breach because this type of breach more readily accords with the imposition of security protections for personal information within a readily identifiable and largely institutionalized focus.[215] It is clearly arguable that ChoicePoint failed to implement adequate security measures in relation to the storage of personal information which is a key element of most information privacy laws.[216] The outside third party in that

214. Burdon, *First Generation Laws*, *supra* note 17, at 35-38 (regarding the ineffectiveness of privacy protections in relation to publication on the internet).

215. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 35 (stating that fundamental classifications under information privacy law are predicated on an institutionalized basis).

216. *See, e.g.*, BYGRAVE, *supra* note 58, at 67 (regarding the role of information security as a key principle of information privacy laws).

breach is therefore considered in information privacy laws as being a reasonable eventuality unlike the third parties in the other two data breaches.

Accordingly, the application of information privacy laws makes it difficult to cope with the insertion of most third parties into the contextual mix of privacy problems even though the transition from binary to multiple information relationships is now an everyday part of life in the information society.[217] Information privacy laws overtly focus on the process of personal information exchange rather than the relationships or social contexts involved in that process.[218] The law's focus on process has the benefit of providing a manageable and implementable set of fair information principles that can readily translate to a regulatory mechanism but it relegates the protection of privacy to limited circumstances and thus greatly reduces the potential scope for legal redress or remedial action. The inherently reductionist scope of information privacy law[219] has created the situation in which even legislative rights granted through the law are nonetheless limited because they are based on mechanistic processes of personal information exchange.[220]

Data breach notification laws, on the other hand, have been developed to tackle a specific substantive issue regarding the mitigation of identity theft risks arising from specified misuses of personal information. In effect, they are less concerned about the process of information exchange and pay lesser heed to regulating the activities of personal information collectors and re-users by giving personal information providers a set of limited rights. Accordingly, data breach notification laws do not suffer from the same sort of difficulties pertaining to chains of accountability due to their limited focus. If an organization loses control over an individual's personal information, then they have to notify that individual.[221] If a chain of

217. Burdon, *First Generation Laws*, *supra* note 17, at 36.

218. *See, e.g.*, BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 35 (stating that after 30 years of information privacy law there is still very little known about the needs or requirements of 'data subjects').

219. *See* David Lindsay, *An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law*, 29 MELB. U. L. REV. 131, 165 (2005) (regarding the role of excessive rationalization to minimize the scope of information privacy law).

220. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 147 (stating "[information privacy] laws have typically provided procedural rules and devices without greatly tackling many substantive issues concerning the processing of personal data in contemporary society").

221. Dealing with a Data Breach, Federal Trade Commission,

accountability exists, it is a rudimentary one between an organization and an individual regarding the notification of unauthorized acquisition of personal information. However, they do share the same weakness as information privacy laws because they provide a one size fits all remedy.[222]

The three data breaches illustrated in this section emit different types of problems, demonstrate different types of causes and involve different types of parties who have different motives. Despite these differences, the only remedial response available is notification of the incident. Schwartz and Janger have highlighted a number of criticisms of this remedial aspect of data breach notification laws.[223] Notification letters are problematic due to the context in which they are used. For example, ChoicePoint's notification letters attempted to minimize the extent of the breach and were concerned with damage control to the company rather than the provision of accurate and meaningful information to individuals.[224] ChoicePoint was also singled out for significant criticism as their notification letter attempted to sell the company's credit reference products to those persons who were being notified.[225] Notification fatigue may also be a prominent concern as individuals appear to treat notification letters as another form of marketing material and do not read them.[226] Notification may therefore provide a limited remedy.

A greater focus is needed on the context of each individual breach and the remedies appropriate for that breach. For example, in the BNP breach,[227] it is questionable whether notification of the breach would have made any difference given the public nature of the membership lists re-publication. Instead, removal of the published information was required although this would have been practically

---

http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html (last visited Sept. 14, 2010). *See, e.g.*, St. Amant, *supra* note 81, at 511 (stating that the Californian law does not require an actual breach or an identity theft element to oblige notification).

222. *See, e.g.*, Bill Lane, et al., *Stakeholder Perspectives Regarding the Mandatory Notification of Australian Data Breaches*, 15 M.A.L.R 149, 164 (2010) (presenting findings of Australian research that questions the effectiveness of remedies provided by data breach notification laws).

223. Schwartz & Janger, *supra* note 86, at 952.

224. *Id.*

225. *Id.* at 953.

226. *See* PONEMON INSTITUTE, NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION (2005) (regarding a survey of individuals who received notification letters and their subsequent response to those letters).

227. It is of course acknowledged that the breach was not required to be notified under UK law.

very difficult given the extent the list was copied and re-used. Accordingly, as Schwartz and Janger highlight, a more emphasized focus on coordinated responses to data breaches is required that goes beyond simple and blunt notification strategies.[228] However, to do so would require a deeper contextual analysis that is conducted on a case-by-case basis. This contextual analysis may be difficult to implement from a regulatory perspective given the limited role that data breach notification is intended to fulfill because both data breach notification and information privacy laws have an overt focus on the regulation of information which manifests in the mitigation of limited social harms.

C. Information Based Focus and Limited Harms

Both data breach notification laws and information privacy laws are designed to regulate certain types of information. However, there are differences with regard to the inclusion or exclusion of context based approaches. Information privacy has a wider outlook that generally builds on context dependency and is flexible about what information will be regulated.[229] However, while data breach notification laws also regulate certain types of information they do so from a context independent approach that seeks to negate the application of context-based analysis.[230] The reason that both laws use different types of information based regulation mechanisms is due to their different purposes as highlighted above. Data breach notification laws regulate a specific type of information to mitigate a specific problem whereas information privacy laws regulate a wider type of information for a potentially wider purpose. As such, both laws regulate specified types of information to preclude certain harms, but the harms that they seek to preclude are relatively limited as demonstrated below.

Information privacy laws cover personally identifiable information that is generally classified as "personal data"[231] or "personal information."[232] The broad purpose of information privacy

228. Schwartz & Janger, *supra* note 86, at 960.

229. *See, e.g.*, Prins, *supra* note 39, at 247-49 (regarding the difficulties in assigning what is personal information under data protection laws within the broad rubric of economic notions of privacy as property).

230. Schwartz & Janger, *supra* note 86, at 926-27. *See* Needles, *supra* note 15, at 281 (regarding the purpose of data breach notification as "the loss of control over a particular type of data which can cause a "measurable economic harm" in the form of identity theft).

231. Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) (EC).

