Singapore Journal of Legal Studies
[2012] 391–415

# AFTER PRIVACY: THE RISE OF FACEBOOK, THE FALL OF WIKILEAKS, AND SINGAPORE'S *PERSONAL DATA PROTECTION ACT 2012*

SIMON **CHESTERMAN***

This article discusses the changing ways in which information is produced, stored, and shared—exemplified by the rise of social-networking sites like Facebook and controversies over the activities of WikiLeaks—and the implications for privacy and data protection. Legal protections of privacy have always been reactive, but the coherence of any legal regime has also been undermined by the lack of a strong theory of what privacy is. There is more promise in the narrower field of data protection. Singapore, which does not recognise a right to privacy, has positioned itself as an e-commerce hub but had no law on data protection until the passage of the *Personal Data Protection Act 2012*. The passage of that law suggests the possibilities and limitations of an approach to data protection that eschews both the European Union's privacy-rights-based approach and the ad hoc sectoral patches that characterise the U.S. approach to the subject.

## I. INTRODUCTION

In a world of cloud computing—in which remote servers are used for an expanding range of functions, including storage[1]—the ability to safeguard personal data is an essential component of being a global hub in the information economy. Yet privacy is under threat as never before. In addition to the traditional surveillance powers of governments and the growth in electronic commerce, the rise of social networking sites like Facebook has massively increased the volume of personal data being collected—and sold—online. Meanwhile, the emergence of groups like WikiLeaks has undermined faith in the ability to keep anything truly secret. This article discusses the changing ways in which information is produced, stored, and shared, and the implications for privacy and data protection. The focus for the latter is Singapore,

---

* Dean and Professor of Law, National University of Singapore. This article draws on some material first published in Simon Chesterman, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford: Oxford University Press, 2011). Many colleagues provided helpful comments on earlier drafts of that text, including Gary Bell, Lim Yee Fen, David Tan, an anonymous reviewer, and the editors of the Singapore Journal of Legal Studies. I am also grateful to Abu Bakar Munir for our discussions on this topic, as well as to the various public and private sector employees who spoke with me on a confidential basis. Errors and omissions are, of course, my own.

1 See *e.g.*, U.S., National Institute of Standards and Technology, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-145) (Washington, D.C.: National Institute of Standards and Technology, 2011), online: National Institute of Standards and Technology <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>. See also *infra* note 139.

which has positioned itself as an e-commerce hub and yet until recently had no law on data protection.

Part II examines the changing context of debates over privacy and data protection. Law has generally struggled to remain relevant to that changing context, with law reform largely being driven by emerging threats, technological breakthroughs, and evolving cultural sensitivities. The pace of change has accelerated today, with radical transformations in the way information is produced, stored, and shared. Part III then turns to the largely unsuccessful efforts to produce a coherent theory of privacy. These efforts have foundered in part because of distinct visions of privacy, epitomised by a U.S. approach focusing on protection from external interference and a European conception of human dignity. A second barrier to a robust theory of privacy is the contradiction between any such model and the actual practice of individuals.

Many privacy laws are, as a result, confusing and confused.[2] Nevertheless, significant advances have been made in adopting data protection laws across the world. Though data protection is not synonymous with privacy, the concepts are linked and the distinct approaches in the United States and Europe reflect the divide over privacy.[3] Part IV considers data protection and the efforts to harmonise norms, with particular reference to the decision to adopt a data protection law in Singapore, which is discussed in Part V. Two trends can be identified. The first is that the driving force of reform is not the rights of data subjects or indeed concerns about privacy *per se*; rather, it is the commercial realities of globalisation and the integration of information economies.[4] The second is that changing data processing practices are forcing a reconsideration of basic premises of privacy laws and data protection—in particular, the need to move focus from limiting the collection of data to regulating their use.

## II. The Changing Context

### A. *The Rise of Facebook*

The history of privacy is a tale of threats, technology and culture transforming the context within which laws struggle to remain relevant. Though the desire to keep certain information about oneself private has ancient origins, the modern assertion of a legal 'right' is frequently traced to late nineteenth century developments in the United States—where it was the response to the rise of sensationalistic journalism, the invention of the handheld camera, and changing views on the proper role of mass media.[5] At the heart of this early conception of privacy was the right "to be let

---

2 See *e.g.*, Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor, Michigan: University of Michigan Press, 1971) at 25; Julie C. Inness, *Privacy, Intimacy, and Isolation* (Oxford: Oxford University Press, 1992) at 3.

3 Some scholars dispute whether U.S. laws regulating privacy are properly regarded as data protection laws. See generally Daniel E. Newman, "European Union and United States Personal Information Privacy and Human Rights Philosophy—Is There a Match?" (2008) Temp. Int'l & Comp. L.J. 307.

4 This is not new, of course. See *e.g.*, Lilian Edwards & Charlotte Waelde, eds., *Law and the Internet* (Oxford: Hart Publishing, 1997).

