Michigan Telecommunications and Technology Law Review

Volume 17 | Issue 2

2011

Does Law Matter Online - Empirical Evidence on Privacy Law Compliance

Michael Birnhack
Tel Aviv University

Niva Elkin-Koren
University of Haifa, elkiniva@law.haifa.ac.il

DOES LAW MATTER ONLINE? EMPIRICAL EVIDENCE ON PRIVACY LAW COMPLIANCE

*Michael Birnhack**
*Niva Elkin-Koren***

Cite as: Michael Birnhack and Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMM. TECH. L. REV. 337 (2011), *available at* http://www.mttlr.org/volseventeen/birnhack&elkin-koren.pdf

Does law matter in the information environment? What can we learn from the experience of applying a particular legal regime to the online environment? Informational privacy (or, to use the European term, data protection) provides an excellent illustration of the challenges faced by regulators who seek to secure user rights and shape online behavior.

A comprehensive study of Israeli website compliance with information privacy regulation in 2003 and 2006 provides insights for understanding these challenges. The study examined the information privacy practices of 1360 active websites, determining the extent to which these sites comply with applicable legal requirements related to information privacy and examining other privacy-related practices. Information practices were explored on three levels: first, we examined the legal requirements applicable to each information practice under current Israeli law (legal analysis); second, we analyzed the declared privacy policies posted on each website; and third, we studied the actual information practices of each website.

The findings show that only a small minority of websites comply with legal requirements. Most websites do not provide privacy

---

* Professor of Law, Faculty of Law, Tel Aviv University.

** Dean & Professor of Law, Faculty of Law, University of Haifa; Director, Haifa Center for Law and Technology. We thank participants at the 9th Annual CIPLIT conference (DePaul, Oct. 2009), the 37th TPRC (Washington, Sept. 2009), and the Empirical Legal Studies Conference (Tel Aviv University, Mar. 2009) for helpful comments. This research was funded by the Israel Science Foundation (grant 867/04). We thank Yael Onn-Weisshof and Roman Krupnik-David (research coordinators), Nir Servaka (research assistant), and Dr. Nitza Barkan (data analysis). We thank ISOC-Israel and Tehila, Governmental Infrastructure for Internet Era for providing data sets of websites, and Shimon Gruper of Aladdin Knowledge Systems Ltd. for data security analysis.

protection to users at the level required by the law. Websites routinely collect personal data from users, although the practice of collecting data is slightly lower among commercial and organization websites than in other categories. Among public and private sector websites, compliance was relatively low, with 16% and 22% of websites that collect personal data giving users some sort of notice. The popular and sensitive websites, generally owned by large corporations, had substantially higher levels of compliance, and the most popular websites had the lowest number of violations.

The overall picture that emerges from the findings is one in which the law seems to have only a relatively minor role in shaping users' privacy experiences online, while other forces and factors are clearly at play. The findings further suggest that information privacy regulation is most effective among commercial enterprises, which are better able to acquire legal advice and respond to potential legal liability. It is less effective among small enterprises and individual users who operate websites, because they typically cannot afford the somewhat sophisticated legal counsel that is required for establishing and maintaining a data protection policy. This is a troublesome conclusion, given growing threats to user privacy in the Web 2.0 environment. As a whole, the findings suggest that data protection regulators may be unable to craft a single legal measure that fits the Internet. Regulating the online behavior of various players may require tailored regulatory measures.

INTRODUCTION

The online environment increasingly provides us with "privacy events."[1] These are situations that place privacy-related issues at the forefront of our daily lives, attract media attention, and cause an online buzz. Online privacy events occur when user privacy is compromised in ways that frustrate common expectations. The dynamics of each such event are different. Some privacy events fade out with users adjusting to the new situation. Other privacy events result in online civic resistance.[2] An application recently offered by Google, Google Buzz, is a clear example of the latter.[3] Users of Google's email service, Gmail, learned that they were automatically added to a new social network composed of their email and chat correspondents. Online friends included many business contacts or others whom the users did not wish to befriend or publicly reveal. Opting out of the service was possible, but as in many privacy events, the invasion of privacy had already occurred. Public outcry followed, and Google was forced to apologize and change its privacy policies.[4]

Privacy events draw much attention, and as Google Buzz illustrates, social resistance can reverse encroachments on our privacy. However, privacy threats are often more subtle than the Google Buzz example, and can have more profound effects. Our individual privacy is regularly compromised, by many websites, including those that do not make the

1. "Privacy events" is a take on "media events," a term discussed in DANIEL DAYAN & ELIHU KATZ, MEDIA EVENTS: THE LIVE BROADCASTING OF HISTORY (1992).

2. Civic resistance to new privacy threats is not a new phenomenon. Alan Westin, in his seminal 1967 work on privacy, documented such resistance to a proposal to add a religious question to the census and to the introduction of a national identification system. ALAN WESTIN, PRIVACY AND FREEDOM 302–05 (1967); *see also* COLIN J. BENNETT, THE PRIVACY ADVOCATES—RESISTING THE SPREAD OF SURVEILLANCE (2008) (examining the organization and strategies of privacy advocates).

3. *See generally* GOOGLE BUZZ, http://www.google.com/buzz (last visited Sept. 11, 2010).

4. *See* David Coursey, *Google Apologizes for Buzz Privacy Issues*, PC WORLD (Feb. 15, 2010, 10:07 AM), http://www.pcworld.com/businesscenter/article/189329/google apologizes_for_buzz_privacy_issues.html. Google later faced a lawsuit and settled out of court. *See* Damon Darlin, *Google Settles Suit over Buzz and Privacy*, BITS BLOG (Nov. 3, 2011, 12:19 AM), http://bits.blogs.nytimes.com/2010/11/03/google-settles-suit-over-buzz-and-privacy.

top of the most visited lists. These websites comprise the long tail, which is the focus of our attention here.[5]

Certain non-legal mechanisms can affect online privacy and shape the power of individuals to control their personal data. A website's technological architecture, or to use Lawrence Lessig's term, code, may enable or disable particular forms of data collection, processing and surveillance.[6] For example, Google chose to include all of its Gmail users automatically in the Google Buzz service by using an opt-out mechanism that required active efforts by those who wish to be pulled "out."[7] Changing default rules, especially those embedded in technology, is not an obvious or easy task for many Google users.[8]

Social norms also shape our online privacy. Our expectation of privacy in personal data may differ among individuals and between groups. We may each hold a different perception regarding the meaning of privacy online and the extent to which our privacy is threatened by online information flows. On one side is the view conveyed by the famous *New Yorker* cartoon in which a dog tells another "[o]n the Internet, nobody knows you're a dog."[9] At the other extreme stands Scott McNealy, cofounder of Sun Microsystems, who once announced in reference to the Internet: "You have zero privacy anyway, get over it."[10] In reality, we experience a more complex and nuanced privacy environment than either of these views suggests, with many factors shaping our online privacy and risks.

Finally, the law may also affect online privacy. Informational privacy remains on the table of policymakers in the United States. As of the time of this writing, the Obama administration is reconsidering its privacy policies.[11] What role does the law play in shaping our privacy online?

---

5. The "long tail" refers to the large number of websites that each attract only a small number of users. The cumulative usages of these websites is substantial. For an introduction to the idea of the long tail, see CHRIS ANDERSON, THE LONG TAIL: WHY THE FUTURE OF BUSINESS IS SELLING LESS OF MORE (2006).

6. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE *passim* (1999).

7. *See supra* note 4.

8. Paul Schwartz, quoting Neal Stephenson, called this phenomenon the "blinking twelve," referring to the common display on VCRs, which many users do not change. *See* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 754 (2000).

9. Peter Steiner, *On the Internet Nobody Knows You're a Dog*, NEW YORKER, July 5, 1993, at 61, *available at* http://www.cartoonbank.com/1993/on-the-internet-nobody-knows-youre-a-dog/invt/106197.

10. Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED.COM (Jan. 26, 1999), http://www.wired.com/politics/law/news/1999/01/17538.

11. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE—A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS (2010), *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf (proposing a new framework for addressing

Various types of private ordering, including contracts, licenses, privacy policies, bylaws and Terms of Use, define the rights and duties of the parties involved regarding the collection and use of personal data. Public ordering, namely, statutes and regulations, also affect online privacy by setting limits on the use of personal data and informational surveillance, also known as dataveillance.[12] Legal jurisdictions take different approaches to online privacy. Some are comprehensive, such as the European data protection regime, while others offer a narrower regulatory scheme tailored to address particular threats to online privacy, namely the American model.[13]

This Article addresses the role of the law in shaping online privacy. Does law matter in the information environment? What can we learn from the experience of applying a particular legal regime to the online environment? The empirical study presented here (the "Privacy Study") explores the efficacy of law in regulating online privacy and data protection.

Informational privacy (or, to use the European term, data protection) provides an excellent illustration of the challenges faced by regulators who seek to secure rights and shape the behavior of online users. The appropriate limits in regulating online privacy are highly controversial, providing the opportunity for valuable case studies exploring different regulatory strategies. There is continuous debate among European and American regulators and commentators regarding the proper understanding of *privacy in information*.[14] In the American model, privacy is understood as a *liberty*, protecting citizens against the State.[15] In contrast, the common European understanding is of a *right to human dignity*—an individual right to determine the end uses of our personal data—in which threats to privacy arise from both the State and the free market.[16]

---

commercial use of consumer data, composed of privacy by design, simpler consumer choices and making data practices more transparent).

12. *See* Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (1988).

13. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1230–32 (1998); discussion *infra* Part II.B.

14. *See* Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633 (2000); Matthew A. Chivvis, *Consent to Monitoring of Electronic Communications of Employees As an Aspect of Liberty and Dignity: Looking to Europe*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 799 (2009); Kang, *supra* note 13, at 1230–32; Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

15. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

16. *Id.*; *see also* Edward J. Bloustein, *Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1000–07 (1964) (refuting Prosser's claim that no single thread connects common law privacy cases and identifying human dignity as the

The disagreement extends to the proper policies to be adopted. The European approach is based on heavy regulation of any collection and processing of personal information under the data protection regime.[17] On the other hand, the current American approach generally favors a "hands off" position, except for particular kinds of data such as credit information, health information, or data collected from children under the age of thirteen.[18]

The Privacy Study explored the question of whether it is constructive to shape informational practices through regulation. A comprehensive empirical study of information privacy practices of 1360 Israeli websites showed a very low level of compliance with informational privacy regulations. Furthermore, the Privacy Study explored the behavior of various online actors and outlined differences in responses to these regulations. By comparing the levels of compliance among different actors and analyzing differences in their responses to regulatory schemes, we are able to identify circumstances where legal intervention could be effective and also detect other forces that shape online behavior.

The Privacy Study explored the level of compliance of Israeli websites with information privacy regulations in 2003 and 2006. The Israeli online sphere provides an interesting case study. Although Israel enjoys a high level of Internet penetration, its size offers a convenient laboratory for a case study, at times enabling us to test the entire population of websites rather than samples.[19] Furthermore, the few studies that have examined privacy practices targeted mostly American websites which are subject to a thin, sectoral informational privacy regime.[20] The Privacy Study explored the efficacy of a thicker legal regime in regulating online privacy, similar to the European data protection regime. This case study thus provides a basis for comparative analysis with the studies of American websites.

The Privacy Study focused on two bedrock standards of any data protection regime: *notice* and *consent*. Thus, the implications of our find-

---

unifying thread); Kang, *supra* note 13, at 1230–32 (arguing for a default rule regarding privacy based on dignity grounds).

17. *See* Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 1995 O.J. (L 281) (EC) [hereinafter Data Protection Directive].

18. *See* Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2006) (regulating the collection and use of financial data); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201 (2006) (regulating the collection and use of medical data); Children Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06 (2006) (regulating the collection and use of data from children under the age of thirteen).

19. *See Internet Usage Statistics of Countries Ranked by Penetration Rates*, INTERNET WORLD STATS, http://www.internetworldstats.com/list4.htm#high (last updated Mar. 31, 2009); *infra* note 117.

20. *See infra* Part II.B.

ings go beyond any particular legal regime and may be relevant in various jurisdictions. Information privacy practices were explored at three levels: first, we examined the legal requirements that apply to each information practice (legal analysis); second, we analyzed the declared privacy policies posted on each website; third, we studied the actual information practices of each website, focusing on data security. The results showed a low level of compliance with the legal requirements.

The study further compared compliance with the legal requirements among four clusters of websites: public, private, popular, and sensitive websites.[21] While compliance among public and private sector websites was relatively low, the popular and sensitive websites had substantially higher levels of compliance; the popular websites had the lowest number of violations.

