Brigham Young University International Law & Management Review

Volume 5 | Issue 1 Article 6

12-20-2008

International Data Privacy lawws and the *Protectors of Privacy*

ILMR Editors

International Data Privacy Laws and the *Protectors of Privacy*

ILMR Editors[*]

Abraham L. Newman's *Protectors of Privacy*[1] provides a stirring review of past and present international data privacy laws. Throughout the detailed historical narrative of global privacy laws, Newman analyzes not only the causes of change that brought about new laws, but also the effects the laws have had and will have in the future on individuals, governments, and businesses. His central theme is how the organization of businesses and politics affects data privacy laws and regulations—specifically the central role that intragovernmental and intergovernmental regulatory bodies, the "protectors of privacy," play in shaping privacy protection in Europe and throughout the world.

I. WHY PRIVACY LAWS MATTER

Newman opens his book by discussing how nations and businesses within those nations regulate vast amounts of personal information, including social security numbers, credit card purchases, website history, mobile phone logs, and even biometric data.[2] For example, Wal-Mart must manage its more than 460 terabytes (460 trillion bytes) of customer data—twice as much data as is housed on the entire Internet.[3] Although most nations have established some sort of data privacy regime under which businesses and governments operate, those regimes are imperfect. Identity theft and fraud alone cost U.S. consumers more than $50 billion every year.[4]

The technological advances allowing for rapid transfer and inexpensive storage of large amounts of data, coupled with the increasingly large electronic commerce market,[5] exacerbates the data privacy problem within a state or nation. In addition, these advances

---

* The ILMR editors responsible for writing and editing this book review include Joshua Engel, Lorie Hobbs, Parker Morrill, Devin Wagstaff, and Dorothy Hatch Ward. All five are J.D. candidates, J. Reuben Clark Law School, Brigham Young University.

1. ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY (2008). The book contains 221 pages (including extensive notes and a bibliography), and the ISBN is 0-8014-4549-3.

2. *Id.* at 1.

3. *Id.*

4. *Id.*

5. Estimated at $12 trillion in 2006.

may cause international disputes because of the ease with which personal information can flow across jurisdictional boundaries.[6] While these disputes have frustrated international trade and business, they have also promoted greater cooperation and compromise among the world's superpowers.

Newman states that privacy policies have implications for individual liberties, the powers of state, and the global economy.[7] Individuals should be concerned with the dangers of discrimination, surveillance, and other potential abuses of their private information.[8] Governments should be concerned with trade and security issues, especially counterterrorism. Businesses should be concerned with privacy laws as they directly affect the management of client information, especially that of international clients, when it is gathered and shared with other businesses and governments. In particular, privacy laws may have potentially severe consequences for international trade and outsourcing.[9] Rather than being just an abstract legal concern, Newman says, data privacy laws and regulations affect "patterns of information exchange: how individuals express their identity, how companies differentiate markets, and how governments manage risk."[10]

II. COMPREHENSIVE AND LIMITED REGIMES

Newman broadly categorizes data privacy regimes used in various countries into two groups: comprehensive regimes and limited regimes. Comprehensive regimes regulate both the public and private sectors, while limited regimes regulate only the public sector.[11] Newman recognizes the substantial differences in the implementation of these two regimes but focuses on the general ideologies to demonstrate how the regimes control data. By comparing and contrasting comprehensive and limited regimes, particularly those of the European Union and the United States, Newman identifies the effects of global politics, the factors that lead a country toward one regime or the other, and the effect the type of regime has on international negotiations.

6. *Id*. at 2, 8.

7. *Id*. at 3.

8. *Id*. at 47–48.

9. *Id*. at 3–5.

10. *Id*. at 6. Although this review will mostly be limited to the effects on businesses, a large portion of the book deals with effects on governments.

11. *Id*. at 23.