5 Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. Rev. 193; Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 8-22; Richard F. Hixson, *Privacy in a Public Society* (Oxford: Oxford University Press, 1987) at 3-25.

alone".[6] (This view is challenged by some scholars who point to earlier codification and occasional litigation in Europe.[7])

The latter half of the twentieth century saw a second phase in the evolution of privacy, with an explosion in literature dealing with the question. Prescient warnings were issued in the 1960s about computerisation increasing the amount of information available to governments and other actors, as well as the ease of accessing it.[8] Computerisation removed what the U.S. Supreme Court once termed the "practical obscurity" of paper records.[9] Much information that one might consider private—aspects of one's family life, finances, medical records, for example—had long been effectively protected through the difficulty of locating and analysing specific records. When the same records are computerised and stored in a form accessible by a variety of actors, this practical obscurity may disappear.[10]

In the United States, concerns about privacy were addressed by sectoral patches as they arose, such as the *Right to Financial Privacy Act* and the *Electronic Communications Privacy Act*. The focus of the legislation tended to be on limiting the collection or restricting the storage and dissemination of data.[11] In Europe, a more thematic approach was adopted, consistent with a distinct conception of privacy that stresses the importance of preserving a sphere of life that is outside the public gaze. Across Asia, the absence of European-style rights protection meant that an approach similar to the U.S. model was initially taken, with piecemeal legislation or episodic court intervention—or, as in many jurisdictions, the matter was either left to the market or essentially ignored.[12]

The early years of the twenty-first century saw another shift in the way in which data are used and the beginning of a third phase. The popularity of social networking sites like Facebook has radically increased the number of entities with which individuals share personal data. Name, contact details, birthday, relationship status, and the contents of updates are shared with nominal "friends" but also "friends of friends" and frequently with any person having access to the Internet. One measure of the transformation underway is that Facebook briefly overtook the search engine Google to be the most visited website in 2010—perhaps marking the point at which sharing information became as popular as searching for it.[13] Facebook has also been

---

6 This formulation derives from Thomas M. Cooley, *A Treatise on the Law of Torts, or the Wrongs Which Arise Independent of Contract*, 2nd ed. (Chicago: Callaghan & Co., 1888) at 29.

7 See *e.g.*, *L'affaire Rachel* (Tribunal civil de la Seine, 16 June 1858). Many thanks to Gary Bell for his discussions with me on this subject.

8 See *e.g.*, Westin, *supra* note 5 at 158.

9 *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 at 762 (1989).

10 Paul M. Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 Vand. L. Rev. 1607 at 1644.

11 *Right to Financial Privacy Act*, 12 U.S.C. § 3401 (1978); *Electronic Communications Privacy Act*, 18 U.S.C. § 2510 (1986).

12 See *infra* notes 42-52 and accompanying text. *Cf.* the A.P.E.C. Privacy Framework adopted in 2005, a non-binding framework outlining principles based on the O.E.C.D. *Guidelines*, *infra* note 82: *APEC Privacy Framework* (Singapore: A.P.E.C. Secretariat, 2005), online: A.P.E.C. Privacy Framework <http://publications.apec.org/publication-detail.php?pub_id=390>.

13 Andrew Ross Sorkin & Evelyn M. Rusli, "Facebook Deal Puts Its Value at $50 Billion" *New York Times* (3 January 2011), online: New York Times <http://query.nytimes.com/gst/fullpage.html?res=9406E3D91438F930A35752C0A9679D8B63>. See also Samantha L. Millier, "The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet" (2008) 97 Ky. L.J. 541.

the subject of particular criticism because of its practices with regard to the collection and dissemination of user data.[14]

Together with the increasing sophistication of websites that gather information through cookies,[15] spyware that collect data on users,[16] and smartphones that record one's movements,[17] the amount of personal data being collected has grown to the point where it appears pointless to attempt to stop that collection. Instead, the new focus must be on addressing how the collected data are used.

### B. *The Fall of WikiLeaks*

An example of the radical changes in the production, storage, and sharing of information is the guerrilla journalism website WikiLeaks.[18] Launched in 2006, the site capitalised on the virtues and the vices of the Internet. The virtues are that the Internet is decentralised, anonymous, and user-driven: decentralisation makes it hard to shut WikiLeaks down; anonymity enables the protection of its sources; the user-driven nature of this Web 2.0 phenomenon encourages those sources to come forward. These virtues of the Internet, of course, are also its vices: decentralisation undermines meaningful accountability; anonymity enables the avoidance of responsibility; being user-driven leaves quality control to the consumer rather than the disseminator.[19]

Nevertheless, WikiLeaks was initially acknowledged as an important phenomenon. It won Amnesty International's New Media award in 2009, for the documents it published on extra-judicial killings in Kenya;[20] the Index on Censorship gave it a Freedom of Expression Award.[21] It rose to international prominence in 2010 after it released a video entitled "Collateral Murder" showing U.S. helicopters firing on Iraqi civilians, arguably out of context. WikiLeaks later released huge volumes of field reports from Afghanistan and Iraq, and most notoriously it worked with the *New York Times* and other major papers to release a trove of 250,000 State Department cables allegedly passed to it by Private Bradley Manning. It later claimed to

---

14 See *e.g.*, Yasamine Hashemi, "Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability" (2009) 15 B.U.J. Sci. & Tech. L. 140; Haley Plourde-Cole, "Back to Katz: Reasonable Expectation of Privacy in the Facebook Age" (2010) 38 Fordham Urb. L.J. 571.