232. S6(1) PRIVACY ACT 1988 (Cth) (Austrl.)

laws is reflected in how personal information is classified. A key component of information privacy law is that personal information will be construed expansively,[233] and thus the classification of personal information is potentially a complex task. The complexity generates from the tacit acceptance of the need for context dependent approaches in classifying personal information that go beyond the information itself and require an examination of the social context of information generation.[234] For example, the definition of personal information in the Australian Privacy Act has two distinct elements.[235] The first element states that personal information is information that makes an identity apparent, and the second element is information from which an identity is reasonably ascertainable.[236] The first element is a context-independent approach because there is no recourse to the context of information generation because the information itself is enough to enable identity. However, the second element offers a different approach. It allows for the situation in which information can be combined with other information to enable identity. Accordingly, the second element relies heavily on social context and this is seen as an integral element of Australian privacy law.[237]

The issue of harm negation is a key element in the use of context dependent approaches to the classification of personal information. Harm in the eyes of the Australian law is the revealment of identity.[238] Accordingly, the law takes an open approach to what

---

233. *See, e.g.*, ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 4/2007 ON THE CONCEPT OF PERSONAL DATA. (2007) (confirming that a "wide notion" of personal data is to be applied).

234. *See, e.g.*, BOOTH, *supra* note 138 (providing models of how data protection authorities conceptualize personal information both from a context independent and dependent approach); Burdon & Telford, *Conceptual Basis*, *supra* note 138 (applying the models put forward by the Booth Report to Australian legislation); WACKS, *supra* note 24, at 20 (regarding the normative and descriptive role of personal information).

235. S6(1) PRIVACY ACT 1988 (Cth) (Austrl.) ("[P]ersonal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.").

236. *Id. See* Burdon & Telford, *Conceptual Basis*, *supra* note 138, at 12 (describing both elements within the context of Australian privacy law).

237. *See* KAREN CURTIS, Speech to the Australian Corporate Lawyers Association on Privacy and 'Walking the Line,' Canberra, (29 February 2009), at http://www.privacy.gov.au/materials/types/download/9473/7038 ("This idea of what can be 'reasonably ascertained' is significant. Clearly, whether an individual's identity can be ascertained depends on the context in which the information is held.").

238. *See* Burdon & Telford, *Conceptual Basis, supra* note 138, *at* 17-20 (regarding a review of Australian legislation and confirming the centrality of identity revealment in

constitutes personal information because the harm and the use of such information are directly linked. However, it is acknowledged that not all information privacy laws have an identity-related focus and some laws require a type of privacy-related harm, above and beyond, the revealment of identity.[239]

Data breach notification laws attempt to mitigate the specific harm of identity theft and they do so by regulating specified forms of personal information in combination with other information. For example, although the California law requires notification upon the unauthorized acquisition of personal information, the definition of personal information is different to those found in most comprehensive information privacy laws because it seeks to negate a context dependent analysis. As such, personal information under the California law is

> [A]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[240]

The California law is therefore solely concerned with combinations of personal information that can be used to give rise to identity theft harms. Some US state-based laws have attempted to expand definitions to include other identifying information, for example, biometric information,[241] passport number[242] and account passwords or other access codes.[243] The North Carolina law has one of the most expansive definitions relating to "identifying information" that also includes digital signatures, parents' former legal surname[244]

Australian privacy law).

239. *See, e.g.*, BOOTH, *supra* note 138, at 95-102 (regarding different conceptualizations of harm).

240. CAL. CIV. CODE § 1798.29(E). *See also* Bingisser, *supra* note 198 (regarding an overview of differences).

241. *See, e.g.*, NEB. REV. STAT. §§ 87-801(5)(e) (2006).

242. *See, e.g.*, MONT. CODE ANN. § 30-14-1704 (2006) (5)(B)(4); OR. REV. STAT. § 646A.600 (2007).

243. *See, e.g.*, ALASKA STAT. § 45.48.010 (Michie 2009); D.C. CODE ANN. § 28-3851 (2007); GA. CODE ANN. §§ 10-1-911 (2005); IOWA CODE § 715C.1 (2008); N.C. GEN. STAT. §§ 75-60 (2005); ME. REV. STAT. ANN. 10, §§ 210-B-1346 (West 2007); 9 VT. STAT. ANN. §§ 2430 (2007).

244. *See also* N.D. CENT. CODE §§ 51-30-01 (2005).

and email addresses, amongst others.[245] The Texas law recognizes both "personally identifying information"[246] and "sensitive personal information."[247] The former can be information that does not require cross-referencing with other information to trigger notification of a data breach whereas the latter requires the combination of personal information and other identifying details. Likewise, the New York law incorporates both "personal information"[248] and "private information,"[249] and the latter is the type of information normally covered by data breach notification laws. The purpose of the different definitions in the New York law is to clearly identify what will be viewed as personal information for combination with private information to create a specified sub-set of regulable information. As such, all of these laws specify the types of information or combinations of information that when breached could give rise to an obligation to notify. What constitutes personal information within the rubric of data breach notification is therefore deliberately constrained.[250]

Data breach notification proposals that have been put forward in comprehensive information privacy laws also have a context independent approach as to what information will trigger notification. For example, the data breach notification proposal put forward by the Australian Law Reform Commission (ALRC) uses a new form of information called "specified personal information" that is designed to limit the broad ranging definition of personal information in the Privacy Act for data breach notification purposes. Specified personal information prescribes combinations of information that would, "when acquired without authorization, give rise to a real risk of serious harm requiring notification."[251] According to the ALRC, such

245. N.C. GEN. STAT. §§ 75-60 (2005).

246. TEX. BUS. & COMM. CODE § 48.002(1) (2008).

247. *Id.* at § 48.002(2).

248. N.Y. GEN. BUS LAWS §§ 899-aa (2005) §1(a) ("Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person").

249. *Id.* at §1(b) ("Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password").

250. *See* St. Amant, *supra* note 81, at 526 (criticizing this approach and calling for flexible definitions of personal information similar to comprehensive information privacy legal regimes).

251. AUSTRALIAN PRIVACY LAW AND PRACTICE, *supra* note 6, at 1693.

information is likely to include an individual's name and address in combination with other identifying information that could enable a person to commit an "account takeover" or "true name fraud" while recognizing that other harms can also arise.[252] The ALRC's approach to information that could oblige notification is in some respects similar to that of US state-based data breach notification laws as it is largely founded upon a context independent approach to classifying sensitive personal information.

The EU has taken a different approach in the e-Privacy Directive.[253] The e-Privacy Directive differs substantially from the purpose of US data breach notification laws as it has a much wider ambit about the type of situations and the sort of information that will trigger notification of a data breach.[254] However, it is limited in the sense as it only covers data breach incidents in the telecommunications sector.[255] The e-Privacy Directive simply states that notification is required where there is a breach of network security that lies beyond the provider to remedy.[256] The e-Privacy Directive is potentially more expansive than its US data breach legislative counterparts because it does not require a specified type of information to trigger notification. The European Commission has recently addressed this point by putting forward a new version of the e-Privacy Directive which amends the existing security breach notification requirements.[257] A provider of a publicly available electronic communications services will now have to notify a competent national authority about a personal data breach.[258] The definition of a personal data breach is "[a] breach of security leading to the accidental or unlawful destruction, loss, alteration,

252. *Id.* at 1694.