Newman suggests that comprehensive regimes limit the development of business sectors, citing, for example, the lack of a subprime mortgage market in countries with comprehensive regimes. He explains that the restrictive data privacy rules prevent lenders from (1) identifying high-risk clients and (2) providing customized real estate products.[12]

Newman finds that businesses in limited regimes rely on self-regulation and market mechanisms to control the use of personal data. Governments in limited regimes impose some oversight of certain private sector industries, such as health care and financial services, but the oversight is limited.[13] Personal data in limited regimes is valuable because, upon agreement, businesses can use and/or sell that data, especially for marketing purposes and consumer profiling. Newman notes that the financial services industry earns $17 billion annually from the free flow of information.[14] The U.S. government is also a major player in the information market—just four of the many government agencies purchased roughly $30 million worth of information from data compilers in 2005.[15]

Newman compares and contrasts the effects of the regimes on businesses in the United States and the European Union. Companies in the United States frequently buy and sell personal information. Publicly available information can also be gathered and transferred with minimal restrictions on its use.[16] On the other hand, E.U. countries limit the transfer of personal information, even if obtained from public registries. Credit reporting agencies are also more restricted. French credit reporting agencies are public sector institutions and only provide negative credit information (e.g., defaults and bankruptcies). Limiting this profiling under a comprehensive regime would impose significant costs on U.S. businesses. The information industry estimates that costs would increase in excess of $16 billion if a comprehensive regime was put in place in the United States.[17] Without the collection and distribution of positive financial information concerning potential customers' spending habits or investment information, businesses would have to

12. *See id.* at 29.
13. *Id.* at 30–31.
14. *Id.*
15. *Id.* at 31.
16. *Id.* at 30.
17. *Id.* at 30.

adapt their business models and find other ways to focus their advertising.[18]

III. HISTORICAL PERSPECTIVE

After introducing his topic and explaining some general privacy law principals, Newman begins his lengthy discussion of privacy law history. He then details the historical origin of privacy regulation in the European Union, which would come to characterize the privacy regulation for most of the rest of the world.

A. Early Privacy Laws

Newman posits that data privacy concerns began about the same time as the arrival of the mainframe computer in the 1970s, when scholars began discussing the implications of the new technology and data collection.[19] As a result, a set of principles called the Fair Information Practice Principles was developed and included the right to be notified before the collection of the information, the right to consent to the further distribution of the information, and the right to object to incorrect data.[20]

Newman observes that the U.S. policy regarding data privacy began when Congress passed the 1974 Privacy Act.[21] Industry lobbyists quickly pointed out that there had been no problems in the private sector that warranted comprehensive rules. Furthermore, U.S. President Gerald Ford threatened to veto any bill that contained private sector regulation and to further institute public sector regulation via executive order if Congress did not enact a limited privacy regime.[22] Congress therefore adopted a limited privacy regulatory regime under pressure from private industry and the President.[23] Eventually the United States became the strongest proponent of limited data privacy regimes.

B. Creation of Privacy Laws in the European Union

Newman then proceeds to discuss the creation and evolution of the E.U. privacy regime. In the early 1970s, privacy advocates in

18. *See id.* at 28–29.
19. *Id.* at 25.
20. *Id.*
21. *Id.* at 43, 57.
22. *Id.* at 59.
23. *Id.* at 60.

Europe worried that countries without privacy regulations would become havens for large banks of personal information.[24] Delegates from European countries joined forces to find a solution to increasing international data sharing. For the next ten years, privacy regulation discussions continued and eventually a group of privacy experts convened and made recommendations to the Council of Europe.[25] These recommendations were adopted in the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981. Although some European countries ratified the convention, it was not self-executing and ultimately failed to produce any comprehensive regulation.[26]

Although the European Union was, by and large, indifferent and even resistant to private sector privacy controls in the 1980s, a few individual countries in Europe did implement private sector privacy controls. For example, French and German officials overcame opposition to bureaucratic constraints and adopted privacy rules in both public and private sectors.[27]

Newman theorizes that the acceptance of comprehensive privacy laws in the European Union began in response to concerns about cross-border data sharing. European countries created a group of privacy officials to address these concerns.[28] As their influence increased, these officials were able to overcome opposition and indifference in the European Union. By 1988, eleven European countries had agencies to address important issues including safe havens created by countries with lax standards and multi-national companies engaging in Pan-European data exchange.[29]

Newman explains that by the late 1980s, conflicts between European nations concerning data privacy were on the rise. He notes, in particular, the French data authority blocking the flow of personal data to both Italy and Belgium in 1989.[30] Other conflicts continued to mount, eventually threatening several European

24. *Id*. at 83.

25. *Id*. at 84.

26. *Id*.

27. *Id*. at 52. Even though Germany was an early adopter of comprehensive privacy regulations, Newman rejects the popular belief that countries with fascist histories tended to be more sensitive to privacy concerns and more likely to adopt a comprehensive regime. *See id*. at 52–54.