15 See *e.g.*, Rachel K. Zimmerman, "The Way the 'Cookies' Crumble: Internet Privacy and Data Protection in the Twenty-First Century" (2000) 4 N.Y.U.J. Legis. & Pub. Pol'y 439.

16 See *e.g.*, Daniel B. Game, Alan F. Blakley & Matthew J. Armstrong, "The Legal Status of Spyware" (2006) 59 Fed. Comm. L.J. 157.

17 See *e.g.*, William Curtiss, "Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes" (2011) 45 Colum. J.L. & Soc. Probs. 139.

18 WikiLeaks has at best a tangential relationship to data protection, but it is used here to illustrate the changing manner in which information can now be disseminated.

19 For an early discussion of such concerns, see Cass Sunstein, *Republic.com* (Princeton: Princeton University Press, 2001).

20 Amnesty International, "Amnesty International Media Awards 2009", online: Amnesty International <http://www.amnesty.org.uk/uploads/documents/doc_20539.pdf>.

21 "Winners of Index on Censorship Freedom of Expression Awards Announced" *Index on Censorship* (22 April 2008), online: Index on Censorship <http://www.indexoncensorship.org/2008/04/winners-of-index-on-censorship-freedom-of-expression-award-announced/>.

be sitting on potentially embarrassing documents from a bank, widely believed to be Bank of America.[22]

WikiLeaks was often incorrectly characterised as having collected the sensitive information, when in fact its primary purpose was distribution—or, arguably, unauthorised secondary use of data. The various efforts to prosecute WikiLeaks founder Julian Assange in the United States foundered on the inability to prove his involvement in acquiring classified material. Prosecuting him for disseminating the material—that is, publishing it—raised the concern that any alleged crimes might equally apply to the activities of the *New York Times*.[23]

For present purposes, WikiLeaks is a useful example of how the most pressing issue today is not the collection of data but their use and, in particular, their dissemination to third parties. This phenomenon is presently discounted by many computer users, but the rise of cloud computing means that an increasing number of third parties hold potentially sensitive data.[24] The reality of globalisation and the Internet means that such third parties may be in different jurisdictions, with predictable problems of harmonisation and enforcement.[25]

These new ways in which information is produced, stored, and shared present two types of problems. One is how we conceive of 'privacy' today, which is considered in Part III. Another is how we protect potentially sensitive information, discussed in Part IV.

## III. Privacy in Theory and in Practice

As indicated earlier, the desire to control information about oneself is ancient, yet legal protections of a right to privacy are often traced only to the late nineteenth century. These two aspects of privacy—the ostensibly self-evident basis for the concept, but the reactive nature of efforts to protect it—have led to incoherence in both the theory and the doctrine of privacy.

Theories of privacy typically seek to identify a foundation for the various intuitions commonly shared concerning its meaning and scope. One approach focuses on the information in question. Some scholars emphasise the element of *intimacy*, with privacy embracing intimate information, access, and decisions. Such an approach is extremely narrow, however, as much information one might wish to keep private—one's financial records, political affiliations—could not accurately be described as

---

22 Mark Fenster, "Disclosure's Effects: WikiLeaks and Transparency" (2012) 97 Iowa L. Rev. 753 at 774; Yochai Benkler, "A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate" (2011) 46 Harv. C.R.-C.L.L. Rev. 311 at 342.

23 "Extradition and WikiLeaks: Courting Trouble" *The Economist* (16 December 2010), online: The Economist <http://www.economist.com/node/17730546>.

24 See *e.g.*, Virginia Boyd, "Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization" (2006) 24 Berkeley J. Int'l L. 939; Sarah Salter, "Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages" (2010) 32 Hastings Comm. & Ent. L.J. 365.

25 See Basil Markesinis *et al.*, "Concerns and Ideas About the Developing English Law of Privacy (and How Knowledge of Foreign Law Might Be of Help)" (2004) 52 Am. J. Comp. L. 133; Cécile de Terwangne, "Is a Global Data Protection Regulatory Model Possible?" in Serge Gutwirth *et al.*, eds., *Reinventing Data Protection?* (Berlin: Springer, 2009) 175 at 175.