The overall picture that emerges from our findings is one in which the law seems to play only a relatively minor role in shaping users' online privacy experience, while other factors have a larger impact. The findings further show that information privacy regulation is most effective in commercial enterprises and less effective in small enterprises or individual user-operated websites. Consequently, the Privacy Study suggests that data protection regulations should not approach the task with a single legal measure that fits all players. Rather, regulating the online behavior of various players may require segmented regulatory measures.

This Article proceeds in three parts. We begin by laying out the foundations of privacy and data protection law in Part I. Part II provides an overview of the empirical study, describing its methodology and primary findings. In addition, we discuss some methodological challenges that might be relevant to similar empirical legal studies in other jurisdictions. Finally, in Part IV, we discuss the ramifications of the findings for policies aimed at promoting online informational privacy, and further elaborate on the contribution of the Privacy Study to the understanding of the limits of regulation in the online environment.

---

21. "Public websites" are operated by the government or public agencies, or operate under a governmental license. "Private websites" are independently owned and managed by private entities. "Popular websites" are drawn from a list of most frequently visited websites. "Sensitive websites" are commercial sites that provide services usually considered to be private, such as health or financial services. For the relevant definitions and discussion of these categories, see *infra* Part III.

I. PRIVACY AND INFORMATION PRIVACY REGULATION

A. *Conceptions of Privacy*

Privacy is both a social norm and a legal concept. These cultural constructs are interdependent and evolve with changing technologies. Perhaps the most uncontroversial statement regarding privacy is that it is a contested concept. In order to provide the reader with background regarding informational privacy, we begin with a concise overview of the theoretical map of privacy.

There are many conceptions of privacy, and the term is invoked to cover a wide range of interests, such as the wish to remain secluded, the power to prevent disclosure of private information, control over commercial use of one's name and likeness, the desire not to be presented in a false light, or the right to make intimate decisions without interference.[22] There are two principal understandings of the right to privacy in personal data: privacy as a right to control data ("privacy as control") and privacy as a right to prevent access ("privacy as access").[23] Privacy as control emphasizes a person's ability to control her data, activities and any other aspect of her individual autonomy.[24] Privacy as access emphasizes the border between the individual and others and empowers the individual to prevent unwanted access. Ruth Gavison presented a comprehensive view of privacy as a concern over one's accessibility to others, identifying three primary interests: "the extent to which we are known to others, the extent to which others have physical access to us,

---

22. For a well-known early discussion of privacy as seclusion, see Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). For a discussion of privacy as control against unwanted disclosure, appropriation and false presentation, see RESTATEMENT (SECOND) OF TORTS § 652A (1965) and William L. Prosser, *Privacy (A Legal Analysis)*, 48 CAL. L. REV. 383 (1960). For background on decisional privacy, see *Griswold v. Connecticut*, 381 U.S. 479 (1965) and ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY (1995).

23. For a discussion of privacy as control, see WESTIN, *supra* note 2, at 7. For a background on privacy as access, see Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE L.J. 421, 428 (1980).

24. The idea of privacy as control is usually attributed to sociologist Alan Westin. *See* WESTIN, *supra* note 2. This conception sometimes redefines privacy as property, though control and property do not necessarily overlap. For a discussion of the "privacy as property" argument, see LAWRENCE LESSIG, CODE: VERSION 2.0 228–30 (2006). This view is both unnecessary and problematic. First, there is no need to conceptualize one fundamental human right in terms of another right, especially the right to personal property, which in itself has several differing conceptions. Second, once we equate privacy with property, it enables the quick commodification of people, which contradicts the privacy interests. For criticism of the privacy as property model, see Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as an Object*, 52 STAN. L. REV. 1373, 1377–92 (2000) and Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2076–94 (2004).

and the extent to which we are the subject of others' attention."[25] She termed these interests secrecy, anonymity, and solitude.[26]

However, even within these two conceptions, privacy covers many different interests. Moreover, once we focus on the threats to privacy, another important distinction is apparent. A common threat to privacy, like any other human right, lies with government. George Orwell's "Big Brother" is the metaphor commonly used to describe this concern, presenting privacy as a matter of liberty and protecting citizens vis-à-vis the state.[27] This view is primarily associated with the United States.[28] Other jurisdictions are more likely to focus on threats posed by the market. Various individuals and corporations maintain data on individuals.[29] Individuals are thus both *citizens* of the state and *data subjects*. This threat is relatively new, dating to the early 1970s, and is a product of the emergence of computing and new business practices based on data management, including the collection, processing and onward transfer of personal data.[30] New developments in information technologies further enhance the possibilities for capturing personal data, therefore multiplying the concerns related to privacy. Moreover, the distributed online environment weakens the traditional mechanism of enforcement by sovereign states and also enhances the active collaboration between state players and the private sector in collecting and processing information on individual users.[31] As we have argued elsewhere, this development blurs the distinction between state actors and market players and introduces a new category of threats to privacy.[32]

Articulating the threats to individual privacy requires a deeper and broader basis than the concept of liberty. The fundamental value of *human dignity* provides such a basis. Human dignity is a fundamental principle of some legal systems, such as those of Germany and Israel.[33]

---

25. Gavison, *supra* note 23, at 423. For current views of "privacy as access," applying and updating Gavison's analysis to the digital environment, see Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, 15 INFO. SOC'Y 141, 142 (1999), *available at* http://www.nyu.edu/projects/nissenbaum/paper_anonimity.html.

26. Gavison, *supra* note 23, at 428.

27. *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

28. *See* Whitman, *supra* note 15. The government is thus subject to constitutional limitations on its powers. However, governmental cooperation with the market might bypass these limitations. *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003).

29. Schwartz, *Property*, *supra* note 24, at 2056–57.

30. For discussion of this threat in the Israeli context, see for example, Ministry of Justice, Report of the Committee on Preventing Harm to Citizens by Data Stored in Computers (1981) (Isr.).

31. *See* Birnhack & Elkin-Koren, *supra* note 28, at 3.

32. *See id.*

33. *See* GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [BASIC LAW FOR THE FEDERAL REPUBLIC OF GERMANY] [CONSTITUTION] May 8, 1949 (as amended through Dec.

Several meanings are offered for dignity, but all share a set of Kantian principles, according to which all persons should be treated as inviolable.[34] The understanding of privacy as a matter of dignity is often thought of as a European view.[35] Once privacy interests are understood in this manner, it does not matter whether the source of the threat emanates from the government or the market. The relevant idea is that each person has the power to determine who may do what with his personal data. Significantly, while the dignity conception of privacy can encompass liberty interests, the opposite does not necessarily hold: the liberty conception is generally narrower, in that it focuses mostly on the protection of the citizen vis-à-vis the state.

Today, we are witnessing the emergence of a third kind of threat: one's peers.[36] Adding a new "friend" to one's personal page on a social network might expose the friend's information to third parties, enable tagging of the friend's photos, and unfavorably alter the results of a search engine query. Privacy law has not yet addressed this new threat category.

The task of defining privacy is rendered almost impossible by the broad range of interests covered by the term, divergent conceptions of privacy, and the dynamic business, cultural, and technological environments in which the concept must interact. Daniel Solove thus suggests that instead of searching for a core element of privacy, we should settle for understanding it "as a set of protections against a plurality of distinct but related problems."[37] Accordingly, he offers a taxonomy of privacy, divided into groups of harmful activities which the law should address, including information collection, processing, dissemination and invasion.[38] Each category is further sub-divided.[39]

1993), art. 1(1) ("Human dignity shall be inviolable."); Basic Law: Human Dignity and Liberty, 5752–1992, SH No. 1391, § 2 (Isr.) ("There shall be no violation of the life, body or dignity of any person as such.").

34. For example, in the famous "census case," the Federal Constitutional Court of Germany, articulated a right to self-determination concerning personal data based on the notion of human dignity. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1 (Ger.). For an English-language summary, see *Privacy, Property, Personality—Germany Case List*, ARTS & HUMAN. RES. COUNCIL, http://www.law.ed.ac.uk/ahrc/personality/gercases.asp#Volksz%C3%A4hlung (last visited Apr. 3, 2011).

35. Whitman, *supra* note 15, at 1161.

36. This category of peer-surveillance is sometimes referred to as coveillance. *See* Steve Mann et al., *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURVEILLANCE & SOC'Y 331, 338 (2003).

37. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 171 (2008).

38. *Id.* at 101.

39. *Id.* at 103.

Another way to organize the various aspects of privacy is to identify categories of its subject matter. Privacy in "places" is one such category, under the caveat that privacy belongs to people and not to places.[40] Most legal systems protect one's behavior in certain places, with the home as the quintessential private place.[41] The degree of protection varies, of course, and is in any case not absolute. A second privacy category is privacy in communications; for example, wiretapping or opening someone else's letters without permission are violations of privacy. Two other categories, decisional privacy and informational privacy, are more controversial as independent categories. Decisional privacy provides a person with the power to make intimate decisions without governmental interference. Examples include the decision to use contraception or to have an abortion.[42] These rights are classified in American law as matters of privacy, while in Europe (and Israel) the same interests are more likely to be framed as matters of autonomy or dignity, related to privacy yet understood as a separate legal principle. Helen Nissenbaum frames the concept of privacy differently, calling it contextual integrity.[43] According to this view, "privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information."[44] The appropriateness of the flow is determined, according to Nissenbaum, by reference to the expectations of the people who engage in a specific social context.[45]

The last category—informational privacy—is also controversial. Under this category, information about a person is a matter of privacy. While American law protects only specific enumerated kinds of personal data, European law protects *all personal data*, defined broadly as identifying or identifiable data.[46] This American-European legal divergence reflects the ideological divide. The liberty conception of privacy protects privacy interests, but it limits the protection to specific kinds of information against governmental intrusions.[47] The dignity conception of privacy protects *all* kinds of personal information and provides protection

40. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

41. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 36–38 (2001) (discussing the importance of the home to human activity).

42. *See* Roe v. Wade, 410 U.S. 113, 154 (1973) (holding that the constitutional right to privacy is broad enough to include a woman's decision whether or not to terminate her pregnancy); Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (holding that a law forbidding the use of contraceptives unconstitutionally intrudes upon the right of marital privacy).

43. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 127 (2010).

44. *Id.*

45. *Id.*

46. *See* Data Protection Directive, *supra* note 17, art. 2(a).

47. *Id.*

against anyone or anything that may threaten it.[48] This Article places the dignity conception of informational privacy under the spotlight.

Regardless of what conception of privacy holds sway, privacy itself is under constant attack from a coalition of stakeholders and various ideologies. Law enforcement agencies often portray privacy as an obstacle to national security;[49] freedom of speech and the press more generally are limited by privacy;[50] feminists warn against reconstructing the private/public divide;[51] economists argue that privacy is an obstacle for the free flow of information which is crucial for proper functioning of a free market.[52] Finally, in connection with the latter critique, businesses are interested in an uninhibited informational market that serves their marketing and other business purposes.[53]

The concept of privacy is complicated and troublesome, but it is nevertheless adequate for the purposes of this Article. Within the framework presented here, the current research focuses on the category of privacy in information, examining a legal regime which purports to be universal and comprehensive in the European model, a regime which is better explained under the *privacy as control* conception of privacy, but does not necessarily negate the alternative *privacy as access* conception. We examined both governmental (and other public) websites and private websites of various kinds in order to compare the two principal categorical threats to informational privacy: the government and the market. The practices fall within Solove's taxonomy under the headings of collection,

---

48. The theoretical gap that underlies the legal divergence creates a practical problem. The ease with which information crosses borders makes it difficult to assure that the privacy of citizens are protected as defined by applicable laws of a given jurisdiction. The EU attempts to limit the transfer of personal data to jurisdictions that do not offer sufficient protection. Thus, the U.S.-EU gap required a solution. This was devised in the form of a safe harbor that enabled American firms to handle European personal data. *See, e.g.*, Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC); *U.S.-E.U. & Swiss Safe Harbor Frameworks*, EXPORT.GOV, http://www.export.gov/safeharbor (last updated Mar. 31, 2011).

49. Privacy is viewed as a vehicle for protecting the secrecy of (sometimes illegal) activity. Reducing privacy protection is perceived as a means for eliminating obstacles that may interfere with the use of surveillance for law enforcement purposes. For further discussion of these competing values see Jeremy Waldron, *Security and Liberty: The Image of Balance*, 11 J. POL. PHIL. 191 (2003).

50. For example, when the media joins the police while conducting arrests in homes, privacy and free press conflict. *See, e.g.*, Wilson v. Layne, 526 U.S. 603 (1999).

51. *See* CATHARINE MACKINNON, *Privacy v. Equality: Beyond* Roe v. Wade, *in* FEMINISM UNMODIFIED: DISCOURSES ON LIFE AND LAW 93, 93 (1987).

52. For a pre-Internet era economic analysis of privacy, see RICHARD A. POSNER, *An Economic Analysis of Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 333 (Ferdinand David Schoemen ed., 1984).