28. *Id*. at 87.

29. *Id*. at 87–88.

30. *Id*. at 89–91.

Community projects.[31]

In response to the growing conflicts, the European Community formed a committee, consisting of national privacy officials and European Commission officials, to draft a privacy directive to facilitate uniformity.[32] When the draft was released, the industry lobbyists pushed for flexibility between national regimes because of the high cost of additional compliance in addition to the capital already spent on compliance with national rules.[33] Finally, in October 1995 the Council of Ministers and the European parliament adopted the Commission's resolution.[34]

Newman explains that the directive required member states to do three things: enact legislation for the public and private sectors, create an agency to implement and enforce the directive, and ensure that countries outside the European Union demonstrate adequate privacy protection as a condition of data transfers.[35] The directive also created several entities to help the European Union and individual member states implement the directive's policies both inside and outside of the European Union. The directive resulted in harmonized privacy protection within Europe and gave greater power to privacy regulators.[36]

One of the most important parts of the directive for both European and non-European businesses is Article 25, which requires European data transfers to be restricted to those countries with adequate data privacy laws.[37] However, rather than imposing a comprehensive regime across the board, as would normally be required under Article 25, the United States negotiated the Safe Harbor Agreement with Europe whereby U.S. businesses may transfer data from their European affiliates as long as the businesses comply with E.U. standards. Under the Safe Harbor Agreement, U.S. firms must choose to be monitored and enforced by self-certification or self-regulation. Firms that choose to self-regulate agree to abide by certain dispute resolution requirements and become subject to the scrutiny of the Federal Trade Commission, which monitors the firms' compliance with their self-regulatory

31. *Id*.
32. *Id*. at 91.
33. *Id*. at 91–92.
34. *Id*. at 93; *see also* Council Directive 95/46, 1995 O.J. (L 281) (EC).
35. *See id*. at 93–94.
36. *Id*. at 94–96.
37. *Id*. at 36.

agreements. Firms that choose to self-certify must register with the European data privacy authority and agree to be regulated by that agency. A 2004 study showed that seventy-five percent of U.S. multinational firms chose to self-certify.[38] Newman shows that the European requirements have motivated international businesses to take the initiative in developing their own internal privacy regulations and promoting privacy enhancing technology throughout all of their operations.

IV. THE SPREAD OF PRIVACY LAWS AND IMPLICATIONS FOR INTERNATIONAL BUSINESSES

Following an extremely detailed narrative of early U.S. and E.U. data privacy laws, the author next explores how and why the European Union influenced countries outside of Europe to adopt a comprehensive privacy policy.[39] The author argues that many countries follow the E.U. pattern because of the influence of its comprehensive regulatory model for regulating privacy issues, rather than its sheer market power. Although he does not discuss each country in detail, Newman notes that since the adoption of the E.U. regulations "over thirty countries from five continents have moved toward adopting comprehensive [privacy] regulations."[40] Furthermore, a number of countries that "previously regulated only the public sector have adopted private sector legislation."[41]

Initially, international resistance to the European Union's comprehensive model was strong and vocal. Nonetheless, Newman argues that the E.U. data privacy authorities came to dominate the international market as a result of the following four successful policy mechanisms: "control over market access, E.U. enlargement, centralized negotiating authority, and oversight networks."[42]

A. Controlling Market Access

Newman notes that the European Union's market size, combined with its regulatory capacity, allows it to project its rules to other nations, monitor compliance, and enforce its rules on firms participating in the European market. The size of the market alone

38. *Id*. at 39.
39. *Id*. at 99.
40. *See id*. at 101–03.
41. *Id*.
42. *Id*. at 105.

might be enough for many firms to adopt E.U. standards because of the costs of non-adjustment.[43]

Newman explains that two provisions of the E.U. directive are central to controlling market access. Article 25 gives authority to ban transfers of personal information from the European internal market to nations that fail to enforce adequate privacy protections standards and levy fines for violations.[44] Article 29 confers authority on a Working Party to determine the adequacy of privacy protection in other countries, release opinions on such adequacy, make recommendations, and interpret directives. The determinations and decisions of the Working Party have an influence on privacy regulations in other countries.[45]