"intimate" unless the word is defined so broadly as to become, in essence, a synonym for "private".[26]

A second approach therefore emphasises the relations between individuals and the right to be "let alone". Privacy is compromised when others obtain information about an individual, pay attention to him or her, or gain physical access. Privacy should therefore protect secrecy, anonymity, and solitude. This definition may be too broad, however, as it would appear to include rights—not to be pushed, for example—that go well beyond a meaningful definition of privacy.[27]

These first two conceptions of privacy are often associated with the approach adopted in the United States that sees privacy primarily as protecting a liberty interest, a freedom from external interference. This may be distinguished from what is sometimes termed a "European" understanding that stresses protection of the personal honour or dignity of individuals.[28] A third approach focuses on this notion of dignity, which is said to be stripped away if a person is denied a meaningful private life.[29] The need for a "private place" finds support among psychologists, yet as a theory it is imprecise, as a life with dignity requires more than merely the possibility of seclusion from society.[30]

A fourth approach therefore looks not to the individual's interest in preventing inconvenient or embarrassing disclosures, but to the benefits for society as a whole of maintaining a sphere of life that is insulated from the public gaze.[31] This is a promising line of inquiry, but if privacy is considered to be an individual right in tension with societal interests (such as security), the individual right will generally lose.[32] In any case, the sphere that can be insulated in this way has now diminished to the point where its physical borders are probably the confines of one's home, with temporal limits determined by the moments when one's telecommunications devices are switched off or out of range.

Despairing of conceptual clarity, some scholars resort to argument by intuition alone: the "twinges of indignation" that are said to be suggestive of the breaching of social norms.[33] That may well be how most people think of privacy, but intuitionism is a highly dubious basis for law. Taken seriously, it requires a pluralism that would make a choice between the different conceptions of privacy outlined above impossible; accepting that such pluralism derives from different social conditioning

---

[26] See *e.g.*, Inness, *supra* note 2; Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego L. Rev. 745 at 755 [Solove, "Misunderstandings of Privacy"].

[27] See *e.g.*, Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale L.J. 421; Solove, "Misunderstandings of Privacy", *ibid*. at 755.

[28] See *e.g.*, James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale L.J. 1151.

[29] See *e.g.*, Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 N.Y.U. L. Rev. 962.

[30] Sidney M. Jourard, "Some Psychological Aspects of Privacy" (1966) 31 Law & Contemp. Probs. 307; Tim Frazer, "Appropriation of Personality—A New Tort?" (1983) 99 L.Q. Rev. 281 at 296.

[31] Robert C. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 Cal. L. Rev. 957; Lisa M. Austin, "Privacy and the Question of Technology" (2003) 22 Law & Phil. 119 at 164, 165.

[32] *Cf.* Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999).

[33] Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public" (1998) 17 Law & Phil. 559 at 583.

undermines the claim that the relevant intuitions are self-evident.[34] Others have gamely attempted to develop taxonomies based not on doctrinal coherence but "family resemblances".[35] None of these approaches are satisfactory, supporting Jonathan Franzen's pithy account of privacy as "the Cheshire cat of values: not much substance, but a very winning smile."[36]

Not surprisingly, the legal protection of privacy—in the United States in particular—is inconsistent. Courts loosely embraced the idea of a right to be "let alone" articulated in the late nineteenth century, but a proliferation of cases ended up coalescing around four distinct kinds of interference with different interests of the plaintiff. These were linked by the name "privacy" but otherwise had little in common. Writing in 1960, William Prosser grouped them into an analytical framework that continues to be recognised today: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity that places a person in a false light in the public eye; and (4) appropriation of a person's name or likeness for another's advantage.[37]

The *European Convention on Human Rights* establishes a quasi-constitutional basis for privacy protection, unlike the common law and sectoral approach developed in the United States. This requires any interference with the right to "respect for private and family life" to be in accordance with the law, and necessary in a democratic society in the interests of "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[38] Privacy protections in Europe are significantly stronger than the United States, with the result that European standards often become global in areas such as Internet policy.[39] Nevertheless, the European Court of Human Rights has concluded that it would not be possible or desirable to attempt an exhaustive definition of "private life" for the purposes of its convention, instead developing specific protections that can be tied to that vague term incrementally.[40] (A recent battleground is the so-called "right to be forgotten", by which individuals may seek to have information about them deleted from the Internet.[41])

The various Asian jurisdictions initially tended to follow the model of sectoral or ad hoc approaches—or to lack privacy protections at all. Statutes regulating aspects of data protection closer to the European model were adopted as early as 1995 in

---

34 *Cf.* John Rawls, *A Theory of Justice* (Oxford: Clarendon Press, 1972) at 34-40.

35 Solove, "Misunderstandings of Privacy", *supra* note 26 at 756.

36 Jonathan Franzen, *How to Be Alone* (London: HarperCollins, 2002) at 42.

37 William Prosser, "Privacy" (1960) 484 Cal. L. Rev. 383. See *Restatement of the Law, Second, Torts* (Philadelphia: American Law Institute, 1977), § 652A.