53. For an argument explaining the business importance of collecting data, see FRED H. CATE, PRIVACY IN PERSPECTIVE 10–17 (2001).

processing, and dissemination of information.[54] Framed in Nissenbaum's thesis, the law is insensitive to the particular social contexts.[55]

B. *The Legal Layer*

The American liberty and the European dignity conceptions of privacy translate into two distinct legal regimes. The law of the United States protects individual privacy interests against governmental encroachment even though privacy is not mentioned in the Constitution, but does not provide a general, universal right to privacy in other contexts. Instead, U.S. federal law provides a set of legal regulations tailored to several sectors. Examples include the Fair Credit Reporting Act of 1970 (FCRA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Children's Online Privacy Protection Act of 1998 (COPPA).[56] This sectoral approach provides informational privacy protection in enumerated activities, but has a far narrower scope than a general legal privacy regime.[57]

The European dignity view of privacy provides such a general right to privacy.[58] The general right is particularized in regional and local instruments. Within the Council of Europe, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention 108") provides a principled framework for regulating privacy.[59] Within the European Union, Directive 46/95/EC provides a detailed regulatory mechanism.[60] As the titles of these instruments indicate, the main privacy category is that of informational privacy, or, to use the European terminology, data protection.

The European legal mechanisms are part of a larger picture. Beginning in the early 1980s, the enactment of a series of international instruments—generally "soft law" declarations and guidelines—addressed the regulation of personal data, including transborder transfers

---

54. *See* SOLOVE, *supra* note 37.

55. *See* NISSENBAUM, *supra* note 43.

56. *See* Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2006); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201 (2006); Children Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06 (2006) (regulating the online collection and processing of data from children under the age of thirteen).

57. Several American scholars advocate the recognition of a general category of informational privacy in the U.S. *See* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1087 (2006).

58. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1, 10; European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

59. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108. The Convention is also open to countries which are not members of the Council.

60. *See* Data Protection Directive, *supra* note 17.

(within the EU, the Directive is mandatory, and thus "hard law"). These instruments include the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* of 1980;[61] the 1990 UN Guidelines Concerning Computerized Data Files;[62] the Asia-Pacific Economic Cooperation (APEC) Privacy Framework of 2004;[63] and a series of declarations by a group of national data protection commissioners in 2005 and onwards.[64] Viewed together, these legal instruments form the foundations of an emerging global data protection regime.[65]

This emerging regime, comprising such sources as the OECD Guidelines, the CoE Convention, the EU Directive, and U.S. federal laws that provide privacy protections, exhibits strikingly similar standards derived from the same core principles.[66] These principles can be understood under either the control or access conceptions of privacy, conform with both the liberty and dignity models, and fit nicely within Solove's privacy taxonomy.[67] The set of principles relates to *personal data*, which can be defined in various ways.[68] The resulting legal mechanisms impose several duties on those who collect, process, and transfer such data, accord certain rights to data subjects, and includes various means of enforcement.

The core principles are notice, choice, limited use, access and rectification, confidentiality, and data security. Some jurisdictions and legal

---

61. OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

62. Guidelines for the Regulation of Computerized Personal Data Files, G.A. Res. 44/132, U.N. GAOR, 44th Sess., Supp. No. 49, U.N. Doc. A/44/132, at 211 (Dec. 5, 1989).

63. ELEC. COMMERCE STEERING GRP., ASIA-PAC. ECON. COOPERATION, APEC PRIVACY FRAMEWORK 8–19 (2004), *available at* http://www.apec.org/en/Press/News-Releases/2005/~/media/Files/Press/NewsRelease/2005/04_amm_014rev1.ashx.

64. *See, e.g.*, *Montreux Declaration: The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities*, 27TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS (2005), http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf; *Resolution on International Co-operation*, 29TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS (2007), http://www.privacyconference2007.gc.ca/Resolution%20on%20Global%20cooperation%20-English.pdf; *Resolution on Privacy by Design*, 32ND INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS (2010), http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf.

65. Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SEC. REP. 508, 508 (2008).

66. *See id.* at 511.

67. *See* SOLOVE, *supra* note 37, at 171.

68. One way to define "personal data" is to list the kinds of data that are considered personal. This is the current approach of the Israeli law. *See* Privacy Protection Act, 5741–1981, 1011 LSI 128, § 7 (1980–81) (Isr.). Another way is to define "personal data" in a general manner; this is the approach taken in the European Union. *See* Data Protection Directive, *supra* note 17, art. 2(a); Kang, *supra* note 13, 1206–08 (1998).

frameworks contemplate additional core principles, such as a relevance requirement found in the EU Directive (referred to therein as the quality and proportionality principles),[69] or additional enforcement-related principles.[70] Given that these principles are stated as general standards and do not in themselves contain sufficient instructions, they require particularization. The implementation and interpretation of these principles vary, but they create common ground to facilitate the international flow of personal data. Instead of drawing a broad range of possible implementation strategies, we shall turn to the Israeli data protection regime, which encompasses most of these core principles and serves as the case study for the Privacy Study discussed in this Article.

C. *Israeli Informational Privacy Regulation*

The Privacy Study examined compliance of websites with the Israeli privacy law. The Israeli informational privacy regime is more closely related to the European model of data protection than to the thin sectoral regime in the United States.[71] The European model provides a general right to informational privacy in a detailed regulatory regime, imposing a series of duties upon processors of personal data.[72]

Privacy is considered a fundamental human right under Israeli law and is guaranteed by section 7(a) of the Basic Law: Human Dignity and Liberty, which declares that "[a]ll persons have the right to privacy and to intimacy."[73] Privacy was also protected before the enactment of the Basic Law in 1992, in the Privacy Protection Act of 1981 (PPA).[74] The PPA, a product of several expert committees in the 1970s and early 1980s, was one of the first privacy laws of its kind in the world.[75] The statute achieves a comprehensive scope, addressing various categories of privacy, including privacy in places, in communications,

69. *See* Data Protection Directive, *supra* note 17, art. 6.

70. *See id.* art. 28 (requiring Member States to establish a supervisory authority).

71. *See* Whitman, *supra* note 15, at 1193.

72. *See supra* Part I.

73. Basic Law: Human Dignity and Liberty, 5752–1992, SH No. 1391 (Isr.).

74. Privacy Protection Act, 5741–1981, 1011 LSI 128 (1980–81) (Isr.).

75. The overall Act is based on recommendations of the Cohen committee, chaired by Supreme Court Justice and later Chief Justice Yizhak Cohen. *See* Ministry of Justice, Committee on the Protection from Harm to the Privacy of the Individual (1976) (Isr.). Other members of the committee included Aharon Barak, later the Chief Justice of the Supreme Court, Professor Ruth Gavison, and Dr. Gabriel Kling. The second committee focused on databases, and its recommendations provided the basis for Chapter 2 of the PPA. It was chaired by Knesset Member David Glass. *See* Ministry of Justice, Report of the Committee on Preventing Harm to Citizens by Data Stored in Computers (1981) (Isr.). A third committee, chaired by Haim Klugman of the Ministry of Justice, formed the basis of Chapter D of the PPA, which regulates governmental and public data transfers. *See* Ministry of Justice, The Committee on Transferring Data Between Public Bodies (1982) (Isr.).

and—significantly for the current debate and our research—informational privacy under various provisions, including a detailed chapter dedicated to databases.[76] Israeli law thus long ago chose the European understanding of privacy. The so-called "constitutional revolution" of 1992, which emphasized the centrality of human dignity as a foundational concept in Israeli law, strengthened the European orientation which was already present in Israeli privacy law.[77]

Chapter B of the PPA forms a five-prong regulatory regime. First, it requires *registration* of certain databases with the Database Registrar.[78] A database is defined, with some exclusions, as any non-manual collection of data.[79] Several factors can trigger the registration duty: the number of data subjects contained in the database (exceeding 10,000 subjects); the kind of data (when the data is sensitive, as defined in section 7, referring to data content in several situations); the source of the data (when the source is not with the data subject); the owner of the data (a public body); and the purpose of the data collection (direct marketing).[80]

Second, the PPA mandates *regulation* by the Database Registrar. The PPA provides the Registrar with certain powers, including discretion to refuse the registration of a database.[81] If a required registration is refused, the database is considered illegal and its operation should be prohibited.[82] The Registrar also has some investigatory powers and the legal authority to impose fines.[83]

Third, the law imposes a series of *duties* on database owners or their operators. The PPA requires a database owner to notify the data subject when collecting data to be kept in the database.[84] The notice requirement is central to our study, as it requires an explicit statement addressed to the subject. Section 11 reads:

> A request to a person for information with a view to keeping and use thereof in a database shall be accompanied by a notice indicating—

---

76. *See* Privacy Protection Act, 5741–1981, 1011 LSI 128, §§ 7–17I (1980–81) (Isr.).

77. For a general discussion of the Constitutional Revolution, see Daphne Barak-Erez, *From an Unwritten to a Written Constitution: The Israeli Challenge in American Perspective*, 26 COLUM. HUM. RTS. L. REV. 309, 311 (1995). For its implications for privacy, see HCJ 8070/98 ACRI v. Ministry of Interior, 58(4) PD 842 [2004] (Isr.)

78. *See* Privacy Protection Act, §§ 8–9 (Isr.).

79. *Id.* § 7.

80. *Id.* § 8(c).

81. *Id.* § 10(a)(1).

82. *Id.* §§ 8(a)(1), 10(b)(2).

83. *Id.* § 10(e)–(f).

84. *Id.* § 11.

(1) whether that person is under a legal duty to deliver that information or whether its delivery depends on his volition and consent;

(2) the purpose for which the information is requested;

(3) to whom the information is to be delivered and the purposes of such delivery.[85]

Notice is thus a prerequisite for consent, reflecting the underlying theories of privacy as either control or access. As indicated by the PPA's notice requirements, Israeli privacy law is based on a principle of consent. If an internet user consents to an act that would otherwise amount to a violation of her privacy, then consent eliminates the harm.[86] Consent should be informed, but can be either explicit or implicit.[87]

Where the user is unaware of the prospective uses of the data, it is meaningless to say that she has consented to data collection. Once she freely consents, based on her understanding of prospective uses, to provide the requested data, she has given informed consent. Providing information based on a true choice means that the data subject has exercised control over her privacy; it means that the person actively permitted access to her person. Thus, notice is not a mere technical duty. Rather, it reflects the most basic understanding of privacy as dignity. Whether viewed under the privacy as control model (where the data subject exercises control over the elements of her privacy) or the privacy as access model (where the subject allows access to her data), the presence of informed consent is the key distinguishing factor between personal and external control of personal data.

Consent does have limits. The consent model may fail when the party asking for data and the data subject have unequal power vis-à-vis each other. The employment context is a common example.[88] A second consent-failure scenario occurs when data subjects fail to comprehend the notice provided, thus failing to make a meaningful choice.[89]

Significantly, the PPA does not state exactly how notice should be given: the proper location, wording, visibility, and comprehensibility of notice are left to the data collector's judgment. Consistent with the

85. *Id.*

86. *See id.* § 1.

87. *Id.* § 3.

88. A recent decision by the Israeli National Labor Court set rules for employee privacy in the workplace. *See* Labor Appeal 90/08 Issakov-Inbar v. State of Israel (2011) (Isr.). The opinion is based on the notion of unequal power of the employee and the employer.

89. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341 (Jane K. Winn ed., 2006) (providing a critical analysis of consent and its limits).

purposive approach to legal interpretation undertaken by Israeli courts,[90] the notice duty should be read to achieve the purpose of the PPA as indicated by its name—protection of privacy. Further, the PPA must be interpreted in light of general principles of the Israeli legal system, such as the fundamental duty of good faith which applies to all actions subject to private law—a general duty of fairness throughout public law.[91] Moreover, the notice duty has a close kinship to the law of consumer protection, which requires businesses to be transparent about their consumer practices.[92]

Database owners and operators also have explicit duties to keep data confidential and to provide data security.[93] The latter duty is generally stated, but accompanying regulations provide more specific rules.[94]

Fourth, the database owner is obligated to respect the *rights* of the data subjects. These rights are explicitly granted to data subjects under the PPA.[95] The PPA allows the subject to access his personal data held in the database.[96] There are some qualifications to this right, including exceptions when the data relates to the subject's mental health and the database owner believes that disclosure might harm the person, and reservations based on national security and law enforcement needs.[97] The PPA further allows the data subject to require the amendment or deletion of incorrect, inadequate, or outdated data.[98] Moreover, the data subject has rights correlating to the duties imposed on the database owner regarding notice, confidentiality, and data security.[99]

Notably, other than the notice requirement, the other rights and duties (confidentiality, data security duties, access, and rectification rights), if properly observed, do not require that the data subject be informed thereof.[100] In other words, only the notice duty mandates that information

---

90. *See* Aharon Barak, *A Judge on Judging: The Role of a Supreme Court in a Democracy*, 116 HARV. L. REV. 16, 28 (2002) (explaining that a judge's role is to "understand the purpose of law in society and to help the law achieve its purpose").