As an example of the impact of the European Union's market access control, Newman notes that in 1999 the Spanish data privacy authority investigated a data exchange between Microsoft U.S. and Microsoft Iberia.[46] The Spanish authority determined that Microsoft acted contrary to European data privacy laws and fined Microsoft $60,000 for the illegal transfer of Spanish citizens' personal information without their consent.[47]

The author further explains that the European Union used control of market access to shape regulatory reform in Australia.[48] Australia initially adopted a limited privacy regime in 1988.[49] Later, in 1997, despite pressure from the European Union to adopt a comprehensive privacy scheme, the Australian government ordered private industry to develop self-regulating standards instead of expanding privacy regulations. Some industry groups, however, recognized that Australian self-regulations would have difficulty meeting the Article 29 adequacy requirements and would therefore isolate Australian business from the European market.[50] Bowing to these concerns, the Australian government reluctantly enacted private sector privacy rules. However, even after Australia introduced comprehensive rules, the Article 29 Working Party deemed the Australian legislation inadequate and suggested reforms. Yielding to

43. *Id*.
44. *Id*.
45. *Id*. at 106.
46. *See id*. at 111.
47. *Id*.
48. See *id*. at 106–10.
49. *Id*. at 106.
50. *Id*. at 106–07.

pressure from privacy advocates who leveraged the threat of E.U. sanctions, the Australian government strengthened privacy regulations to comply with the privacy directive, pending final European Commission approval.[51] Although Australian privacy regulations are not an exact replica of European rules, market access control was critical in moving Australia from a limited to a comprehensive regime.[52]

Although U.S. companies are not directly subject to the E.U. privacy regime, they may be forced to comply in order to conduct business in the European Union. Newman notes that although many countries have adopted comprehensive privacy policies because of the European Union's market access control, the United States has maintained its limited privacy regime. As mentioned above, however, in order to comply with the Article 29 Working Party privacy adequacy requirements, the United States entered into the Safe Harbor Agreement with Europe.[53] Thereby, American firms who register and agree to the terms of the Safe Harbor Agreement are able to store and use private data of European citizens.

B. Expansion of the European Union and Its Centralized Negotiation Authority

To obtain membership in the European Union, prospective countries must demonstrate that their political, economic, and regulatory standards comply with E.U. expectations.[54] Newman explains that the European Union uses the allure of prospective E.U. membership as an incentive for potential E.U. countries to adopt comprehensive data privacy laws.[55] In addition, the European Union sends experts to candidate countries to monitor and advise on specific aspects of policy reform and implementation.[56] These requirements are often a bureaucratic barrier to E.U. membership and do not necessarily benefit businesses. The author found no evidence that industry groups in the prospective countries promoted comprehensive privacy legislation.[57] Rather, some candidate countries have succumbed to E.U. peer pressure and passed privacy

51. *Id.* at 109.
52. *Id.* at 110.
53. *Id.*
54. *Id.* at 112.
55. *Id.* at 113.
56. *Id.* at 114.
57. *Id.*

legislation initiated through programs funded by an E.U. investment of over three million Euros.[58]

The well-developed regulatory capacity of the European Union allows it to act as a centralized negotiation authority. The European Union capitalized on this advantage in negotiating the General Agreement on Trade in Services (GATS). Initially, privacy rules banning data transfers to countries that lacked adequate privacy regulations violated GATS. The European Union pushed for a privacy exemption, which the United States did not oppose. However, after the exemption prevailed, the United States realized that privacy rules could hinder international trade. Unable to weaken privacy rules because of the GATS exemption, the United States softened its position in future privacy negotiations with the European Union.[59]

C. Oversight Networks

The European expansion of regulatory capacity gives European regulatory institutions the ability to affect behavior in world markets. The Article 29 Working Party serves as policymaker by interpreting privacy laws and recommending privacy policy changes. The Working Party has released over one hundred opinions, which although nonbinding, are relied on by national courts as well as multinational businesses.[60]

The Working Party opinions have influenced the debate over online authentication services. For example, following the release of a nonbinding Working Party opinion addressing its concern with the lack of disclosure about the use of their consumer information in online authentication services, Microsoft integrated new privacy enhancing features into its online authentication service.[61] Similarly, in 2007 the Working Party influenced Google to shorten its data retention policy from twenty-four months to eighteen months. Shortly thereafter, Yahoo and Microsoft followed Google's lead.[62]