253. Council Directive 2002/58/EC.

254. *See, e.g.*, Preston & Turner, *supra* note 64, at 463-64 (commenting on the "organic development" of EU privacy legislation and the application of general data protection rules to the telecommunications sector in the e-Privacy Directive).

255. *Id.*

256. Council Directive 2002/58/EC, Art. 20 ("Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network.").

257. *See Commission Proposal for a directive of the European Parliament and of the Council amending Directives 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation*, at 2 COM (2007) 698 [hereinafter *Updated E-Privacy Directive*] (adopted at the GAERC Council of 26/10/2009).

258. *Id.* at 33.

unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."[259]

The e-Privacy Directive now focuses mandatory data breach notification on situations that (a) relate to personal data, (b) involve specified unauthorized uses of personal data, and (c) personal data is stored or processed in connection with a publicly available electronic communications service.[260] Nevertheless, the definition of a personal data breach is still reliant upon the definition of personal data in the Data Protection Directive.[261] The EU consequently differs from both the US and the Australian approaches to data breach notification because it does not include a specifically modified definition of personal data (or information) for the purposes of data breach notification. Moreover, the definition of personal data under Article 2(a) is to be construed expansively rather than prohibitively and therefore has a fundamentally context dependent element.[262]

A context independent approach can have some benefits because it is possible to predict what information will constitute personal information as it is pre-defined by regulatory authorities.[263] However, an overt focus on types of information to stimulate regulatory activity can produce anomalies because it forsakes a contextual analysis of information generation. For example, some data breaches would not be covered even though they could have significant ramifications. This point is demonstrated by the BNP data breach.[264] There is little doubt that the BNP data breach should meet most of the requirements for notification under a data breach notification law as there was an unauthorized acquisition of personal information and there were

259. *Id.*

260. *See, e.g.*, Burdon, et al., *Mandatory Notification of Data Breaches, supra* note 5, at 127 (regarding the potentially problematic application of data breach notification in the Directive).

261. *See* Council Directive 95/46, art 2(a), 1995 O.J. (L 281) (EC) ("'[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.").

262. *See generally* ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 4/2007, *supra* note 233.

263. *See* BOOTH, *supra* note 138, at 12 (emphasizing that a "context independent" approach facilitates consistency because it would not require analysis outside of the data at issue).

264. *BNP members 'targeted by threats,'* BBC News, Nov. 19, 2008, http://news.bbc.co.uk/2/hi/uk_news/7736794.stm.

clearly harms and risks arising from the breach. However, under most data breach notification laws, the breached organization would not have to notify an individual about the breach because the type of information that was breached would not necessarily trigger a notification requirement.

In the BNP data breach, the type of personal information breached did not entail personal information that would necessarily enable identity theft, such as a credit card or bank account number. Thus, under US state-based laws, there would not be a legal requirement to notify because the BNP breached data would not meet the determinant threshold required for publication, namely, that the breached data gives rise to a risk of identity theft. The same is less so with regard to the ALRC's proposal as it acknowledges that wider harms to identity theft are applicable. However, and somewhat perversely, under Australian information privacy law, the Internet is construed as a generally available document and the Privacy Act would not have applied because personal information published would be construed as a generally available record and thus is exempt from the Act.[265]

The BNP example shows the limits of an overt focus on the types of personal information that is predicated on a context independent approach which seeks to minimize the complexities of social context as part of the fulfillment of legislative obligations. Data breach notification laws, regardless of whether sectoral or comprehensive based, have such a limited view of what constitutes harm that they preclude a range of data breaches, like the BNP data breach, even though material harms and risks arose to those persons whose information had been accessed without authorization. This highlights the weaknesses of analysis that is focused predominantly

265. The ALRC examined whether personal information held within a generally available publication should be regulated under the Privacy Act. Currently, the Act only covers personal information held in records and a generally available publication, such as most public registers or telephone address books, are classed as a record so they are not covered within the auspices of the Act. As regards publication of personal information on the Internet, the determining factor to decide whether a publication is generally available online is "whether access to that publication [e.g. a website] can be obtained by public." As such, a website that has encryption and password protections is not considered generally available and therefore may be subject to the Privacy Act, whereas a website without such protections is not subject to the Act because it is a publication that can generally be obtained by the public. The ALRC contended that it was not appropriate to enforce greater restrictions of the use of personal information on the Internet by tightening regulation of personal information held in 'generally available publications', e.g. websites. However, the ALRC stated that both organizations and agencies should be encouraged to put restrictions on the publication of personal information in electronic form. *See* AUSTRALIAN LAW & PRACTICE, *supra* note 6, at 462.

on information and the process of information exchange and not the context of which the information is used.[266] Even the e-Privacy Directive, which has a more expansive, context dependent approach to the classification of personal information, would encounter problems with this data breach[267] due to the fact that the Directive only covers organizations in the telecommunications sector[268] and would therefore have not applied to the BNP.

Potential weaknesses of data breach notification law that is founded on a sectoral approach can still exist when implemented within comprehensive frameworks. The effect of a purely context independent approach is to minimize the scope of data breach notification either by developing restrictive forms of personal information or by reducing the scope of coverage to particular sectors.[269] However, this minimization can reduce the effective potential of data breach notification because it provides bounding limits to the obligation to notify. The definition of personal information in the Australian Privacy Act[270] demonstrates that a context independent and dependent approach can work together but that does not mean that the former can be imposed upon the latter without any significant consequences. Data breach notification can work in comprehensive information privacy frameworks, but it will produce anomalies if it is implemented from a context independent perspective. The complex issue of contextualization is thus fundamental to the effectiveness of regulatory remedies in relation to data breaches.

V. INTRODUCING CONTEXTUALIZATION

The above analysis highlights concerns relating to the underlying approaches of both laws that seek to minimize the role of social context. Consequently, the legislative requirements of both laws focus upon restricted notions of harms, confined types of regulable information and one size fits all conceptions of how problems emerge and how they are to be remedied. However, the inclusion of a wider contextual analysis into the application of both laws produces a different perspective. First, it highlights that information privacy law

266. *See, e.g.*, Solove, *Conceptualizing Privacy*, *supra* note 34, at 1110 ("The theory's focus on information, however, makes it too narrow a conception, for it excludes those aspects of privacy that are not informational.").

267. UPDATED E-PRIVACY DIRECTIVE, *supra* note 258.

268. *Id.*

269. Burdon & Telford, *Conceptual Basis*, *supra* note 138.

270. Privacy Act, 1988, pt. III, div. 3, 16B (Austl.).

needs to pay greater heed to issues of privacy rather than issues of personal information management. Second, it highlights that data breach notification law should be considered as part of a wider concern that relates to the societal use of critical information infrastructures that entail the protection of personal information.