38 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 222, Eur. T.S. 5, art. 8 [*European Convention of Human Rights*]. See Chesterman, *supra* note * at 132.

39 Jack Goldsmith & Timothy Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006) at 174. See also *infra* notes 115-118.

40 See *e.g.*, *Niemietz v. Germany* (1992) 16 E.H.R.R. 97 at para. 29.

41 Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009). See also Suzanne Daley, "On Its Own, Europe Backs Web Privacy Fights" *New York Times* (9 August 2011), online: New York Times <http://www.nytimes.com/2011/08/10/world/europe/10spain.html?pagewanted=all>.

Hong Kong S.A.R.[42] and Taiwan,[43] but they were relative outliers. Legislation was subsequently adopted in South Korea (2000),[44] Japan (2003),[45] Malaysia (2010),[46] India (2011),[47] and the Philippines (2012).[48] Vietnam has limited protections under a consumer protection law;[49] legislation was also proposed some years ago in Thailand.[50] None goes as far as the *E.U. Data Protection Directive* in covering all personal data processed by public and private sector bodies,[51] with the possible exception of Macao S.A.R.'s 2005 legislation—which at least in theory applies to public and private sector activities.[52]

In this way, the protection of privacy has been largely conceived in terms of functional restrictions: an activity is identified—the collection, use, or dissemination of information characterised as private—and a legal regime is developed in the hope of restricting that activity to legitimate purposes.[53] Conceptual clarity is not helped by the routine inclusion of matters not properly tied to privacy. The ability to correct information about oneself, for example, may be an important aspect of living in a world of computer databases and central to notions of data protection, but it is not helpful to link this to a core understanding of privacy.[54]

The incoherence of privacy as a concept in theory and the reactive approach to its protection by law in practice helps to explain why privacy activists have been so unsuccessful in drawing lines in the sand to stop the perceived erosion of privacy in a meaningful sense. Many writers have tried and failed to reconcile the apparent sincerity of individuals claiming to be concerned about their privacy with

---

42 *Personal Data (Privacy) Ordinance* (Cap. 486, 1995 Hong Kong S.A.R.), online: Department of Justice <http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf>.

43 *Computer-Processed Personal Data Protection Law* 1995 (Taiwan) (applies to the public sector and parts of the private sector). Significant amendments were adopted in April 2010, including the new *Personal Data Protection Act* 2010 (Taiwan), which came into force on 1 October 2012.

44 *Act on Promotion of Information and Communications Network Utilization and Data Protection* 2000 (South Korea) (limited to "providers of information and communications services"). This was recently supplanted by the *Personal Information Protection Act* 2011 (South Korea).

45 *Act on the Protection of Personal Information* (Act No. 57 of 2003) (Japan), online: <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf> (limited to the private sector).

46 *Personal Data Protection Act* 2010 (Act No. 709 of 2010, Malaysia) [Malaysia's *PDPA*] (limited to the private sector); Abu Bakar Munir & Siti Hajar Mohd Yasin, *Personal Data Protection in Malaysia: Law and Practice* (Petaling Jaya, Selangor: Sweet & Maxwell Asia, 2010).

47 *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules* 2011 (India) (limited to the private sector).

48 *Data Privacy Act* 2012 (Republic Act No. 10173) (Philippines).

49 *Consumer Protection Law* 2010 (Vietnam).

50 David Duncan, "Thailand: Personal Data Protection in Thailand" (London: Mondaq, 2011), online: Mondaq <http://www.mondaq.com/x/139148/Privacy/Personal+Data+Protection+in+Thailand> (discussing the draft *Personal Data Protection Bill*).

51 EC, *Commission Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L 281/31, online: European Commission <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> [*E.U. Data Protection Directive*]

52 *Personal Data Protection Act* (Act 8 of 2005, Macao S.A.R.), online: Office for Personal Data Protection <http://www.gpdp.gov.mo/cht/forms/lei-8-2005_en.pdf>. See Graham Greenleaf, "Macao's EU-influenced Personal Data Protection Act" (2008) 96 Privacy L. & Bus. Int'l Newsl. 21.

53 Jonathan Zittrain, *The Future of the Internet—and How to Stop It* (New Haven, Connecticut: Yale University Press, 2008) at 202.