Multinational firms comply with Working Party opinions in order to avoid litigation or penalties. [63] The changes made by these

58. *Id.* at 115.
59. *Id.* at 116–17.
60. *Id.* at 118.
61. *Id.* at 119–20.
62. *Id.* at 120.
63. *Id.*

firms are eventually integrated into their global best practices.[64] The firms employ professional advisors who bolster the authority of the Working Party opinions by advising their clients to follow those opinions.[65]

The European Union circumvents the need for new legislation by influencing firms directly through the Working Party opinions.[66] Working Party officials can avoid the inefficient institutional processes of the European Union and "regulat[e] through recommendation."[67] If multinational firms desire to compete in the European market, they must integrate the Working Party's decisions into their privacy policies, thus demonstrating the European Union's powerful ability to define, monitor, and enforce market rules.

Businesses and industries must be aware that regulatory agencies are exerting a powerful influence on privacy laws and should pay attention to the trends established by such agencies. Newman implies that by focusing on the above-mentioned four factors—control over market access, E.U. enlargement, centralized negotiating authority, and oversight networks—businesses may be able to predict the power that a regulatory agency can exert on a particular industry.

V. CHANGING THE RULES

After explaining the international spread of E.U. privacy laws, Newman explores the limits of the E.U. regulatory authority in non-market settings in view of recent events.[68] Newman illustrates some of these limitations in the telecommunications and national security debates following terrorist attacks in the United States, Spain, and the United Kingdom.[69] He concludes that in highly sensitive areas, such as national security, the power of transgovernmental regulatory bodies diminishes when confronting strong national interests. However, these regulatory bodies may still have a place in determining policy within individual countries.[70] The compromises

64. *Id*.

65. *Id*.

66. *Id*. at 121.

67. *Id*.

68. *Id*. at 123–24.

69. *Id*. at 124. *See generally id*. at 132–139 (discussing the effects of the war on terror on data privacy).

70. *Id*. at 125.

also show that data privacy is not an absolute right, but a freedom subject to limitation.[71]

A. The Telecommunications Debate

Newman gives a lengthy description of the fierce debate over telecommunications data privacy and the qualified victory of E.U. data privacy authorities in national security disputes.[72] While recognizing that E.U. data privacy authorities modified their initial proposals, the authorities served as a counterbalance against rules that would have substantially eliminated privacy rights. In 1997, and again in 2002, E.U. data privacy authorities in Europe pressed for regulations that preserved telecommunications data privacy with minor exceptions for national security.[73] For example, data authorities quickly quashed a Belgian proposal for mandatory data retention on limited issues.[74] It appeared that data privacy advocates had successfully defended the individual's right to privacy against national security concerns with only limited concessions.

However, the terrorist attacks in Spain and the United Kingdom during 2004 and 2005 shifted the telecommunications data privacy debate from an E.U. trade issue to a national security issue.[75] Ultimately, the European Parliament reached a compromise and passed legislation providing for the limited retention of telecommunications data for "between six months and two years."[76] While unsatisfactory, the legislation "limited the use of the retained data to issues directly related to international criminality."[77] This compromise appeased the E.U. data privacy authorities, but angered industry, placing the cost of data retention squarely on industry's shoulders.[78] Firms were required to maintain data for government use without reimbursement or the freedom to use the data for their own marketing or economic benefit.[79]

71. *Id*. at 22.
72. *See id*. at 125–32.
73. *Id*. at 126–27.
74. *Id*.
75. *Id*. at 128–29.
76. *Id*. at 130.
77. *Id*.
78. *Id*.
79. *Id*.

B. The War on Terror

Newman discusses in detail the conflict of U.S. data retention laws and E.U. data privacy directives necessitated by terrorist attacks.[80] Although terrorist attacks in Europe prompted a review and ultimately a reform of E.U. data privacy regulations, the changes were not as extensive as the reforms made by the United States in response to the September 11 attacks.[81]

The gap between the U.S. requirements and the E.U. regulations resulted in negotiations between the European Commission and the United States facilitating the exchange of some sensitive data. However, the negotiations limited which agencies would have access to the data until a more detailed agreement could be reached.[82] In December 2003, the European Commission renegotiated a compromise with the United States, but according to E.U. data privacy authorities and the European Parliament, the regulations remained inadequate.[83] As a result, the European Parliament filed a suit against the European Commission in the European Court of Justice, claiming the Commission had overstepped its authority. The court ruled that because the issue was one of national security and not "internal trade," the Commission violated its authority.[84] Following the 2004 ruling, the European Commission and the United States reached an agreement in 2007 that was less protective of privacy than the prior accord.[85]

Newman observes that regulatory bodies have strong influence and power within the narrow scope of their expertise, but are subject to limitations established by the authorizing statute. Regulatory bodies lose power and influence when they venture outside of their expertise or delegated authority.