A. The Contextual Element

The social context of information generation and provision is a latent but ever-present component of information privacy that is directly or indirectly recognized by different laws.[271] For example, Bennett and Raab contend that the content and provision of a privacy right is inherently dependent on the context of social application and is thus applied subjectively by individuals to their own circumstances.[272] Allen offers a different view of information privacy and social context that is intimately bound with the creation, development, and maintenance of social relationships.[273] Privacy is "down time" that provides the space for reflection and thus allows individuals to prepare themselves for their wider social responsibilities within the context of their own lives.[274] Schoeman also outlines that the wider concept of privacy is part of a "historically conditioned, intricate normative matrix with interdependent practices" and is best understood when viewed contextually.[275] Privacy as a social practice thus shapes individual behavior in conjunction with other social practices and is "central to social life."[276] Likewise, Moor and Tavani also acknowledge the importance of "situations" in deciding when an individual has a condition that is equivalent to privacy.[277] However, the notion of a situation is characterized as "deliberately indeterminate or unspecified" so that it can be construed

271. *See* BOOTH, *supra* note 138, at 10-11 (highlighting a context dependent approach to the identification of personal information is a key element of some information privacy laws).

272. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 9 ("But for the most part, the content of privacy rights and interests have to be defined by individuals themselves according to context.").

273. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999).

274. *Id.* at 739-40 (The value of privacy therefore lies in "the context in which individuals work to make themselves better equipped for their familial, professional, and political roles."); *See also* FERDINAND DAVID SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (CAMBRIDGE UNIVERSITY PRESS. 1992) (regarding the role of privacy in the balancing of social freedoms and an individual's need to be part of a "human context").

275. SCHOEMAN, *supra* note 274, at 137.

276. *Id.*

277. Moor, *supra* note 35, at 30 (stating privacy is normatively prevalent if an individual or group is protected from intrusion, interference and access by others).

in a number of different ways in circumstances that would normally be regarded as private.[278]

One of the most recent and perhaps fullest accounts of the importance of context in the regulation of information privacy is Nissenbaum's *Privacy in Context*[279] which outlines and expands the theory of Contextual Integrity.[280] Nissenbaum puts forward an analytical framework to examine potential privacy concerns arising from the introduction of new technologies or technological structures principally involving the use of personal information.[281] Privacy is sufficiently important to the continued existence of social and political life that it cannot be compartmentalized and reduced in social importance.[282] Instead, contextual integrity represents privacy as a "delicate web of constraints,"[283] relating to flows of personal information that balance the multiple political and social spheres of human life. An attack on individual privacy is therefore an attack at the "very fabric of social and political life."[284] Privacy in this regard is not a claim regarding an individual's control of their personal information but rather entails a right to appropriate flow of personal information which is systematically grounded in the characteristics of social situations.[285]

Contextual Integrity is therefore based on social context and gains expression through its primary concept, context-relative informational norms. These norms govern entrenched expectations that govern flows of personal information in everyday life. Accordingly, a breach of privacy under the theory of Contextual Integrity equates to a violation of an established informational norm.[286] These norms are characterized by the following four key parameters.[287] *Contexts* provide a backdrop for norm development and feature an array of components[288] that abstractly represent the

278. Tavani, *supra* note 18, at 10 (explaining the role of Moor and Tavani's Restricted Access/Limited Control (RALC) theory).

279. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford Law Books 2010) [hereinafter NISSENBAUM, PRIVACY IN CONTEXT].

280. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

281. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 6-7.

282. *Id.* at 128.

283. *Id.*

284. *Id.*

285. *Id.* at 129.

286. *Id.* at 140.

287. *Id.*

288. *Id.* at 132 (defining the components as canonical "activities, roles, power structures,

experienced social structures of everyday life.[289] *Actors* are those participants involved in direct context of information exchange: senders and receivers of information and information subjects.[290] However, the types of relationship that each party has with each other is not fixed and is acknowledged that both individuals and organizational representatives can have different capacities in different situational circumstances.[291] *Attributes* refer to the type or nature of the information in question.[292] For example, the same type of information can have different meaning or application in different contexts.[293] Finally, *transmission principles* provide a constraint on the flow of information from party to party in a given context by stipulating terms and conditions which govern the transfer of personal information.[294]

These parameters are embedded within informational norms which in turn are embedded within different social contexts.[295] Flows of information are intrinsic to human society and informational norms regulate these flows within the context of socially expected information uses and within socially specified situations. As such, different parameters come to the fore in different social contexts and in the guise of different privacy-related problems. For example, in a context of information exchange amongst friends, there is expected transmission principles, namely that the personal information exchange is usually volunteered freely and there are certain trust-based expectations about how that information will or will not be used. However, the medium of exchange can impact upon friend-based transmission principles especially in situations involving a broader and thus less controlled transmission of personal information.[296] Likewise, the provision of the exact same personal

---

norms (or rules) and internal values (goals, ends, purposes)").

289. *Id.* at 134.

290. *Id.* at 141.

291. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 143. Nissenbaum contends that an actor in one situation may not act in the same way as in another. For example, the difference between an actor in a "businessman to employee" relationship compared to a "parent to child" relationship. Accordingly, the capacity within which an actor may act has an "innumerable number of possibilities."

292. *Id.* at 144.

293. *Id. See, e.g.*, Burdon, et al., *Encryption Safe Harbours, supra* note 72 (contrasting the different requirements for the loss of personal information involving different types of data breach).

294. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 145.

295. *Id.*

296. *Id.* at 145-46 (describing the characteristics of friend-based transmission principles as voluntary sharing of information, in combination with locally relative prohibitions on

information is likely to vary between the context of a patient to doctor relationship during a medical consultation compared to an interviewee-interviewer relationship in relation to an employment application. The analysis of informational norms and component parameters are best conceived as juggling balls[297] that move in sync with different emphases placed on different balls depending on the social context involved and the privacy concern emanating.