54 Austin, *supra* note 31 at 165.

the nonchalant behaviour of those same individuals in revealing personal information voluntarily or engaging in activities where there is manifestly no reasonable expectation to privacy.[55]

There is also a generational element to the transformation underway. Whereas in the 1960s activists opposed even the creation of files, today's fears tend to stress the potential for abuse by private actors—identity theft, stalking—rather than nefarious activity by governments. The activists, like the generation that once wrote, signed, and sealed envelopes, or confided in diaries locked with a key, are being succeeded by a generation that posts updates on their lives to bare acquaintances and stores their personal files on remote servers around the world.[56]

Rather than seeking an overarching theory of privacy, a better approach may be to consider whether it is possible to reconceptualise privacy from the bottom up, focusing on "the concrete, the factual, and the experienced situations" of privacy.[57] Such a pragmatic approach to privacy as a practice rather than as a theory has two potential advantages over previous attempts to offer a coherent theory of privacy. The first is that it acknowledges the dynamic aspect of this field, which struggles to be defined by reference to nominally innate human qualities that nonetheless are changing swiftly and with widespread effects. The second is that such an approach more properly focuses attention on the true area of concern, which has largely moved from the preservation of a sphere of life isolated from the public gaze to the management of how information about oneself is produced, stored, and shared.[58]

As a theory of privacy, "control over information" has many deficiencies. Its focus on information excludes many areas widely held to be basic to privacy, such as the ability to make fundamental decisions about one's body and family life;[59] insofar as it suggests that control is limited to the individual who is the subject of that information it fails to account for the social value of privacy.[60] Nevertheless, as a framework through which to view present debates over what is loosely termed "privacy", the focus on information accurately highlights the overlapping but discrete subject of data protection. If only for functional reasons associated with the globalisation of information flows, this is an area that has seen far greater movement and relative coherence. In Asia in particular, many jurisdictions now embrace data protection laws even in the absence of any formal protection of a more abstract right to privacy. In Europe, it is telling that the recently proposed changes to the *E.U. Data Protection Directive* similarly focus on data protection while barely mentioning "privacy" as such.[61]

---

55 Charles J. Sykes, *The End of Privacy: Personal Rights in the Surveillance Society* (New York: St Martin's Press, 1999) at 8.

56 *Cf.* Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago: University Of Chicago Press, 1996) at 151, 152.

57 Daniel J. Solove, "Conceptualizing Privacy" (2002) 90 Cal. L. Rev. 1087 at 1129 [Solove, "Conceptualizing Privacy"]. *Cf.* Kirsty Hughes, "A Behavioural Understanding of Privacy and Its Implications for Privacy Law" (2012) 75 Mod. L. Rev. 806.

58 *Cf.* Westin, *supra* note 5 at 7.

59 Solove, "Conceptualizing Privacy", *supra* note 57 at 1109-1115.

60 Ferdinand Schoeman, "Privacy: Philosophical Dimensions of the Literature" in Ferdinand Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984) 1 at 3.

61 EC, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement*

## IV. The Turn to Data Protection

Despite the significant barriers to general acceptance of a right to privacy, there have been considerable steps towards a unified approach to data protection. Though the two terms are often used as if they were interchangeable, data protection is a narrower concept and more susceptible to definition.[62] An additional difference is that the right to privacy is generally understood as *limiting* government powers that might otherwise interfere with reasonable respect for a private life. Data protection, by contrast, typically requires an *expansion* of government powers, to monitor compliance of both government and third parties that collect, use, or disseminate personal data.[63]

For Singapore, like many Asian jurisdictions, the driving force behind reforms was not the threat-technology-culture mix that has driven reform in the United States, nor the human rights-led approach that characterises Europe. Rather, it is the economic imperative of globalisation and the need to adopt standards that will afford trust in national institutions and seamless integration into global networks.[64]

### A. *The Situation before the* Personal Data Protection Act 2012

Before passage of the *Personal Data Protection Act 2012*,[65] no legislation in Singapore dealt comprehensively with privacy or data protection. Numerous statutes did include secrecy and disclosure provisions that affected the processing of personal data; the National Internet Advisory Committee ("N.I.A.C.") in a 2002 report listed 161 such laws.[66] The most important laws governing data held by the Government and statutory boards include the *Official Secrets Act*,[67] the *Statistics Act*,[68] the *Statutory Bodies and Government Companies (Protection of Secrecy) Act*,[69] the

*of such data (General Data Protection Regulation)*, Brussels, 25 January 2012, COM/2012/011 final - 2012/0011 (COD), arts. 30(3) (reference to privacy by design), 32(1) (requirement of notification where a data breach "is likely to adversely affect the protection of the personal data or privacy of the data subject"), online: European Commission <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> [*Proposal for a General Data Protection Regulation*].

62 *Cf.* Karen McCullagh, "Protecting 'Privacy' Through Control of 'Personal' Data Processing: A Flawed Approach" (2009) 23(1-2) Int'l Rev. L. Computers & Tech. 13.

63 Newman, *supra* note 3 at 328, 329.

64 Lee Kuan Yew's notorious quote is often invoked in such discussions: "I am often accused of interfering in the private lives of citizens… Had I not done that, we wouldn't be here today. And I say without the slightest remorse: that we wouldn't be here, we would not have made economic progress, if we had not intervened on very personal matters—who your neighbour is, how you live, the noise you make, how you spit, or what language you use." Lee Kuan Yew, quoted in *The Straits Times* (20 April 1987).