91. For a discussion of the principle of good faith in Israeli private law, see CA 9/82 Beit Yules Ltd. v. Raviv Moshe & Co., 43(1) PD 441 [1989] (Isr.). For background on the fairness principle in Israeli administrative law, see HCJ 164/97 Kontram Ltd. v. Ministry of Fin.—Customs Dep't, 52(1) PD 289, 316 [1998] (Isr.).

92. *See* Consumer Protection Act, 5741–1981, 1023 LSI 248 (1981) (Isr.).

93. Privacy Protection Act, 5741–1981, 1011 LSI 128, §§ 16–17 (1980–81) (Isr.).

94. *See* Privacy Protection Regulations (Conditions for Holding Data and Protecting It, and Arrangements for Transferring Data Between Public Bodies), 1986, 4931 KT 858 (Isr.) (discussing conditions for data storage and transfer of information among public agencies).

95. Privacy Protection Act, §§ 13–15 (Isr.).

96. *Id.* § 13.

97. *Id.* § 13(e).

98. *Id.* § 14.

99. For example, the data subject can sue the database owner or operator for failing to perform duties under the PPA. *Id.* § 31B.

100. *See id.* § 11.

be conveyed to the data subject before obtaining the subject's data.[101] Of course, a court might reach the conclusion that in order to fulfill the requirement of informed consent, additional information is needed, but to date no court has ruled to this effect.

The fifth prong is *enforcement*. The PPA invests the Database Registrar with investigative powers, limited prosecution powers, and the authority to deny registration in some cases.[102] The Act also creates causes of actions for data subjects; a violation of the duties imposed on the collecting party or the denial of rights afforded to data subjects is both a criminal offense and a tort.[103]

In practice, the five-prong regulatory regime described above is far from perfect. There is a general consensus among data protection agencies (including the Registrar) and privacy experts that the regulatory registration system has failed.[104] An Expert Committee report ("Schoffman Report") estimated that only two percent of all databases are registered.[105] Enforcement is also lacking, and very few data subjects have initiated proceedings under Chapter B of the PPA.[106] This situation led to the appointment of an expert committee chaired by Israel's Deputy Attorney General.[107] In 2007, the committee recommended a series of amendments to the PPA, including a major limitation on the registration duty, a strengthening of substantive duties imposed on databases, the strengthening of data subjects' rights, and a series of incentives to enforce these recommendations, including new statutory damage and class action provisions.[108] As of the time of publication of this Article, the recommendations have not yet materialized into actual amendments, but these are expected within the foreseeable future.

Another important development in Israeli data protection involves the establishment by the Ministry of Justice of a new agency, the Israeli

---

101. *See id.*

102. *Id.* § 101(A)(1).

103. *Id.* § 31. An expert committee also recommended enhancing the Registrar's powers in addition to enabling class actions and statutory damages. *See* Ministry of Justice, Committee for the Examination of Legislation Relating to Databases, 42–43 (2007) (Isr.) [hereinafter Schoffman Report], *available at* http://www.justice.gov.il/NR/rdonlyres/B11D19EE-7FC0-42ED-B2F5-2B4FDEE66BD4/18343/SchoffmanReport1.pdf.

104. *See id.* at 26. The Schoffman Report recommended limiting the registration duty. *Id.* at 35. In the interest of disclosure, one of the authors, Michael Birnhack, was a member of the committee. *See* Omer Tene, *Israeli Data Protection Law: Constitutional, Statutory and Regulatory Reform*, 8 PRIVACY & DATA PROTECTION 6 (2007) (reviewing recent changes in Israeli data protection law and assessing its adequacy under European standards).

105. Schoffman Report, *supra* note 103, at 8.

106. *Id.* at 7.

107. *Id.*

108. *Id.* at 8–9.

Law Information Technology Agency (ILITA).[109] In late 2009, the professional data protection unit of the EU recommended a declaration that Israel maintains an adequate data protection regime,[110] and in January of 2011, the European Commission accepted the recommendation.[111] The declaration would streamline data transfers between the EU and Israel while maintaining a high level of privacy protection.[112]

In sum, the Israeli data protection regime is aligned with the European privacy standards and includes a complex and detailed legal regime for the regulation of personal data. The most important provision is the notice requirement, which mandates that certain information be given to the data subject before collecting data. The information must include whether there is a duty to provide data, the purpose of the data collection, to whom it will be transferred, and for what purposes.[113] The notice requirement does not cover information about other duties acting on the database holder or other rights of the data subject. Any additional information conveyed thus exceeds the legal requirements of the PPA, although there is no prohibition on providing such information. The legal contours of the notice requirement enable us to examine both whether database holders comply with the law (i.e., the notice requirement), and to identify the cases where the database holders go beyond the legal requirements.

II. ONLINE COMPLIANCE

A. *Overview*

The Privacy Study explored the information privacy practices of websites and the extent to which they comply with applicable legal requirements related to information privacy. Previous studies exploring these practices in various jurisdictions examined specific categories of websites (i.e., children's or health websites) or a limited number of

109. *See About the Israeli Law, Information and Technology Authority*, MINISTRY OF JUST., http://www.justice.gov.il/MOJEng/ILITA/About.htm (last visited Feb. 15, 2011).

110. *See* Article 29 Data Protection Working Party, Opinion 6/2009 on the Level of Protection of Personal Data in Israel, 02316/09/EN, WP 165 (Dec. 1, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp165_en.pdf.

111. *See* Commission Decision, 2011/61/EU, 2011 O.J. (L 27) 39, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:EN:PDF.

112. Note that the adequacy finding does not mean that the laws are identical. Indeed, the Israeli data regime lacks an explicit data quality and proportionality requirement. Thus, a data collector may state any legal purpose for collection and may, upon notice, collect data in excess of that needed for the immediate intended purpose. *See* Omer Tene, *Is Israeli Data Protection 'Adequate' Under Article 25?*, PRIVACY & DATA PROTECTION, Apr.–May 2008, at 9, 10.

113. Privacy Protection Act, 5741–1981, 1011 LSI 128, § 11 (1980–81) (Isr.).

popular websites.[114] The purpose of the Privacy Study was to provide a comprehensive picture of a particular regime and to track the differences in compliance levels with information privacy regulation in different sectors.

We hypothesized the presence of a substantial gap between legal requirements and information privacy practices. Based on the results of our 2003 Study, our subjective impressions, and our familiarity with the Israeli privacy community's views, as well as the European privacy discourse, we assumed that only a few websites conform to the law. We also predicted a high level of deviation in compliance with different legal rules. Finally, we assumed that different sectors (e.g., the public and private sectors) as well as particular sub-categories of websites would manifest different levels of compliance.

Information practices were explored at three levels: first, as discussed in Part II, we examined the legal requirements which apply to each information practice under current Israeli law (legal analysis); second, we analyzed the declared privacy policies posted on each website; and third, we studied the actual information practices of each website.

The study focused on 1360 Israeli websites active from 2006 to 2007.[115] The Israeli online sphere provides a unique case study for two reasons. First, the few studies that have examined privacy practices of websites in other jurisdictions studied mostly American and English websites.[116] The current study explores the efficacy of the denser European-style legal regime in regulating online privacy, thus providing a basis for comparative analysis with studies of American websites.

Second, notwithstanding Israel's relatively high Internet penetration rate, the relatively small population size enabled us to study the entire population for some categories of websites.[117]

---

114. *See, e.g.*, COMPLIANCE CHECK PROJECT, STUDY OF COMPLIANCE WITH THE DATA PROTECTION ACT 1998 BY UK BASED WEBSITES (2002), *available at* http://www.privacydataprotection.co.uk/pdf/website_compliance_report.pdf; JOSEPH TUROW, PRIVACY POLICIES ON CHILDREN'S WEBSITES: DO THEY PLAY BY THE RULES? (Annenberg Pub. Policy Ctr., Report Ser. No. 38, 2001), *available at* http://www.asc.upenn.edu/usr/jturow/Privacy%20Report.pdf.

115. The study was performed in 2006 by a team of law students. Inter-coder reliability was examined and consistency was achieved. All forms completed by the examiners were forwarded to the Statistics Consultants. Data was coded and ambivalent data was marked and addressed individually.

116. *See, e.g.*, COMPLIANCE CHECK PROJECT, *supra* note 114, at 5; TUROW, *supra* note 114, at 2.

117. The Internet penetration rate in Israel is one of the highest in the world, reaching over seventy-five percent as of March 2009. *See Internet Usage Statistics*, *supra* note 19. A country's Internet penetration rate is the ratio between the aggregate number of Internet users speaking a language and the total estimated population of speakers of that language. *Internet World Users By Language*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats7.htm (last updated Mar. 26, 2011).

We defined "Israeli websites" using a formal two-part test to assure that the websites are subject to Israeli law. Thus, we studied only websites that were: (1) registered under the Israeli Country Code Top Level Domain (ccTLD) (<.il>), and among these, 2) registered up to the third-level domain name (3LD).[118] The rationale for the first test is that the uniqueness of the Hebrew language makes it unlikely that a foreign firm would register its non-Israeli website with an Israeli ccTLD.[119] We assumed that Hebrew websites registered in Israel are owned and operated by local citizens or firms and organizations that operate in Israel, and are therefore uncontroversially subject to Israeli law.[120] The second test's limitation to third-level domain names assured that fourth-level domain names are in most cases internal pages of the main website registered under the parent, 3LD website.[121]

In order to explore whether the rules carry a different impact on different types of online players, we studied four categories of websites: public websites, private websites, popular websites, and sensitive websites.

Public websites. Public websites consist of the following categories: gov.il (government and governmental agencies), ac.il (academic institutions), muni.il (municipal authorities), k12.il (elementary schools and kindergartens), and net.il (Internet Service Providers—ISPs).[122] Public law principles apply directly to the gov.il, muni.il and k12.il public schools; academic institutions are either public organizations subject to administrative law or universities and colleges that courts subject to pub-

---

118. I.e., the study covered ynet.co.il, but not ynet.co.il/culture or culture.ynet.co.il.

119. These websites are registered with the Israeli Chapter of the Internet Society (ISOC-IL), a private, non-profit organization responsible for the registration of the <.il> domain names. *See Domain Registration*, ISR. INTERNET ASS'N, http://www.isoc.org.il/domains/registration.html (last visited Aug. 30, 2010).

120. Some Israeli entrepreneurs, however, may have registered their websites under non-Israeli domain names, such as .com. These websites might also be subject to Israeli law, but were not part of the current research.

121. This choice is also dictated by a statistical limitation, as the number of domain names in 3LD is known (due to ISOC's allocation process), but the number of internal pages or sub-sites is unknown.

122. *See Domain Registration*, ISR. GOV'T TECH, http://www.itpolicy.gov.il/registrar/gov-1.htm (last visited Oct. 30, 2010). ISOC-IL rules for domain name allocations assure that most of these are indeed "public websites," i.e., that they belong to public organizations or are of a public nature and subject to the same legal regime. <gov.il> 3LD is allocated by the Ministry of Finance. *Id.* For a listing of the allocation rules, see *Rules for the Allocation of Domain Names*, ISR. INTERNET ASS'N (Aug. 2010), http://www.isoc.org.il/domains/il-domain-rules.html. (<ac.il> is allocated to accredited academic institutions, after consultation with the Council for Higher Education. <muni.il> is allocated to municipal bodies, according to the official list published by the Central Bureau of Statistics. <k12.il> is allocated to kindergartens and schools as classified by the Ministry of Education. <net.il> is allocated to ISPs who are licensed by the Ministry of Communications).

lic law norms.[123] The ISPs were classified as "public" since they act under a governmental license and are subject to that extent to public law. Overall, 497 public websites were reviewed, constituting the entire population of these websites. We were also able to provide a temporal analysis by comparing current data to a prior study of public websites conducted in 2003 ("The 2003 Study").[124]

Private sector websites. The largest population of websites is that of commercial websites within the SLD (Second Level Domain) <co.il>,[125] and the second largest consists of <org.il> websites.[126] The co.il domain level is often a default category—i.e., if the party interested in registering the domain does not qualify for any other categories, it will register under the co.il group. Websites in this category are often operated by individual users or small businesses. Websites in the SLD <org.il> category include nonprofit organizations, non-governmental organizations, and individuals active in civil society. Each website is independently owned and managed by its owners.[127] A representative sample of randomly selected active websites was reviewed.[128]

---

123. Administrative law applies directly to public entities such as statutory bodies or governmental agencies. However, Israeli case law has extended the reach of administrative law so it also applies to some private bodies that perform public functions. These are known as bodies of "dual normativity," meaning that they are subject to both private and public norms. This Israeli doctrine is broader than the American "state action" doctrine. The Israeli Supreme Court also applied the dual normativity doctrine to universities. *See, e.g.*, AdminA 7151/04 Technion v. Dats 59(6) PD 433 [2005] (Isr.) (explaining the legal status of public universities as subject to certain common law rules of administrative law).