The introduction of contextualization consequently adds a sophisticated and multi-dimensional element to conceptualizations of 'privacy problems.' Nissenbaum developed the theory of Contextual Integrity as a "framework for determining, detecting, or recognizing when a [information privacy] (sic) violation has occurred."[298] To do so requires a comparison between entrenched and novel practices to adduce whether there has been a violation of context-relative informational norms.[299] *Privacy in Context* is a valuable addition to the literature in that regard as it cements the importance of contextualization in the examination of concerns relating to the provision, protection and use of personal information. However, Nissenbaum acknowledges that much work has yet to be undertaken about how Contextual Integrity can apply to existing information privacy legal regimes, especially comprehensive frameworks.[300]

The purpose of introducing Nissenbaum's work into this article is not to provide a framework for specifically assessing the weaknesses of information privacy and data breach notification laws but rather to reinforce the importance of applying social context to laws that govern the protection of personal information. The recognition that information privacy issues have a contextual element is integral because it focuses greater attention to key foundation stones, namely, social relationships, expectations of social and legal norms, and the differing, subjective values of privacy that emanate in different guises and in different social circumstances. Privacy

information use which thus provide confidential settings for sharing information between friends). Accordingly, the provision of personal information directly between an individual and other friends via email and one via open Facebook pages impacts upon the applicability of friend-based transmission principles. The prospect of uncontrolled, wider distribution may in itself act as a factor upon the release of information because there is less control over transmission principles.

297. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 145.

298. *Id.* at 148.

299. *Id.* at 148-49.

300. *Id.* at 238. Nissenbaum suggests that her theory of contextual integrity may be more suited to sectoral frameworks because "it embodies informational norms relevant to specific sectors, or contexts, in the law."

regulation has many singular facets that involve diverse parties that have dissimilar values relating to the protection of privacy, both at a societal and individual level. The protection of personal information is consequently an essentially contestable issue and is determined in fluid rather than static environmental circumstances. Laws that involve the protection of personal information need to be cognizant of the wider social contexts involving the creation, exchange, and re-use of personal information. However, as highlighted in this article, both information privacy and data breach notification laws forsake a context dependent approach and focus on deterministic modes of regulation that overtly focus on specified types of information and management processes. The final sub-sections of this article incorporate ideas of contextualization to suggest new courses of action.

B. More Privacy, Less Information

The introduction of a contextual analysis assists to highlight that information privacy problems in relation to data breaches are not simply related to a loss of control over personal information. Instead, problems emerge from the breakdown of social relationships and these relationships vary from context to context and data breach to data breach. For example, the three illustrative data breaches employed in this article show that information privacy problems involve auxiliary third parties that are typically beyond the accountability framework of information privacy law. The BNP data breach[301] showed that the actual privacy problem was exacerbated by the advent of geo-mashup creations that not only increased the number of generative sources available but also provided a different context on how the list was used.[302] The Pfizer data breach[303], on the other hand, involved two third parties ulterior to the context of personal information provision, storage, and use: the Pfizer employee's spouse and the peer-to-peer users. Finally, the ChoicePoint breach[304] involved identity theft-related criminals that were able to acquire individual's personal information due to the corporation's failure to provide adequate security.

The application of a contextual analysis, especially within the

301. *See* Burdon, *First Generation Laws*, *supra* note 17, at 12.

302. *See, e.g.*, *id.* at 37 (outlining the role of geo-mashup creation in the data breach).

303. *See* PFIZER, *supra* note 192.

304. *See* P.N. Otto, et al., *supra* note 199.

framework of Bennett and Raab's infallibility matrix,[305] demonstrates that data breaches as information privacy problems are predicated upon multiple rather than binary relationships and that the mechanics of privacy-related problems arising from data breaches can manifest outside the chain of accountability created by information privacy law. Moreover, information privacy laws find it difficult to acknowledge the importance of multiple relationships in regard to data breaches because information privacy law is postulated on the regulation of information management processes involving defined parties. Accordingly, the issue is not about the length or strength of an accountability chain between singular parties. Rather, the issue regards how information privacy law attempts to identify and reconcile situations that are deemed to be 'privacy problems.' It is this deeming and reconciliation that is the ultimate limitation of information privacy law because it is management processes rather than social relationships that are deemed to be the problem. Regulatory remedies therefore focus on the provision of limited rights of control or access to that process as opposed to the provision of remedies to actual privacy concerns. Thus, for example, a BNP member has no redress against a geo-mashup creator and a Pfizer employee is in the same position against a member of a peer-to-peer network.

However, the ChoicePoint data breach provides a different perspective as it involves an ever-present figure that is partially recognized by the security principles of information privacy law—the computer hacker or identity theft criminal. The security principles of information privacy laws require organizations to maintain levels of adequate security regarding the storage and transfer of personal information.[306] An individual who provided personal information to an organization was reassured that their personal information would be secured. Expectations are such now that, if an organization has a database of personal information, that organization then must expect an unauthorized attempt to access or acquire it. This is a new information security reality in our information society. Including the hacker/identity theft criminal as an ever-present third party within the contextual situation of personal information exchange therefore brings a third party into play that is separate to the accountability framework of information privacy law. This hacker/identity theft

305. *See* BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 25-6.

306. *See, e.g.*, BYGRAVE, *supra* note 58, at 68 (regarding the role of information security principles in data protection laws).

criminal is, at least, tangentially foreseeable. In turn, the enhanced identification of third parties touches on a further significant benefit of a contextual approach as it recognizes the possibilities for wider informational harms and injustices than those currently envisaged by information privacy laws.[307]

Nissenbaum incorporates van den Hoven's account of privacy which provides four moral justifications for *information privacy, informational harms, information inequality, informational injustice,* and *encroachment on moral autonomy*, in order to prevent further harms and thus promote equality, justice, and personal autonomy.[308] *Informational harms* acknowledge that a much greater span of harms can arise from the unauthorized or illicit use of many types of personal information in many different ways.[309] Harms consequently do not simply involve identity theft-related issues but can cause fear and anxiety to individuals which can lead to a withdrawal from social life.[310] *Informational inequality* recognizes that information asymmetries exist between different parties and therefore social benefits can be accrued disproportionately.[311] Individuals may provide their personal information to organizations but, by and large, they are generally unaware about organizational uses of personal information and have limited roles of involvement in essentially market-based informational structures.[312] The notion of inequality is important because it brings to the fore an analysis of power

307. *See* Bellia, *supra* note 111, at 898 (contending a requirement for a wider notion of dignitary harms that goes beyond material harms relating to identity theft).

308. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 78. *See, e.g.*, Jeroen van den Hoven, *Privacy and the Varieties of Moral Wrong-Doing in an Information Age*, 27 SIGCAS Comput. Soc. (1997); Jeroen, van den Hoven, *Information Technology, Privacy and the Protection of Personal Data, in* INFORMATION TECHNOLOGY AND MORAL PHILOSOPHY (Jeroen van den Hoven & John Weckert eds., 2008).

309. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 78.

310. For example, a data breach concerning sensitive law enforcement related information provided by informers can have serious consequences that include threats or loss of life. *See, e.g.*, Michael Isikoff, *Missing: A Laptop of DEA Informants,* NEWSWEEK, June 7, 2004, *available at* http://www.newsweek.com/id/53958 (regarding the loss of a laptop containing informant details relating to investigations conducted by the Drug Enforcement Administration in the US); *MoD Inquiry After Laptop Stolen from Headquarters,* BBC NEWS, Dec. 12, 2009, *available at* http://news.bbc.co.uk/2/hi/uk_news/8409363.stm (regarding the theft of a laptop from MoD headquarters in the UK); and *Previous Cases of Missing Data,* BBC NEWS, Dec. 12, 2009, http://news.bbc.co.uk/2/hi/uk_news/8409405.stm (regarding other instances of security failures involving laptops and sensitive UK government information).

311. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 79.

312. *See generally* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001) (regarding a conceptual overview of the imbalance of power between individuals and corporations).

relationships which is largely a latent aspect of the information privacy law literature.[313]

Informational injustice refers to the importance of personal information remaining within the contextual sphere within which it was created and disseminated.[314] For example, a recent study by Microsoft about the employment checks conducted by human resources departments in four different countries found that forty-three percent of US departments had rejected a prospective candidate based on comments provided by the candidate's 'friends' on Facebook.[315] This 'trial by friends' is thus considered an informational injustice because it not only takes information from one context and applies it in another but also because its use of information in this way ignores the crucial role of context and meekly accepts that what is being said is representative of an individual.[316] Finally, *encroachment on moral autonomy* is linked to the situation just described as it seeks to protect an individual's capacity to shape his or hers own life without undue interference and pressure to conform to some ascribed social norm.[317] Information privacy is therefore a key issue in society because it allows space for individuals to generate and fix their identity within a wider social sphere.

The relational and harm elements of a greater contextual approach are instructive because it highlights some fundamental limits of information privacy law. Information privacy should not just relate to problems regarding the governance of a management process.[318] Instead, information privacy should focus on problems that are inherently related to social relationships and their management.[319] Accordingly, within the context of data breaches and how information privacy law responds to such issues, this article contends that a

313. *See, e.g.*, Rosa Ehrenreich, *Privacy and Power*, 89 GEO. L. J. 2047, 2055 (2001) (regarding the unacknowledged role of power in privacy law).

314. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 80.

315. *See* Posting of Daniel Solove to Concurring Opinions Blog, Googling Employees: Why Your Online Reputation Matters, http://www.concurringopinions.com/archives/2010/03/googling-employees-why-your-online-reputation-matters.html (Mar. 15, 2010, 8:15) (last visited Sept. 10, 2010) (outlining the details of the study).

316. *See, e.g.*, Solove, *supra* note 312, at 1421 (regarding the dangers of digital dossiers as how bureaucracies relate database information to an accurate and entire view of individuals).

317. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 279, at 80.

318. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 230 (The University of North Carolina Press 1995) ("privacy is becoming less an attribute of individuals and records and more an attribute of social relationships and information systems or communication systems").

319. BENNETT & RAAB, GOVERNANCE OF PRIVACY, *supra* note 20, at 25.

contextual approach is required and a greater focus on privacy rather than information is needed. Contextualization thus recognizes the wider relational and harm issues that can arise through a context dependent analysis. Data breach concerns are not fixated to specific types of personal information.[320] Information privacy problems do not simply involve providers, collectors and users of personal information. Regulatory and legislative remedies do not merely entail simplistic solutions of redress in information management processes. However, the problem with contextualization is that it requires much greater legislative, regulatory, and judicial input than information privacy law currently allow. This point is addressed in the final sub-section of this article that explores a different view of the important role that data breach notification could have within the regulatory guise of protecting critical information infrastructures.

C. From Data Breach Notification to the Protection of Critical Information Infrastructures

As highlighted throughout this article, data breach notification laws are intended to fix the specific problem of identity theft threats arising from data breaches involving personal information through the mandatory notification of breaches to individuals. The laws also have an auxiliary aim of producing socially optimal side effects through the enhancement of corporate information security practices. Previous sections of this article have highlighted the limits of data breach notification law in sectoral regimes and data breach notification schemes implemented within comprehensive information privacy legal frameworks. Despite the issues highlighted in this article, it must be noted that data breach notification laws appear to have been a resounding success.[321] They have unearthed a previously hidden social problem that has the capacity to negatively affect millions of people's lives. Information privacy laws, as applied in both sectoral and comprehensive frameworks, are seriously lacking with regard to the imposition of legal obligations entailing the adequate protection of personal information. Accordingly, data breach notification laws have potential value and possibly much to offer. In concluding this article, the author asserts that the real problem with data breach notification is

320. *See, e.g.*, ST. AMANT, *supra* note 81, at 523 (highlighting that the revelation of personal health information can be as detrimental to an individual as financial information).

321. *See, e.g.*, Winn, *supra* note 76, at 1133 (noting the "tidal wave" of notifications thus making the "problem of inadequate information security . . . visible" while detailing potential problems with data breach notification law).

that the concept is too narrow; it has a limited notion of harm and it is purposively constrained by an overly context independent approach to the type of information regulated.

Data breach notification law inherits the same concerns of information privacy law because it predominantly regards information management rather than the preservation, protection, and resolution of social relationships regarding disputes over personal information. Moreover, within data breach notification laws themselves, there is a large degree of blame attached to the breached organization within the limits of a proscribed accountability framework. The breached organization is deemed to be at fault and, as a result, needs to provide notification of its failings. Notification is consequently heavily influenced by the concept of reputational sanction.[322] However, not all organizations are to blame extensively particularly in situations involving sophisticated hackers.[323] Some data breaches, such as the ChoicePoint incident[324] highlighted above, are based on situations involving the provision of inadequate security measures, but it should be recognized that some data breaches involving hacking attacks are ground-breaking in their levels of sophistication.[325]

Data breach notification laws attempt to resolve the complex problem of adequate corporate information security measures in a rudimentary way by mandatory notification. However, this remedy does not directly address the underlying issues of ineffective corporate security or indeed whether notification to individuals is an effective remedy.[326] Mandatory notification as a remedy simply cannot sufficiently account for the contextual realities of data

322. Schwartz & Janger, *supra* note 86, at 917. (stating that a significant focus of data breach notification law has been "to impose a reputational sanction on breached entities).

323. *See, e.g.*, Skinner, *supra* note 76, at 10 (regarding the complexities of intrusion detection in relation to phishing attacks); Kris Erikson & Philip N. Howard, *The Information Vulnerability Landscape. Compromising Positions: Organizational and Hacker Responsibility for Exposed Digital Records*, *in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 46 (Andrea M. Matwyshyn ed., 2009) (reviewing 813 publicly reported security breach incidents between 1980 and 2007 and confirming that a small percentage of incidents involve organizations that are "unwilling and unwitting victims of a malicious hacker").