65 No. 26 of 2012, Sing. [*PDPA*]. A copy of the *PDPA* may be found at Sing., Ministry of Communications and Information, *Personal Data Protection Act 2012*, online: Ministry of Communications and Information <http://www.mci.gov.sg/content/dam/mci_corp/Infocomm/Data%20Protection%20Bill/PDPA.pdf>.

66 Sing., National Internet Advisory Committee Legal Subcommittee, *Report on a Model Data Protection Code for the Private Sector* (February 2002), Annex 2, online: Attorney-General's Chambers <http:// app.agc.gov.sg/DATA/0/Docs/PublicationFiles/Model_Data_Protection_Code_Feb2002.pdf>, [N.I.A.C. Report].

67 Cap. 213, 2012 Rev. Ed. Sing.

68 Cap. 317, 2012 Rev. Ed. Sing.

69 Cap. 319, 2004 Rev. Ed. Sing.

*Central Provident Fund Act*,[70] and the *Electronic Transactions Act*.[71] Statutes regulating data held by particular private sector entities include the *Banking Act*[72] and the *Telecommunications Act*.[73] The *Computer Misuse Act* more generally criminalises unauthorised access to data, whether personal or not;[74] it does not regulate the collection and use of personal data by otherwise lawful means.[75]

The common law provides additional protection. The law of confidence is the primary instrument for addressing misuses of private confidential information in many Commonwealth jurisdictions, though this tends to be linked to publication of that information.[76] Additional remedies may be available through the tort of private nuisance[77] and the tort of harassment, which was the subject of a landmark 2001 decision by Singapore's High Court.[78] Trespass and defamation may also play a role.[79]

This piecemeal approach was long recognised as inadequate and, in particular, to limit Singapore's aspirations to be a "trusted node".[80] In February 2002, the Legal Subcommittee of N.I.A.C. published a draft "Model Data Protection Code for the Private Sector". The Model Code drew on a Canadian model code[81] that was in turn based on the 1980 O.E.C.D. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[82] The hope was that such a code could establish baseline standards for data protection and promote harmonisation in an area previously distinguished by its fragmentation.[83] After public consultations, a slightly modified Model Code was released by N.I.A.C. in December 2002.[84]

---

70 Cap. 36, 1999 Rev. Ed. Sing.

71 Cap. 88, 2011 Rev. Ed. Sing.

72 Cap. 19, 2008 Rev. Ed. Sing.

73 Cap. 323, 2000 Rev. Ed. Sing.

74 Cap. 50A, 2007 Rev. Ed. Sing., s. 3.

75 See generally Vili Lehdonvirta, "The European Union Data Protection Directive and the Adequacy of Data Protection in Singapore" [2004] Sing. J.L.S. 511 at 516.

76 *X v. CDE* [1992] 2 S.L.R.(R.) 575 (H.C.). See Megan Richardson, "The Private Life After *Douglas v. Hello*!" [2003] Sing. J.L.S. 311 at 327. For an examination from a U.S. perspective, see Neil M. Richards & Daniel J. Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Geo. L.J. 124.

77 See *e.g.*, *Motherwell v. Motherwell* (1976) 73 D.L.R. (3rd) 62 (Alta. S.C. (A.D.)); *Khorasandjian v. Bush* [1993] 3 All E.R. 669 (C.A.).

78 *Malcomson Nicholas Hugh Bertram v. Mehta Naresh Kumar* [2001] 3 S.L.R.(R.) 379 (H.C.).

79 Michael Hwang & Andrew Chan, "Singapore" in Michael Henry, ed., *International Privacy, Publicity & Personality Laws* (London: Butterworths, 2001) 355 at 356.

80 Infocomm Development Authority of Singapore, Media Release, "Singapore Launches Electronic Commerce Masterplan" (23 September 1998), online: Infocomm Development Authority of Singapore <http://www.ida.gov.sg/About-Us/Newsroom/Media-Releases/1998/20050726105559.aspx#.ULltD2eQNEI>.

81 Model Code for the Protection of Personal Information, CSA Standard CAN/CSA-Q830 (Mississauga, Ontario: Canadian Standards Association, 1996), online: CSA Group <http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code>.

82 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), online: Organisation for Economic Co-operation and Development <http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionof-privacyandtransborderflowsofpersonaldata.htm#top> [O.E.C.D. *Guidelines*].

83 N.I.A.C. Report, *supra* note 66 at para. 1.6.

84 Sing., National Trust Council and Infocomm Development Authority of Singapore, Model Data Protection Code for the Private Sector, v. 1.3 (Final) (December 2002), on file with the author [Model Code].