124. *See* Michael D. Birnhack & Niva Elkin-Koren, *Protection of Privacy on Israeli Public Websites*, Burda Center for Innovative Communications (2004), http://burdacenter.bgu.ac.il/publications/finalReports2003-2004/BirnhackElkin-Koren.pdf.

125. The count was 77,079 commercial website domain names of a total 89,725 registered domain names at the time of our research. The data was provided to us for the purpose of the Privacy Study by the Israeli Internet Society, which administers the ccTLD <.il>.

126. The count was 6289 registered domain names at the time of our research. The data was provided by the Israeli Internet Society, which also administers the ccTLD <.il>.

127. In some cases, a single entity may own several domain names and run several websites. However, our research unit was the website, rather than the owners thereof.

128. In order to ascertain the statistical significance of the sample and to ensure that it was randomly chosen, we had to know the size of the population, i.e., how many registered domain names were active at the time of the research. Apparently, many of the registered domain names had no active website. There is no official verified data about the number of active and inactive websites. Prior to performing our research, we estimated that up to a third of registered domain names are inactive, in the sense that their associated websites lack content. ISOC administrators shared our estimate. As indicated below, these estimates turned out to be rather modest—the actual number of inactive domain names was much higher. Hence, we expanded the initial draw of domain names: a random list of 1000 domains in <co.il> (commercial domains) and <org.il> SLD was provided by ISOC-IL. We then examined which domains had affiliated active websites. We repeated the process several times and identified 190 <org.il> and 736 <co.il> active websites. This provided a large enough group to validate the sample.

Most popular websites. Previous studies of online privacy policies conducted in other jurisdictions explored similar issues but were limited to popular or sensitive websites.[129] Needless to say, the privacy practices of these websites are of special interest due to the volume of website activity. The study reviewed the practices and policies of forty-five Israeli websites listed as the most popular at the time of the research.[130] Unlike the other groups that either covered the entire population of websites in their respective categories or constituted a random sample, this group was selected according to a pre-determined criterion: popularity. Thus, on an imagined curve of website popularity, the most popular websites are located at the beginning of the curve rather than the long tail.[131]

Sensitive websites. The last category of websites likely collects sensitive data from users. We compiled a list of 120 websites which, based on our analysis of their content, clearly engage in collecting and/or processing sensitive information. Sensitive websites were selected in six different categories: e-commerce, gambling, information/communication, dating, financial services, and health. The four examined categories of websites are listed in Table 1.[132]

---

129. *See, e.g.*, COMPLIANCE CHECK PROJECT, *supra* note 114, at 7; *SA Websites Fail the Privacy Test*, ALLAFRICA (Sept. 4, 2003), http://allafrica.com/stories/printable/200309050006.html; *Top UK Sites 'Fail Privacy Test,'* BBC NEWS (Dec. 11, 2003), http://news.bbc.co.uk/2/hi/technology/3307705.stm.

130. The list was compiled based on the results of an omnibus survey commissioned from a market research service (Teleseker Inc.), from April 2–10, 2006, among two representative samples of the population of adults and teenagers aged twelve to eighteen, regarding their surfing preferences. Telesekr Omnibus Research (Apr. 2006) (on file with authors). The survey produced an initial list of 135 websites, from which some websites were omitted (i.e., foreign sites in <.com>, <.net> TLDs, unidentified websites, or those selected twice, once by each group).

131. *See* ANDERSON, *supra* note 5, at 25 (illustrating the long tail curve as it applies to song popularity on one internet music subscription service).

132. In each category, there were some websites which were "inactive," "under construction," or redirected users to another website that had already been examined. These websites were classified "rejected." There is a particularly large group of rejected websites under the subcategory of <.net.il>. While visiting these websites during the research, we realized that ISPs in particular tend to register several domains that redirect users to a single website. Thus, except for the main active domain, all duplicate domains were rejected.

TABLE 1
WEBSITES ANALYZED

Type of Website	SLD	Source	No. Examined
Public Websites	**muni.il**	2003 Study & independent update	75
	gov.il	Tehila & complementary search	80
	k12.il	2003 Study & independent update	39
	ac.il	2003 Study & independent update	68
	net.il	2003 Study & independent update	19
	Sub-total		281
Commercial Websites	**org.il**	ISOC-IL random composition & activity filtering	190
	co.il	ISOC-IL random composition & activity filtering	726
Popular Websites	**co.il**	Survey by TeleSeker	45
Sensitive Website	**Free Internet search & Aladdin**	Content based selection: sensitive personal data	118
Total			1360

The information practices of each website were analyzed individually in order to determine the level of compliance with legal requirements, using a detailed questionnaire based on the PPA. The questionnaire contained three sets of questions. The first aimed at identifying websites subject to the duties defined by the PPA. As discussed in Part II, the PPA imposes duties on collectors of personal data and grants rights to data subjects regarding their data. The first set of questions was aimed at identifying the data at stake, determining whether it is collected and/or preserved, and determining how the data is used.

A second set of questions aimed examined "hard compliance," i.e., whether statements made on the website meet the PPA's formal notice requirement and whether the website disclosures go beyond that formal legal requirement.[133] The goal was to determine whether factors unrelated to the law were at work. For instance, our 2003 Study found that some

133. *See* Privacy Protection Act, 5741–1981, 1011 LSI 128, § 11 (1980–81) (Isr.). For instance, a website may declare its practices regarding the right of the data subject to access her personal data stored with the website, even though the PPA only requires the data collector to enable access and does not require the data collector to notify the data subject thereof.

websites provided information about their data security measures even in cases where it seemed information disclosure was not required.[134]

A third set of questions explored "soft compliance," i.e., actual practices of the websites, such as the visibility of the privacy policy, the title used for the policy, and other factors.

B. *Personal Data Collection Practices*

The Privacy Study also identified websites that collected personal data, as defined by law.[135] Such websites are subject to a variety of legal duties. Some of the PPA's duties are triggered when personal data is collected for the purpose of storage in a *database* as defined by the PPA.[136] This definition excludes databases intended for purely private use and those including only the name, address and means of communications ("contact information"), which in themselves do not characterize the data in a way that violates privacy rights.[137] Thus, we studied websites to identify those that collect personal data, likely held in a database, as defined under the PPA.

Some websites explicitly require personal data as a precondition for accessing or surfing the website. In other cases, acquiring goods or services involves the submission of personal data (e.g., credit card number, contact information, search queries, or publishing comments). We therefore defined websites that collect personal data as follows: any website that provides commercial products or services that require online payment, provides interactive services that record user inputs (search engines, chat rooms, forums, and online games), or requires the user to provide personal data beyond mere communications data.

Another set of questions sought to identify the types of data collected by the websites in order to exclude from the research those databases that are not subject to duties defined by the PPA (i.e., those that contain only contact information). We isolated those websites that required personal data (e.g., identification number, age, profession, income, credit card or real estate information) for obtaining a username

134. Birnhack & Elkin-Koren, *supra* note 28, at 19.

135. Privacy Protection Act, § 7 (Isr.) (defining "information," the equivalent of "personal data," to include "data on personality, personal status, intimate affairs, state of health, economic position, vocational qualification, [and] opinions and beliefs of a person").

136. *See id.* (defining "database" as "a collection of data, kept by magnetic or optic means and intended for computer processing" and listing exceptions).

137. *See id.* ("'[I]nformation' means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualification, opinion and beliefs of a person.").

and password or for accessing website content. These websites collect personal data as defined in the PPA, and hence trigger regulation.[138]

Finally, we examined the feasibility of providing false personal data in order to obtain a username. In such cases, the de facto threat to privacy is less severe, since users aware of this possibility can gain access to the website without disclosing their personal data.

The findings are presented in Table 2.

TABLE 2
DATA COLLECTION BY WEBSITES
(PERCENTAGE OF EXAMINED POPULATION OR SAMPLE)

Type of Websites		Websites Collecting Data	Websites Requiring Identification		Personal Data Required for Obtaining a Username or for Access	Feasibility of False Personal Data
			Of Total Websites	Of Data Collecting Websites		
Public Websites		81%	50%	62%	13%	51%
Private Websites	co.il	60%	56%	93%	13%	85%
	org.il	60%	45%	75%	8%	59%
Popular Websites		93%	84%	86%	53%	67%
Sensitive Websites		89%	84%	94%	49%	71%

These findings point to four main conclusions. First, a high percentage of websites in all subcategories collect users' personal data, with popular websites and sensitive websites at the top. This finding reaffirms the European (and Israeli) concern with the market threat to informational privacy. Second, the results indicate a gap between the public and private sectors; interestingly, the percentage of private sector websites that collect personal data was significantly lower than the rate for public websites. Third, over fifty percent of websites in all categories (except for <org.il> sites) required some level of identification from users. Identification is most likely to be required by popular and sensitive websites (84% of websites). Fourth, the results suggest that current mechanisms are not effective in validating user-provided data and preventing these users from accessing the website using false data. Among public

138. *See id.* (defining "information" subject to PPA regulation).

websites, the results show the lowest percentage of websites that facilitated the use of false data. In addition to findings regarding data collection practices, these results enable us to examine the websites' prima facie compliance with the law.

C. *Privacy Practices and Compliance with Legal Requirements*

In conducting a content analysis of the online privacy policies, we sought to determine whether websites that collect data comply with the legal requirements of the PPA. As discussed in Part II, the PPA imposes a series of *duties* on data collectors and database owners or their operators: notice, confidentiality and data security, and requirements to enable access and rectification.[139] Other than the notice requirement, the data collector is under no duty to notify the data subject of any of his rights. Therefore, other substantial rights may remain unknown to the subject.

We sought to determine the extent to which websites in each category disclose their information practices to users. Our objective was to evaluate compliance with the notice requirement and examine any additional pro-privacy attitudes.

1. Notice

A website seeking to collect personal data must first notify the data subject when data collection is intended for database storage.[140] Notice must take the form of an explicit public statement addressed to the subject.[141] Section 11 of the PPA requires that a notice specify (1) whether the data subject is under a legal duty to provide the data; (2) the purpose for which the information is collected; and (3) whether the data will be transferred to third parties and, if so, for what purpose.[142] Outside of these basic rules, the PPA does not list any requirements regarding additional content or the form or style of notice; these are left to the discretion of the data collectors.

Accordingly, the questionnaire aimed at exploring several practices. First, we examined "hard compliance" with the section 11 notice requirement. Second, we examined "soft compliance," considering various factors in the presentation of the notice, including presentation format (as a privacy policy or otherwise), visibility, and related parameters.

---

139. *Id.* §§ 11–17.

140. *Id.* § 11.

141. *See id.* (requiring data collectors to provide certain types of notice to data subjects); *id.* §§ 1, 3 (requiring data collectors to obtain consent and defining consent).

142. *Id.* § 11.

Third, we analyzed the content of the notices to examine whether the website provided more information than required by law.

Our content analysis also examined whether websites reserved the right to change the privacy policies at the owner or operator's discretion. If a website reserves this right, the mechanism of notice and consent offers little in the way of a guarantee of user privacy. In other words, if the user agrees upfront to any use of data as detailed by an adjustable privacy policy, the user does not exercise real control over the collection and use of personal data. A high percentage of data-collecting websites reserved the option to modify privacy policies: 69% of popular sites, 62% of sensitive sites, and 55% of commercial sites. Lower percentages were found for public sites (26%) and org.il sites (22%).

We examined "hard compliance" by reviewing the notice under various headings and evaluating compliance with the three sub-requirements of section 11. The findings are summarized in Table 3.

TABLE 3
"HARD COMPLIANCE" WITH THE NOTICE REQUIREMENT
AMONG WEBSITES THAT COLLECT PERSONAL DATA

Type of Websites		Notice exists (% of websites that collect data)—sec. 11	Reference to existence of legal duty to provide data (sec. 11(1))	Declare purpose for which data is collected (sec. 11(2))	Declare the transfers of data to third parties (sec. 11(3))	Details regarding third parties (% of those who transfer) (sec. 11(3))
Public Websites		22%	4%	28%	26%	56%[143]
Private Websites	co.il	16%	12%	58%	49%	67%
	org.il	19%	14%	43%	29%	17%
Popular Websites		76%	26%	65%	73%	65%[144]
Sensitive Websites		56%	16%	55%	54%	71%

These findings indicate a low level of compliance with the law. The public and private websites show an especially low level of compliance; of the 232 public websites that collect data, only fifty provided some

143. One would expect that the data for this column was calculated according to the number of websites declaring that they transfer data to third parties under the adjacent column. However, there were several websites that indicated the purpose of onward transfer, but did not specify the onward transfer itself.