In the same vein, Newman reminds his readers that the European Court of Justice and other national courts may yet influence the future of data privacy by ruling on the constitutionality of the final 2007 agreement.[86] The European Parliament is lobbying

80. *See id*. at 132–39.

81. *Id*. at 132–33 (explaining that the United States demanded full access to airline databases, and a 50 year retention policy, and also threatened heavy-handed penalties backed by impressive regulatory power and expertise).

82. *Id*. at 133.

83. *Id*. at 135.

84. *Id*. at 136.

85. *Id*. at 136–37.

86. *Id*. at 138–39.

individual parliaments and E.U. data privacy authorities to review the legality of the act in light of national constitutions and European laws.[87] Additionally, Newman predicts that the decision by the European Court of Justice will further weaken Europe's ability to shape international regulatory debates.[88]

Recent events have shown the volatility and difficulty of establishing a global standard for data privacy; therefore businesses and industry leaders should pay close attention to the negotiations and proposals that will set the stage for the future. Businesses with international interests should strongly consider the national and transgovernmental laws that may affect data use, retention policies, and even business models of their particular industries.

VI. IMPLICATIONS

Throughout the book, Newman notes many implications of his theories for businesses, individuals, and governments. Although he only minimally addresses many relevant issues, such as data privacy concerns in China and India, he does make several observations that could help businesses, individuals, and governments understand the importance of maintaining a historical perspective of international data privacy laws.

Newman perceptively notes that regulation of the international market is becoming "the next wave of globalization" and recognizes Europe's powerful voice in such regulation.[89] Although Europe's influence in data privacy regulation is strong, the E.U. regulatory capacity varies considerably across international business issues.[90] Due to this variation, Newman encourages scholars to assess E.U. involvement in international politics and the role of E.U. political institutions in shaping international governance.[91]

Newman also observes that the regulatory state has "global dimensions" and identifies the changing and increasing E.U. role in international data privacy laws.[92] His research shows a turn from positivist governance towards regulatory strategies in Europe.[93]

87. *Id*.

88. *Id*. at 140.

89. *Id*. at 15–16.

90. *Id*.

91. *Id*.

92. *Id*. at 14–15.

93. *Id*. (explaining that in contrast to Europe, which has increasingly granted more and more authority to regulatory bodies, the United States has shied away from regulatory bodies,

Newman proposes that his "comparative historical institutional research" strategy towards data privacy laws should be used to study other aspects of international law.[94]

The author compares the effects arising from jurisdictions that anticipate new issues with jurisdictions that tend towards reactionary measures—i.e., avoiding regulation until disaster strikes. As regulatory authorities are not elected and often not closely scrutinized by legislative bodies, this lack of oversight raises concerns "about democratic accountability and legitimacy."[95] Newman illustrates numerous conflicts between limited and comprehensive privacy law regimes, even among different comprehensive regimes. Globalization often uncovers conflict of laws between countries, and there is no supreme authority to determine the proper rule of law. Compromises, such as the Safe Harbor Agreement, are imperative to allow multinational firms to conduct business in countries with conflicting privacy regulations. It has yet to be seen which courts are better equipped to resolve conflicting laws and determine whether countries will be bound by decisions of foreign courts. Newman suggests that continued negotiation, compromise, and judicial review will determine the boundaries of privacy law.

VII. CONCLUSION

Newman's book provides businesses with international privacy concerns an excellent review of past and current privacy laws throughout the world. The author examines the history of privacy regulation in striking detail, offers his theory of why privacy laws developed the way they did, and discusses how these laws may continue to develop in the near future. Although somewhat limited in its contemporary application, Newman's discussion illuminates several concerns that all businesses with an international clientele should consider.

viewing them as a form of bureaucracy that unnecessarily interferes with individuals and businesses).

94. *Id.* at 17.

95. *Id.* at 151.