324. *See* ELECTRONIC PRIVACY INFORMATION CENTER, CHOICEPOINT (2008), *available at* http://epic.org/privacy/choicepoint/

325. *See, e.g.*, Kim Zetter, *Google Hack Attack Was Ultra Sophisticated, New Details Show*, WIRED, Jan. 14, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora (regarding details of a recent Chinese hacking attack perpetrated on Google, Adobe and other leading US companies that was "unprecedented tactics that combined encryption, stealth programming and an unknown hole in Internet Explorer").

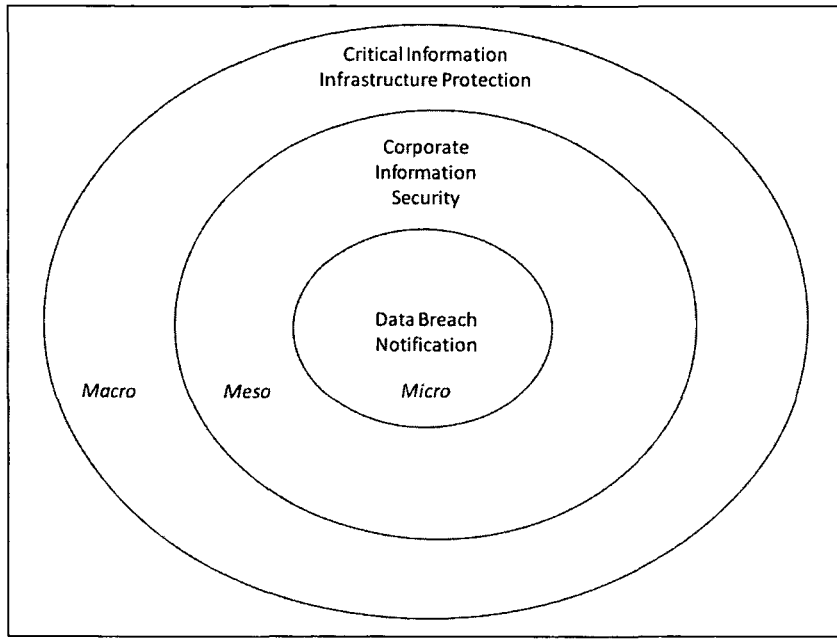
326. *See* Schwartz & Janger, *supra* note 86, at 947 ("Notification letters supply only incomplete, discontinuous, and non-comparative information about data security.").

breaches that regard complex security, social and legal concerns. As highlighted above, a certain type of personal information breached in one incident may have a different type of harm to the same information released in another data breach.[327] The issue of data breach notification is therefore inherently contextual and requires comprehensive case by case analysis regarding the identification of potential harms and the application of potential remedies. However, this in turn requires much greater regulatory oversight than that which is currently envisaged in either sectoral or comprehensive legal frameworks because data breach notification is primarily directed towards the mitigation of identity theft. Data breach notification law attempts to provide instant consumer redress, but in doing so, it misses the potentially important role that the law could have regarding the wider implications of adequate protections of personal information within the fortification of critical information infrastructures.[328] Data breach notification should be viewed in a comprehensively different perspective that regards different levels of social activity and a re-evaluation of the law's role. Figure 3 below provides a diagrammatical representation.

327. *See* discussion *supra* Part IV.B.

328. *See, e.g.*, Picanso, *supra* note 84, at 358 (linking network attacks on personal data to critical information infrastructures).

Fig. 3 – The role of data breach notification in light of critical information infrastructure protection



In Figure 3, three levels of social activity are adduced: *micro, meso,* and *macro.*[329] The *micro* level refers to the arena of human agency in which hackers attack organizational databases of personal information, employees lose laptops, and organizational employees notify individuals who take action to protect themselves. These are the base-level actions that generate issues and concerns regarding breaches of personal information. The *meso* level is the middle ground,[330] the decision making arena in which corporate decisions regarding information security are made. These decisions are crucial regarding the advent of data breaches as they involve declarations of intent regarding the implementation of adequate protections involving personal information. The possibility that a data breach could arise is heavily influenced by the decisions made in the meso level. For

329. *See also* ANDREA M. MATWYSHYN, HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 3-13 (STANFORD LAW BOOKS 2009) (regarding a different perspective of the social macro, meso and micro levels entailing corporate information security).

330. *See, e.g.*, D.W. PARSONS, PUBLIC POLICY: AN INTRODUCTION TO THE THEORY AND PRACTICE OF POLICY ANALYSIS (EDWARD ELGAR 1995) ("Meso analysis is a middle-range or bridging level of analysis which is focused on the linkage between the definition of problems, the setting of agendas and the decision-making and implementation processes.").

example, if an organization decides to implement adequate security measures and policies, then it is less likely that a breach will occur and vice versa. The decision arena of a smaller number of persons can consequently have a major impact on a much wider number of individuals at the *micro* level. Finally, the *macro* level regards the ground of structures and super-structures. In this case, it is the construct of critical information infrastructures, the underlying information and communication systems upon which both organizations and individuals are now so dependent.[331] Again, those decisions made in the *meso* level have the capacity to impact upon the macro level as vulnerabilities arising from corporate actions can traverse both upwardly and downwardly through different levels. For example, a major data breach involving security failures in one infrastructure can have an impact on many other infrastructures including the irreparable damage of consumer trust.[332]

The actions and decisions of different levels can impact upon the structures within which both human and organizational actors reside. Data breaches are consequently linked to corporate information security management procedures which in turn reinforce or reduce protections related to critical information infrastructures. Accordingly, data breaches are a reflection of corporate information security inadequacies, and the latter become weaknesses that need to be addressed in critical information infrastructures. A simple corporate decision to use an outdated type of encryption protocol on its wireless communication system can therefore lead to mass notification to millions of individuals and major upheaval in the banking sector simply because a team of sophisticated identity theft

331. Myriam Dunn Cavelty, *Critical Information Infrastructure: Vulnerabilities, Threats and Responses*, 3 DISARMAMENT FORUM 3 (2007) (outlining the reasons behind critical information infrastructure protection and highlighting that these infrastructures are critical because "their incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a state"); Andrew Rathmell, *Protecting Critical Information Infrastructures*, 20 COMP. & SEC. 44 (2001) (regarding the implications of the "information revolution" for the protection of state infrastructures); *See* Eugene Nickolov, *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations*, 17 INFO. & SEC. 105 (2005) (highlighting the dependency of modern societies on the availability and reliability of technological infrastructures).