144. *See supra* text accompanying note 143.

kind of notice. Compliance is more likely, but still low, among sensitive websites. Popular websites present the highest level of compliance; 76% of those that collect data provide notice. However, the vast majority of websites that provide notice fail to follow the specific notice content requirements of section 11. Compliance with the duty to notify users whether they are under a duty to provide the data is especially low. Compliance rates with the second prong of section 11, the duty to notify users of the purpose for which the data is collected, were slightly higher. Public websites were the least likely to comply (28% of the data-collecting websites provided notice), and popular websites showed the highest compliance levels (65%).

Compliance with the third prong of section 11, the duty to notify users whether the website transfers the data to third parties, is more difficult to assess, as websites that do not include such notice may simply not transfer the data to third parties. Hence, we examined whether the few websites that did notify users of the data transfer complied with section 11(3), which requires the website to disclose to the user to whom the data will be transferred. We found that compliance levels vary. The lowest level of compliance was recorded among <org.il> websites (17%), while there was a moderate level of compliance by public websites (56%) and better compliance rates by the commercial (67%), popular (65%), and sensitive (71%) websites.[145]

Interestingly, although some websites stated they were collecting users' personal data, we found no indication that they actually did so. This was a puzzling result, but there are several possible explanations. First, the website may collect data in some covert manner that we failed to detect. Second, the websites may intend to collect such data in the future and thus have already launched the framework for complying with legal requirements. A third possibility is that the website operators simply copied the privacy notice from other websites without adapting it to their actual data collection practices. Further research is needed to verify these hypotheses.

2. Purpose

As discussed, the PPA requires that data subjects be notified of the purpose of data collection. This requirement implicates a core principle of the PPA: the limited-purpose principle. Under section 2(9) of the PPA, data collected for one purpose cannot be used for another.[146] Section 8(b)

145. Transfer of personal data by public bodies is restricted under Chapter 4 of the PPA, which sets specific rules and imposes further duties on public data holders. Privacy Protection Act, § 23 (Isr.) (finding illegal certain data transfers from the Ministry to private bodies such as banks and public bodies such as the Broadcasting Authority).

146. Privacy Protection Act, § 2 (Isr.).

contains a similar principle regarding data held in databases.[147] The PPA does not state which purposes are legitimate, and it should be read to allow all purposes not prohibited by law.[148]

Given the ubiquity of commercial communications today (e.g., spam), we determined whether the communication of commercial data was specified as a purpose for collection of user data. At the time of the research, commercial communications were not specifically regulated by Israeli law. Only in 2009 was the law (the Communications Act) amended. Hence, the Privacy Study's results provide a pre-2009 basis for a comparative analysis with current, post-2009 compliance levels.[149]

Less than 50% of websites indicate that they use collected data for purposes of communication with the user. Popular websites were most likely to collect data, with 61% stating "commercial communications" as the purpose of the data collection in their privacy policies. In contrast, only 8% of the data-collecting public websites declare they will use data for the purpose of communicating with users, the lowest rate among study websites. This last finding is plausible, as many public bodies already have substantial user data.[150]

Some websites that state the intention to use users' data to communicate with the users also grant users a degree of control over their data. For example, an opt-out mechanism requires users to take steps to remove their information from the website's distribution lists. An opt-in mechanism, by contrast, requires user consent before websites or third parties can use the data for sending communications.[151] While less than 50% of data-collecting websites that comply with the notice requirement in the public and private sectors offer users a choice regarding future communication, a high percentage (76%) of the popular websites provided users with the opportunity to make such a choice. Unsurprisingly, most websites employed the opt-out mechanism, setting a default rule under which the website can freely send materials to users.

---

147. *Id.* § 8.

148. See CA 439/88 Database Registrar v. Ventura 48(3) PD 808 [1994] (Isr.), in which the Supreme Court affirmed the Registrar's decision to refuse to register an illegal database. The database at issue contained credit histories, thus violating § 2(9) of the PPA (stating that using information regarding a person's private affairs for a purpose other than that for which the information was provided constitutes a violation of privacy). Today, credit history services are regulated by a special statute. *See* Credit Data Service Act, 5762–2002, 1825 LSI 104 (2002) (Isr.).

149. *See* Amendment No. 40 to Communications Act, 5742–1982, SH No. 1060, 218 (Isr.).

150. For example, the Ministry of Transportation maintains the database of all licensed drivers, owners' of vehicles, etc., including means of communicating with them.

151. The study did not review means of providing user choice other than opt-in and opt-out mechanisms. In some cases, we were unable to determine whether a choice was offered.

TABLE 4
COMMUNICATIONS DATA PRACTICES

Type of Websites		Data is used for communicating with the user (% of websites that collect data)	Opt-out choice	Opt-in choice
Public Websites		8%	Data unreliable	Data Unreliable
Private Websites	co.il	51%	42%[152]	5%
	org.il	43%	22%	11%
Popular Websites		61%	57%	19%
Sensitive Websites		45%	41%	11%

3. Confidentiality and Data Security

A website collecting personal data is under a duty to keep the data confidential and to provide data security.[153] The PPA requires that data collectors provide data security, but they are under no legal obligation to announce this. Nevertheless, we found that a high percentage of websites claimed to provide data security, including 58% of sensitive websites, 55% of popular websites, and 51% of commercial websites. A substantially lower number of public sites (24%) carried a statement related to their data security. Only a small number of statements detailed the data security measures undertaken by the website.

TABLE 5
NOTICE ABOUT DATA SECURITY MEASURES

Type of Websites		Data Security Statement	Detailed Statement (% of those which have a data security statement)
Public Websites		24%	24%
Private Websites	co.il	51%	50%
	org.il	35%	44%
Popular Websites		55%	29%
Sensitive Websites		58%	34%

4. Access and Rectification Rights

Subject to several exceptions, a data subject has a legal right under the PPA to access his data held in the database and to require the

152. Not all of the data-collecting websites which declared that data will be used for future communication with users offered users a choice. The more interesting comparison is the ratio of opt-out to opt-in mechanisms, with a far greater number of opt-out options.

153. Privacy Protection Act, 5741–1981, 1011 LSI 128, §§ 16–17 (1980–81) (Isr.).

amendment or deletion of incorrect, inadequate or outdated data.[154] As with confidentiality and data security duties, the data collector, although required to enable access and rectification, is under no obligation to disclose to the user that such rights exist. We examined whether websites nonetheless provided such information.

A low percentage of websites informed users of their rights to review the data collected about them. The highest disclosure rates were among popular websites (21%), followed by <org.il> websites (14%) and commercial websites (10%) and sensitive websites (10%). Public websites had the lowest disclosure rates, with only 6% notifying users of their right to access personal data.

Similarly, only a few websites provided the means for updating data collected on the subject, even though the right to amend personal data is secured under the PPA.[155] Here again, the highest compliance levels were detected among popular websites (24%), <org.il> websites (17%), sensitive websites (15%), and commercial websites (11%). Only 7% of public websites provided a mechanism to amend personal data.

TABLE 6
ACCESS AND RECTIFICATION RIGHTS

Type of Website		Voluntary notice regarding the right to access personal data	Mechanisms for updating data
Public Websites		6%	7%
Private Websites	co.il	10%	11%
	org.il	14%	17%
Popular Websites		21%	24%
Sensitive Websites		10%	15%

D. *Privacy Practices: Look and Feel*

A series of factors were reviewed to determine the visibility of notices required by the PPA. We assumed that a notice is most visible when it is clearly displayed under a distinctive, easily located heading. We then examined whether the notice is displayed separately under a distinctive title like "Privacy Policy," whether the website's homepage links to the notice, and the prominence of the link, based both on its location on the

154. *Id.* §§ 13–14 (stating user access rights, exceptions for security bodies, law enforcement bodies, tax authorities, and anti-money laundering databases, and user rectification rights).

155. *See id.* § 14.

webpage and its overall prominence on a scale of 1 to 5, as discussed below.

Heading. The results show that a vast majority of websites in all subcategories include the notice in their Terms of Use (ToU) and bylaws: 81% of public websites, 70% of <org.il> websites, 64% of popular websites, and 62% of <co.il> websites; sensitive websites came in last at 52%. Twenty-nine percent of sensitive websites displayed their privacy policies in other ways.

TABLE 7
HEADING OF NOTICE

Type of Website		Display as "Privacy Policy"	Display under ToU or bylaws	Display under "data security"
Public Websites		4%	77%	2%
Private Websites	co.il	12%	54%	0
	org.il	8%	34%	0
Popular Websites		15%	35%	12%
Sensitive Websites		10%	42%	5%

Visibility of Link to Notice. Most websites maintained a link to the notice on the website's homepage: 88% of popular websites, 85% of public websites, 84% of sensitive sites, 82% of commercial websites, and 65% of <org.il> websites.

Location of Links. Most links to the notice were located at the bottom of the webpage: 90% of popular sites, 79% of sensitive websites, 89% of public websites, 73% of <org.il> websites, and 69% of <co.il> websites.

Links' Reliability. Links to the privacy policy were almost always active: as a whole, links were active in over 94% of websites, with 100% reliability for public websites.

Prominence of Links to Notice. The location of information on websites affects the impact of the information. Accordingly, we examined the prominence of the links to the notice on a scale of 1 to 5.[156]

156. Subjective rankings were based on the examiner's overall impression of the sites.

TABLE 8
PROMINENCE OF LINKS TO NOTICE
[1—HIGHLY VISIBLE; 5—HARDLY NOTICEABLE]

	1	2	3	4	5
Public	0%	28%	37%	24%	11%
Commercial	2%	23%	29%	27%	19%
Org.il	7%	7%	27%	53%	7%
Popular	3%	10%	63%	20%	3%
Sensitive	0%	25%	44%	19%	12%

E. *Actual Privacy Practices*

For a selected group of websites, the sensitive websites, we performed data security testing related to some of their actual privacy practices. The goal was to examine whether there is a gap between their claimed policies and actual information practices. To examine the actual information privacy practices of these websites, we designed a technological test in collaboration with Aladdin Knowledge Systems Ltd., a data security company. The tests aimed to measure the following: tracking cookies used by websites, data security vulnerability, and use of intrusive measures. The evaluation combined several approaches that apply automatic and manual tools, including code and functionality analysis, network traffic analysis, and manual examination.[157] The evaluation of actual information practices was performed in a controlled

157. For each of the sensitive websites, the evaluation proceeded according to the following steps. First, we opened the website with Internet Explorer in a controlled environment. Second, we inspected the main page's code by reviewing the captured Transmission Control Protocol (TCP) packets with Ethereal sniffer to determine whether the main page contains any exploits that may run malicious code. Third, we checked if the website communicated with other websites in order to import extraneous components. This was also done using Ethereal sniffer, which provides an option to list all such communications with displayed TCP packets for easy review. Fourth, we surfed the website, checking the methods it used to protect users' data and running Ethereal to determine whether it used any encryption protocol. Fifth, we inspected the cookies that the website or third-party websites placed on our machine. Sixth, we used LinkScanner (http://linkscanner.explabs.com) to check whether the website was hiding any exploit code. This step is meant to ensure that we did not miss any malicious code during our manual inspection of the packets captured by Ethereal sniffer. Finally, we used Acunetix Web Vulnerability Scanner for two purposes: first as a crawler to determine whether it contained any suspicious pages (if so, we inspected it carefully); second, to scan for vulnerabilities.

environment to ensure reliable, accurate, and comprehensive examination.[158]

We then compared each website's declared privacy statements with actual privacy practices. Actual information practices of sensitive websites showed poor compliance with the legal requirements. We detected a high percentage of websites claiming to provide data security, with the highest percentage among sensitive websites with privacy policies (58%). However, examining the actual practices of these sensitive websites revealed that the vast majority did not provide any sort of data security.

While there is no legal obligation to report which data security measures are undertaken, and no obligation to report the use of cookies, 24% of the sensitive websites provided users with a notice about the use of cookies although none mentioned the use of "third-party cookies." The tests of actual information practices showed that about 90% of sensitive websites used cookies and about 25% also used third-party cookies.

Finally, about 50% of sensitive websites linked to applications on other websites which in some cases collected data from the website users.

F. *Understanding Compliance and Disobedience*

The study demonstrates the marginal role of data protection regulation in shaping the online privacy environment. The findings show a high level of data collection and a low level of compliance with legal requirements. A closer look at these findings, however, reveals interesting variants in actual responses to different legal measures. It further reveals some notable discrepancies between the different sectors. These findings are discussed below.

1. Data Collection. The first significant finding is that websites routinely collect personal data from users. This is of no surprise to anyone who studies data collection practices on the Internet. Nevertheless, users often do not fully realize the extent to which websites collect data. Privacy awareness surveys conducted in the last decade have found that users are suspicious and fear that their privacy is violated online, especially when providing data on their credit cards. However, the main concern that users express is that their privacy will be violated by third

158. The environment consisted of Windows XP and Internet Explorer 6.0 (IE) installed on a VMware machine in addition to Ethereal sniffer installed on the host machine to observe the network traffic of the guest OS (Operating System) installed on the VMware. The tools used to accomplish the evaluation were Microsoft Internet Explorer 6.0 (default configuration), Ethereal Sniffer, VMware, Acunetix Web Vulnerability Scanner and LinkScanner.

parties, such as hackers and identity thieves. As our lives go digital, it is increasingly clear that data is continuously collected by almost *all* websites. Our study indicated that this warning is especially applicable to popular and sensitive websites and, to a lesser degree, public websites.

Another striking finding is the high level of non-compliance among public websites. This finding suggests that the state is still a major threat to the privacy of citizens. The findings further indicate that the practice of collecting data is slightly lower among commercial and organization websites than in other groups.[159]

2. Identification. The study shows that roughly half of public and private sector websites ask for identification, making it a prevalent practice among those websites that collect data. This practice is used more often by the popular and sensitive websites. The commercial and popular websites tend to require identification as a precondition for accessing the website or acquiring services. It is not surprising that a high percentage of interactive websites, which by their nature collect information, require identification. The collection of identifying data has commercial motivations; for example, it might be necessary for facilitating online payments. In other cases it is part of the website's business model, where the website provides a useful service "for free" in exchange for user-identifying data. Such identifying data could be valuable to the website itself or sold to third parties. Another possible explanation for the prevalence of the identification requirement is that websites collect identifying data as a precaution against potential liability for injurious behavior by users (i.e., posting defamatory statements or materials that infringe copyrights).

The findings show that a substantial number of websites requiring identification do not verify this data. The evidence on the feasibility of false personal data is striking.[160] Providing false personal data is a form of resistance, a user self-help measure for protecting one's rights (although it may also facilitate abuses).[161] The current study did not

159. This latter finding can be explained by the diverse composition of the <co.il> and <org.il> groups. The <co.il> and <org.il> categories are loosely defined by the allocation of domain names. *See Rules for the Allocation of Domain Names*, *supra* note 122, at 3.2. Consequently, while other categories require the satisfaction of some formal criteria (i.e., a license or a legal status), the <co.il> and <org.il> categories function as a default. Therefore, these groups are likely to be less homogenous and to include strictly commercial entities alongside smaller NGOs and personal websites. We assume that NGOs and personal websites are less likely to engage in data collection. The differences among these entities are likely to mitigate the final outcome. Further research could verify this hypothesis by differentiating these subgroups and studying their practices separately.

160. *See supra* Table 2.

161. For resistance practices in the context of privacy, see John Gilliom, *Struggling with Surveillance: Resistance, Consciousness, and Identity*, *in* THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY 111, 111–29 (Kevin D. Haggerty & Richard V. Ericson eds., 2006).

systematically measure whether users actually take advantage of this option. Further research is needed on users' behavior regarding the provision of false data.[162]

The law plays only a minor role and does not intervene directly in the domain of identification requirements. The PPA authorizes websites to request data, but it does not prohibit users from providing false data.[163] The only legal issues at stake lie at the background of this practice: websites are subject to the general notice requirement, and users might be required, in some cases, to provide correct data under general principles of private law (such as good faith in negotiation and pre-contractual relations, and the general prohibition of fraud).[164]

3. Notice Compliance. Not surprisingly, the findings on compliance with the strict notice requirements of the PPA indicate that compliance is rather low.[165]

The level of compliance also varies among different sectors. While compliance among public and private sector websites was relatively low, ranging from 16% to 22%, popular and sensitive websites had substantially higher compliance rates, with popular websites showing the lowest number of violations. With over 80% of public websites collecting personal data, low compliance among public bodies raises serious concerns.

The high level of compliance among popular websites is particularly interesting. The popular websites are generally owned by major corporations. These corporations most likely retain competent legal advice and are more informed about potential legal exposure. This suggests that privacy regulation is more effective at shaping the behavior of commercial

---

162. Relevant factors might include the knowledge and technological sophistication of users and social norms regarding the use of such websites. Thus, for example, a user who is not aware of the collection of data or its meaning, is aware but not concerned, is not opposed to data collection, or is simply naïve, is less likely to attempt to use false data.

163. Privacy Protection Act, 5741–1981, 1011 LSI 128, § 11 (1980–81) (Isr.). Of course, other laws prohibit deceit and impersonation. *See, e.g.*, Criminal Act, 5738–1977 (1977) (Isr.).

164. A false statement of fact by users may violate the legal duty to act in good faith in negotiating a contract. *See* The Contracts (General Part) Law, 5733–1973, § 12 (1973) (Isr.). This may also give rise to tort liability for negligent misrepresentation under § 35 or fraud under § 56 of the Tort Ordinance. Tort Ordinance (New Version), 5728–1968 (1968) (Isr.).

165. A caveat is in order here. Our methodology aimed at identifying the websites that collected personal data. We tagged several activities as collection of data and excluded those which seemed to collect only contact data and would therefore not be regarded as databases subject to the notice requirement under the PPA. However, we were unable to determine whether the websites also retained the data, in which case they may qualify as databases, as defined by the PPA. However, if the data is deleted immediately after the transaction or act (for example, search engine queries that are not retained), no database is formed. Privacy Protection Act, § 7 (Isr.) (definition of "database"). We assume that the latter situation is rare, as it is well known that such data is retained for at least some time. For further discussion of voluntary data retention by online players, see Kristine Laudadio Devine, Searching for Privacy Online: Legislating Against the Retention of Search Histories, (March 2007) (unpublished draft), *available at* http://papers.ssrn.com/sol3/papers.cfm? bstract_id=1111378.

players. Compliance with the notice requirement is virtually free, but with a nearly complete lack of enforcement, noncompliance is also virtually free.[166] As long as there is little enforcement and minimal deterrence, it is not surprising that the notice requirement is not followed. This may further explain the failure of public websites to comply, despite the expectation that public bodies would adhere to clear statutory instructions rather than being motivated by economic incentives.

Another possible explanation for high compliance levels among popular websites is their greater sensitivity to demand among users. A notice to potential users may communicate professionalism, legitimacy, and trustworthiness—all standard marketing tools.

By closely examining the PPA's requirements, we are able to reach conclusions regarding these higher compliance levels. The findings as to compliance with the PPA's first requirement, that notice to users include whether the user has a legal duty to provide data, are particularly important.[167] The Israeli law's direct reference to the existence of a legal duty is unique; other jurisdictions have more elaborate duties related to such notice.[168] This requirement is also less intuitive than the other requirements, and less likely to be inferred by simply browsing privacy policies posted online. Hence, we assume that those websites that complied received legal advice regarding compliance with the PPA. Compliance levels with this sub-requirement were the lowest of all three sub-requirements of section 11.[169] Again, the compliance rate for popular websites was the highest of all groups, but objectively low, with only 26% of the collecting websites referring to this prong of section 11.[170] In addition to general enforcement failures, the low compliance rate may be explained by the potential for negative impact of such notices on the data subject's behavior. If a data subject is told that she is under no legal duty to provide the data, she may not provide the requested information, or even worse, may become suspicious of the data-collecting process altogether.

Another possible explanation acknowledges that section 11(1) notice requirements are uncommon. Drafters of website notices, knowing that

166. *See supra* notes 144–148 and accompanying text.

167. *See* Privacy Protection Act, § 11(1) (Isr.).

168. Other data protection jurisdictions, namely the EU, require that when data is collected from the data subjects, the data collector must inform the subject, *inter alia*, of "whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply." *See* Data Protection Directive, *supra* note 17, art. 10(c). This requirement is qualified by language limiting the obligation "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject." *Id.*

169. *See* Privacy Protection Act, § 11 (Isr.).

170. *See id.* § 11(1).

the requirement is not made in other jurisdictions, may not feel obliged to include it in the notice. We suspect that some of these notices are simply copied from foreign websites, and it is likely that the language of the notice is the outcome of independent legal analysis and tailored to the particular needs of the website in only a small number of cases. Further empirical research is needed to explore this issue.

The central finding of the Privacy Study is that many Israeli websites that collect data routinely violate the law. These websites frequently ignore their obligation to state whether there is a legal duty to provide the data. Furthermore, when categories of websites are compared, public websites complied at the lowest rates, and popular websites at the highest.

The lack of compliance is not surprising, but the clear gap between public websites and the other categories of websites, particularly popular websites, is an intriguing finding. Israeli data protection law aims at both sources of harm to individual privacy: the state and the market. It is popular to argue that the market poses no less a threat to personal data than the government. Indeed, our findings indicate that private websites, especially popular ones, are more likely to collect personal data and are slightly less willing to accept false data compared to the other website categories, including public websites. However, at the same time, popular websites are more likely to comply with formal legal requirements. These findings lead us to propose a concrete practical policy recommendation to the Israeli DPA (Data Protection Authority): in order to address privacy and compliance failures among public sector websites, the DPA should design an enforcement mechanism that is tailored for public players.

4. Notice Accessibility. Data protection law in general and the Israeli PPA in particular place a high importance on notice as a basis for a user's autonomous decision, which is based in turn on the concept of informed consent. Accordingly, when a user knowingly agrees to provide personal data for a particular use, there is no privacy violation. Current law elaborates some elements of the content of the notice but is silent regarding its accessibility. We studied the way websites present the notice, including the heading, location on the website, and prominence. A substantial number of websites placed the notice under the general terms of use or bylaws, with only a few in each category using the explicit title "Privacy Policy." This is not a violation of the PPA, but it does indicate that website owner/operators either do not appreciate the benefit of a separate heading or have deliberately avoided providing one. Links to the notice were usually located at the bottom of webpages, resulting in generally lower prominence ratings.

This finding leads to the following conclusions. First, the notice requirement fails to perform its purpose. A statement buried in legalese-heavy "Terms of Use" text at the bottom of a webpage is unlikely to provide a data subject with sufficient information to make an informed decision about providing personal data. A broad reading of the PPA, drawing on its purposes, suggests that the law regulates not only the content of the notice, but also its form. Consumer protection laws provide a useful example of such detailed regulation by explicitly specifying the necessary format of particular notices, such as the font size of certain notices.[171] With the growth of interest in behavioral law and economics,[172] it is not surprising that reform initiatives increasingly focus on rules responding to various cognitive failures.[173] Regulating the heading, location, and prominence of the notice may achieve greater visibility and more meaningful informed consent by users. Of course, such regulation may encounter constitutional difficulties due to interference with the website's property, freedom of speech, and, at least in Israel, freedom of occupation.[174]

5. Additional Content. The notices reviewed by the Privacy Study were notable not only for what they unlawfully failed to include but also for what they voluntarily did include. As discussed in Part II, the PPA requires data collectors to conform to certain core principles (e.g., notice and consent), and to carry out several duties, such as providing access

171. *See, e.g.*, Consumer Protection Act, 5741–1981, 1023 LSI 248, § 4A (1981) (Isr.) (authorizing the Minister of Commerce to set the size of fonts in standard form contracts).

172. *See generally* Christine Jolls, Cass R. Sunstein, & Richard Thaler, *A Behavioral Approach to Law and Economics*, *in* BEHAVIORAL LAW AND ECONOMICS 13 (Cass R. Sunstein ed., 2000); Amos Tversky & Daniel Kahneman, *Rational Choice and the Framing of Decisions*, *in* PREFERENCES, BELIEF AND SIMILARITY: SELECTED WRITINGS 593 (Eldar Shafir ed., 2003) (demonstrating the effects of psychological principles, which govern the framing of choice, on preferences).

173. *See, e.g.*, John C. Anderson et al., *The Mitigation of Hindsight Bias in Judges' Evaluation of Auditor Decisions*, AUDITING: J. PRAC. & THEORY, Fall 1997, at 20 (reporting on a study of hindsight bias among professionally trained judges and arguing that that tort reform is necessary if hindsight bias cannot be mitigated); Richard M. Hynes, *Overoptimism and Overborrowing*, 2004 B.Y.U. L. REV. 127 (2004) (discussing the legal implications for bankruptcy law of a cognitive failure related to overoptimism regarding the risks consumers are facing). Consumer protection laws that require a minimum font size in standard form contracts or certain notices to be printed on separate pages are other examples of legal rules that respond to common cognitive failures or insufficient attention to detail. *See, e.g.*, Consumer Protection Act, § 4A (Isr.) (authorizing the Minister of Commerce to issue regulations concerning display and font size in standard form contracts).