332. *See, e.g.*, Schwartz & Janger, *Notification of Data Security Breaches*, *supra* note 86, at 928 (referring to the data security externality "where a data security breach at one company may cause harm at another company in a way that is untraceable or for which there is no legal recourse"). *See also* Philip E. Auerswald, et al., *Where Private Efficiency Meet Public Vunerability: The Critical Infrastructure Challenge*, *in* SEEDS OF DISASTER, ROOTS OF RESPONSE: HOW PRIVATE ACTION CAN REDUCE PUBLIC VULNERABILITY 8 (Philip E. Auerswald ed., 2006) (highlighting that no corporation is an island and the ripple effect of security breaches across economic sectors).

criminals gained unauthorized access to personal information held by the retailer.[333]

The introduction of contextualization highlights that data breach notification is only one complex system within an enmeshed environment of many complex systems that interact and impact upon each other. The primary focus on the single issue of identity theft partially recognizes some of these complexities, but it does not attempt to represent them in sufficient complexity or depth. Some authors have made the link between data breach notification and the onset of a newly developing legal field, information security law.[334] Equally, a link between corporate information security measures and the protection of critical information infrastructures has also been made.[335] Despite the fact that these links have been recognized, data breach notification laws have continued to have a specific and limited remit.

This article contends that data breach notification law needs to be considered contextually as part of a much wider problem that goes beyond the issue of identity theft mitigation. Moreover, the body of laws should not be viewed as a 'be all and end all' solution to problems relating to the inadequate protection of personal information by corporations. Data breach notification laws are extremely useful at highlighting problems but that does not mean they necessarily have the regulatory tools to remedy the problems that they uncover. Instead, it is more likely that the laws provide a transitory passage that attempts to take regulation from the identification of a significant problem (e.g. inadequate information security of personal information that requires notification) eventually to a potential solution (e.g. the implementation of effective security measures and competent

333. *See, e.g.*, MATWYSHYN, *supra* note 329, at 3 (outlining the simplicity of the initial attack perpetrated on TJX Maxx that was easily avoidable); Kim Zetter, *TJX Hacker Charged With Heartland, Hannaford Breaches*, WIRED, Aug. 17, 2009, http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/ (regarding further sophisticated attacks in the TJX incident which the attackers were able to penetrate most levels of data storage and the legal implications that flowed from the attacks).

334. *See generally* Smedinghoff, *supra* note 100; BH Nearon, et al., *Life After Sarbannes-Oxley: The Merger of Information Security and Accountability*, 45 JURIMETRICS J. 379 (2005); Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669 (2010); Andrea M Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation*, 3 BERKELEY BUS. L.J. 129 (2005); Winn, *supra* note 76.

335. *See generally* MATWYSHYN, *supra* note 329; PHILIP E. AUERSWALD, SEEDS OF DISASTER, ROOTS OF RESPONSE: HOW PRIVATE ACTION CAN REDUCE PUBLIC VULNERABILITY (Cambridge University Press. 2006); Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cybersecurity*, 4 SED. C. J. 109 (2003).

monitoring). Notification is therefore only one element of the issue and should not be deemed as the issue in itself.

Schwartz and Janger emphasized this problem in considerable depth in their influential article on regulatory structures for data breach notification.[336] They examined three regulatory models currently in operation and suggested a fourth model, the Co-ordinated Response Architecture (CRA) as a hybrid of the strengths and weaknesses of existing regimes.[337] The CRA has a system of two-tier disclosure.[338] The first tier requires the breached organization to notify the CRA which then determines whether customer notification is required based on the likelihood of information misuse.[339] Unlike current data breach notification laws, information misuse is to be construed broadly and does not simply relate to identity theft risks. If notification is required, the CRA will coordinate the sharing of information about a data breach, oversee the organization's investigation and response and monitor notification decisions.[340] The emphasis of the CRA model is mitigation response and notification encouragement that seeks organizational cooperation without losing the threat of reputational sanction.[341] The mitigation response element is clearly crucial and the authors recognize that notification has a wider role to play within social, technical, and legal structures.

The protection of individuals at the micro level of society is clearly important, but the protection of the macro information infrastructures that facilitate societal interactions and transactions is equally important. An authority such as the CRA, designed for the purpose of ensuring critical information infrastructure protection, would undoubtedly engender a greater regulatory focus. But that emphasis can be readily justified when viewed through the lens of consumer and infrastructure protection via the encouragement and enforcement of adequate information security measures. Data breach notification laws are important, but that importance goes beyond the specified remit of identity theft and goes to the heart of information-based societies. It involves the preservation of information pathways founded on human relations and maintained through information

336. *See generally* Schwartz & Janger, *supra* note 86.

337. *See id.* at 959-69.

338. *See also* Burdon, et al., *Encryption Safe Harbours*, *supra* note 72; Schwartz & Janger, *supra* note 86, at 960 (advocating for a two-tier system of notification in relation to encryption safe harbors).

339. Schwartz & Janger, *supra* note 86, at 960.

340. *Id.* at 962-63, 65.

341. *Id.* at 959-69.

infrastructures. Data breach notification provides gives a glimpse of these wider issues that unfortunately get subsumed by contested arguments relating to consumer protection and corporate compliance cost minimization. A revision of data breach notification, and indeed information privacy, is required that moves beyond the limited application of individual rights to the societal interests everyone has regarding the protection of personal information and the modes of information exchange. However, a macro perspective reveals complex structures that are difficult to regulate but nonetheless still require governance. The forms of legal governance are not yet adequately defined, and the issues raised by data breach notification laws indicate that there is still much distance to travel.

VI. CONCLUSION

This article contends that both information privacy and data breach notification laws appear to have a similar purpose that involves the protection of personal information. However, both laws have fundamental differences between them and shared weaknesses within them. In some ways, data breach notification is too conceptually complex as it is multifaceted and expansive in its foundation from the California law. This expansiveness is confined by a focus on compliance cost mitigation.

Alternatively, information privacy suffers from the opposite effect. The concept is too limited in focus because it attempts to regulate the process of personal information exchange and that provides a constraint on what is a privacy issue. Data breach notification in both sectoral and comprehensive approaches may therefore be a potentially expansive bolt-on which is implemented by a narrow focused law in an attempt to ascribe limited rights pertaining to an individual's involvement in the collection, storage and use of their personal information. The introduction of contextualization highlights the fact that both laws are predicated on certainty in order to reduce the ambiguous nature of privacy. Nonetheless, both laws need to include the social context of human relationships that underpin personal information exchange processes.

The application of contextualization promotes a revision of both data breach notifications and information privacy laws that move beyond notions of individual rights related to controls over personal information to societal protections of essential information infrastructures. To do so will require new modes of regulation and the development of new types of law. These are complex issues

especially if one considers that the process of personal information exchange is innately human and subject to the application of different contexts. Data breach notification law begins to reveal these complexities, and in doing so highlights the limits of current information privacy laws. However, data breach notification is not a 'be all and end all' solution in itself but merely provides a signpost for a journey to be undertaken. Exactly how that journey will manifest remains to be seen, but it is seemingly clear that the first steps have been taken. It is likely that different directions will be charted based on the application of sectoral and comprehensive regimes, but this article has attempted to show that future journeys should be mindful of the requirement for contextualization given the inherent tensions and weaknesses of both data breach notification and information privacy laws.

* * *