174. Israel has no written constitution, but these rights and liberties are protected by a set of basic laws which are superior to other laws, and on several occasions the High Court of Justice has invalidated legislation contradicting the Basic Laws. The freedom of occupation is protected under the Basic Law: Freedom of Occupation, 5754–1994 SH No. 1454 (Isr.), while freedom of speech and the right to property are protected under Basic Law: Human Dignity and Liberty, 5752–1992, SH No. 1391, § 2, 3 (Isr.).

and rectification rights and maintaining confidentiality and data security.[175] However, the PPA does not require that data collectors announce how they comply with these duties or how the subjects' rights may be exercised. Nevertheless, a substantial number of websites that collect data provide users with information about data security measures, including over half of the sensitive, popular, and commercial websites (58%, 55%, and 51% respectively) but less than a quarter of public websites (24%).

A smaller number of websites informed users of their access and rectification rights although not required to do so under the PPA. Popular websites are most likely to have such information available. One possible explanation is that these websites are also using samples of standard privacy policies posted on major (primarily U.S.) websites. Similar access and rectification provisions are prominent in privacy policy models.[176]

III. RAMIFICATIONS

The overall picture that emerges from these findings is one in which the law plays a marginal role. This Part discusses the meaning of these findings, focusing on implications in privacy policy and data protection regulation in the context of other attempts to regulate online behavior.

A. *Data Protection Regulation*

The empirical study of Israeli websites carries broader lessons for data protection regulation. The law does not appear to play an important role in shaping website behavior and privacy practices. The varied results across categories of websites suggest additional relevant factors, especially with respect to market forces. The owner/operators of commercial websites that ask users to provide sensitive data are aware of user concerns. Hence, to reassure users, the website declares that it safeguards the data.

---

175. *See* Privacy Protection Act, §§ 13–14, 16–17 (Isr.).

176. For example, TRUSTe, a leading privacy seal company, offers guidelines for websites' privacy policies:

> Access to Personally Identifiable Information: If your personally identifiable information changes, or if you no longer desire our service, you may [correct, update, delete or deactivate it] by making the change on our member information page [or by emailing our Customer Support at EMAIL ADDRESS] or by contacting us by telephone or postal mail at the contact information listed below.

TRUSTe Guidance on Model Web Site Disclosures, TRUSTE, http://www.truste.org/docs/Model_Privacy_Policy_Disclosures.doc (last visited Oct. 31, 2010).

One possible conclusion is that we should take the law out of the picture, as it intervenes unnecessarily where market forces provides sufficient redress. In this view, competition among websites may guarantee a sufficient level of data security. A different approach would require that websites that collect data and operate under a duty to provide data security also provide a statement to that effect. Such a statement can have legal implications: a website that falsely claims to have undertaken certain data security measures can be sued not only for breach of duty, but also for false representation.[177] This is the basis of governmental regulation of personal data in the United States, where the Federal Trade Commission (FTC) lacks power to regulate data protection matters directly, but has authority to regulate with respect to false representation.[178]

The findings shed doubt on the efficacy of the notice requirements and their contents and, more generally, on the notice and consent regime. The low level of compliance with notice requirements may call for consideration of a hands-off legal strategy. The market and other factors may provide better mechanisms for securing online privacy.[179] An alternative would be to search for better regulatory mechanisms, perhaps strengthening and enhancing the legal requirements to include more detail about what should appear in the notice and how it should be presented, and accompanying these enhanced requirements with effective private and public enforcement.

Is the law completely irrelevant? We submit that it is not. First, as our findings indicate, there are substantial levels of compliance with the existing legal privacy regime.

In the United States, data protection law plays another role. Given the prominence of the "reasonable expectations" test within U.S. privacy law,[180] concrete regulations help shape these expectations. This has a circular effect. The fact that the law requires certain measures has a large effect on data subjects' expectations and, of course, the reasonability of expectations. The lack of any regulation might indicate that there are no such expectations or that certain expectations are unreasonable. Put differently, when a court has to determine whether certain asserted

177. The cause of action for breach of duty can be found either in contract law or negligence law, if harm is caused. The obligation to avoid false representations is found in the Consumer Protection Act, § 2 (Isr.).

178. Since there is no general U.S. federal law that requires privacy protection measures, the FTC can only enforce privacy rules indirectly. A corporation that states that it provides a privacy-related measure and fails to actually provide it can be investigated for false representation. Thus, the FTC indirectly protects substantive privacy norms. *See* Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2006).

179. The strongest defense for this proposition is provided in FRED H. CATE, PRIVACY IN PERSPECTIVE *See supra* note 53.

180. *See* Katz v. United States, 389 U.S. 347, 360 (1967).

expectations are reasonable, the existence of a statute that addresses the matter at stake might in itself serve as an indication of reasonableness.

Our findings regarding disparate compliance levels across categories of websites are particularly interesting.[181] The low level of compliance among public websites is striking. In fact, some legal regimes assume that the threat to privacy arises from administrative bodies. At the same time, however, comparing the higher level of compliance among large commercial websites (popular, sensitive) with private sector websites may provide insight into the mechanisms affecting online compliance. Data security regulation is perhaps most effective under commercial enterprises, which are more likely to obtain legal counsel and therefore more likely to identify the legal requirements and respond to potential legal liability. Commercial enterprises are generally more risk averse; they are highly visible, have deep pockets, and are more likely to be drawn into expensive litigation.

As suggested above, commercial players might be motivated by an existing demand among users for privacy reassurances. This explanation is supported by findings of over-compliance among commercial websites. Thus, market forces, and not the law, may play a dominant role in shaping the behavior of online players.

Moreover, the regulatory approach is less effective with small enterprises or individual users, neither of which can afford the sophisticated legal counsel that is often required for establishing a data protection policy. These websites are also affected, to an apparently much lesser extent, by market forces.

This finding is troubling given the growing role of individuals and small enterprises in the Web 2.0 environment.[182] As individual users increasingly move to the forefront of news reporting in blogs, micro-blogs, and online forums, or operate small online businesses, they too begin to collect data on fellow users. The low level of compliance with current regulations among individuals is particularly alarming given the increasing threats to the privacy of users in social networks and the social

181. *See supra* Part III.

182. *See* OECD, *Participative Web: User-Created Content* (2007), *available at* http://www.oecd.org/dataoecd/57/14/38393115.pdf. For further discussion of the rise of individual users as major players in the information environment, see generally YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 99–106 (2006); CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATION 25–54 (2008); and Niva Elkin-Koren, *User-Generated Platforms*, *in* WORKING WITHIN THE BOUNDS OF INTELLECTUAL PROPERTY 111 (Rochelle Dreyfuss et al. eds., 2010).

web.[183] A major threat to users' privacy is posed by information they share on social networks without being fully aware of privacy consequences.[184] Moreover, the social web encourages users to share information about their friends and acquaintances by publicizing lists of social connections, posting personal photos, publicly sharing information regarding private events and experiences, and actively linking and using private information provided by others. These major developments suggest that public action to secure privacy in this environment may require different measures. Moreover, our research findings suggest that data protection regulation may be unable to create a single legal measure that fits all online privacy concerns, including these emerging threats.

B. *Online Regulation*

The findings also address the interconnection between law and technology, suggesting that laws aiming to regulate online behavior should be attentive to the inherently dynamic nature of the information environment.

First, the findings bring to the surface some of the underlying assumptions of the legal regime regarding the architecture of the information environment and the ways in which it may threaten privacy. The introduction of digital technology created new opportunities for collecting and processing data—opportunities that threaten individual privacy in the information era. The challenge for policymakers is how to address threats to privacy posed by information processing systems. These new technological capabilities necessitated the expansion of legal measures protecting physical privacy to cover personal data and enable individuals to exercise some control over personal information. Indeed, the data protection legal regime described in Part II assumed a particular architecture where information is collected by large-scale enterprises (the state or commercial entities) that could threaten individual privacy. Our findings show, however, that while such a regime might be relatively effective for regulating the behavior of larger commercial enterprises, it is less effective for regulating the non-commercial private sector. This suggests that the regulatory approach of data protection may prove inadequate, as the information environment has become more diffuse. New threats to privacy emerge in dispersed systems and are often created

183. *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) (arguing that social networks, such as Facebook, facilitate peer-to-peer privacy violations, with users harming other users' privacy interests).

184. *See, e.g.*, Lilian Edwards & Ian Brown, *Data Control and Social Networks: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION 202 (Andrea M. Matwyshyn ed., 2009).

by individuals and small groups with a growing ability to collect and process information (e.g., bloggers).[185] This may require regulators to adjust current legal strategies to the new architecture. As long as regulation is targeted primarily to commercial enterprises, it may fail to achieve its purpose.

Moreover, new technologies often destabilize fundamental legal concepts, requiring lawmakers to reconsider the rationales underlying a regulatory framework.[186] The legal regime that seeks to allow individuals to control the collection and processing of personal data assumes that individual users value such control or, at the very least, would have valued it more had they known and understood the implications of providing such data. Our findings show that in the data security context, websites independently react to the demands of consumers.[187] Such demands often result in better compliance with data protection standards and with standards higher than those required by law. By analogy, in websites with lower compliance levels, one might infer that individuals simply do not care about the collection of their data or the transfer of that data to third parties, or perhaps that they are unaware of, or do not fully comprehend, the privacy threats. If users know, understand, or care about their personal data, websites are more likely to compete in providing appropriate privacy policies to attract more users. As the information environment becomes a greater part of everyday life, shifts in privacy preferences are likely to continue.[188] For example, users of social networks such as Facebook willingly share colossal amounts of personal data and intimate details about their personal affairs.[189] Thus, a second issue that must be considered in adjusting the data protection regime to the dynamic information environment is whether the law is the best tool for facilitating personal privacy.

A final point is that sometimes the architecture effectively determines the extent to which rights are protected. Our findings show that although a large number of websites required the submission of personal information as a prerequisite for obtaining access or services, the ability of users to provide false data enabled them to protect against unwarranted invasion of their privacy. This suggests that privacy regulators may need to focus not only on legal requirements but also on promoting an open infrastructure and enabling means of self-help. Such policies

185. *See supra* notes 183–184 and accompanying text.

186. Niva Elkin-Koren & Eli Salzberger, *The Economic Analysis of Cyberspace: Challenges Posed by Cyberspace to Legal Theory and Legal Rules*, 19 INT'L REV. L. & ECON. 553 (2000).

187. *See supra* Part II.

188. Omer Tene, *Privacy: The New Generations*, 1 INT'L DATA PRIVACY L. 15 (2011).

189. *See* Edwards & Brown, *supra* note 184.

should aim at facilitating privacy enhancing technologies (PETs) and educating users about the risks and opportunities they face online.

CONCLUSION

Privacy has never been a clear legal concept. As our lives move increasingly to the online environment, the future of privacy is more mysterious than ever. Cultural trends, social pressure, and new technologies pull us—or perhaps push us—towards sharing more personal data with others. Our friends in the social network are interested in such data, but so are corporations and governments. This Article focused on the category of privacy in personal data, or informational privacy, in the digital environment. The changing landscape of the online environment will affect the boundaries between the private and the public, and change our views and expectations regarding the privacy of our personal data. These changes, however, are beyond the scope of this Article. Once we—as a society—make the decision that we care about our online privacy, the policy and legal challenge is to figure out the best way to address this issue. One option, thus far undertaken by the United States, is to leave the regulation of online privacy to the market, though with certain constraints on governmental use of the data and some targeted sectoral regulation. An alternative approach, exemplified by the European Union, is to create a robust regulatory regime. As governments consider which route to take and how improve existing policy, more data is needed to assess the pros and cons of these approaches.

This Article provided an empirical study of a legal system that emulates the European model—the Israeli data protection law. The research presented in Part II examined the application and compliance of the law in practice. We found that some areas of the law are simply irrelevant in the daily practices of websites, and that there are clearly other forces at play, namely market forces and dynamic social norms. The findings affirm the concern that privacy is threatened not only by Big Brother but by market players as well. However, these market players often demonstrate better compliance with the law than other players, and far better compliance than the state actors. Large corporate players also respond better to data protection regulation than non-market players such as NGOs, individual users, and small businesses. These findings are particularly informative for policymakers given the recent transformation of the online environment, the rise of the social web, and the centrality of individual users and uncoordinated crowds. At the end of the day, in designing a privacy policy, all of these factors should be taken into

consideration, with special attention to the interplay between the law, technology, and evolving norms.