### B. *The Move to Comprehensive Legislation*

The move to a comprehensive legislative framework in Singapore gained momentum in October 2005 when an inter-ministry Data Protection Subcommittee was convened. The new Subcommittee reviewed, among other things, privacy concerns, commercial requirements, and the national interest, concluding that data protection should be strengthened.[85]

Further consultations ensued, and in February 2011 Singapore's Minister for Information, Communications and the Arts stated that the Government had concluded that it would be in Singapore's interest to put in place a data protection regime with a view to protecting personal data against unauthorised use and disclosure for profit.[86] The Minister outlined plans to introduce legislation for consideration by Parliament in 2012, which would be designed to curb excessive collection of personal data and require the consent of individuals when disclosing those data.[87] At the same time, it was made clear that the intention was to enhance Singapore's overall competitiveness and strengthen its position as "a trusted hub for businesses and a choice location for global data management and processing services."[88]

The reasons for adopting a data protection law were only partly true questions of law reform. Some of these questions had been addressed in the context of adopting the Model Code. The need to guard against outright theft of personal data is real, but can largely be addressed through other laws, notably including the *Computer Misuse Act*.[89] Regulation of an expanding e-commerce sector and maintaining consumer confidence were also a significant consideration in adopting the Model Code,[90] though the absence of legislation does not appear to have impeded growth. More generally, the Model Code did not resolve the basic problem that the patchwork of statute, case law, and guidelines was incoherent and inefficient. This was acknowledged in the N.I.A.C. Report that regarded the Model Code as a "first step" towards potential legislation.[91]

There were other issues that did not appear to have been considered in the context of the Model Code, such as possible inclusion of a "do not call" or "do not S.M.S." mechanism. The 2007 *Spam Control Act* included a requirement that commercial electronic messages (e-mails and text messages) indicate that a message is advertising by prefacing the subject line with "<ADV>"[92] and provide a means of unsubscribing from future messages.[93] Nevertheless, the Act did not cover voice calls, such as those made by telemarketers, which were excluded from the definition of "electronic message".[94] In addition, the unsubscribe function only applied

---

85 "Inter-Ministry Panel Looking at Data Protection", *The Straits Times* (4 March 2006).

86 Sing., *Parliamentary Debates*, vol. 87, col. 2619 (14 February 2011) (Lui Tuck Yew); also available as Notice Paper No. 9 of 2011, Question No. 683 for Written Answer at para. 7, online: Ministry of Information, Communications and the Arts <http://app.mica.gov.sg/Default.aspx?tabid=231>.

87 *Ibid*. at paras. 8, 9.

88 *Ibid.* at para. 8.

89 See *supra* note 74.

90 N.I.A.C. Report, *supra* note 66 at paras. 5.3-5.7.

91 *Ibid.* at paras. 5.15-5.17, 10.2.

92 *Spam Control Act* (Cap. 311A, 2008 Rev. Ed. Sing.), 2nd Sch. at para. 3(1)(b).

93 *Ibid.*, 2nd Sch. at para. 2.

94 *Ibid.*, s. 4(3).

to individual organisations, making it impossible to opt out of receiving unsolicited commercial electronic messages entirely.[95]

Such matters were considered in the drafting of the new law, but the primary impetus for adopting a data protection law was economic. In addition to other shortcomings, the previous regime for data protection in Singapore fell short of European standards that have become, by default, global. This was evident even in the adoption of the Model Code, which highlighted the importance of the European Union as a trading partner and concerns that the lack of a data protection regime might place Singapore at a competitive disadvantage.[96]

It would be wrong, however, to imply that Singapore's new legislation was drafted with an eye to satisfying E.U. adequacy requirements. It is no exaggeration, by contrast, to highlight that unlike most data protection regimes around the world that are intended to slow the flow of data, the *PDPA* was adopted in order to *increase* that flow by cementing Singapore's position as a "trusted node".[97]

## V. SINGAPORE'S *PERSONAL DATA PROTECTION ACT 2012*

The public consultations prior to the adoption of the *PDPA* included two rounds of consultations on the proposed data protection regime and the proposed Do Not Call Registry. In March 2012, the Ministry of Information, Communications and the Arts issued a further consultation paper and took the unusual step of publishing the draft legislation for additional comments.[98] That process—and the obvious efforts to demonstrate sensitivity to industry concerns both in the content of the legislation[99] and the relatively lengthy sunrise period[100]—suggests the hopes that the new law would facilitate rather than impede commerce.

In terms of the implications for privacy, it is telling that although the word "privacy" appeared in passing in the various consultation papers, it is entirely absent from the legislation as adopted. Instead, the purpose as articulated in the Act is clearly focused on the management of information:[101]

> The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

---

95 Karthik Ashwin Thiagarajan, "The Spam Control Act 2007" [2007] Sing. J.L.S. 361; Richard Hartung, "Don't Call Us, Period" *Today* (21 April 2010), online: Today <http://imcms2.mediacorp.sg/CMSFileserver/documents/006/PDF/20100421/2104CAP019.pdf>.

96 N.I.A.C. Report, *supra* note 66, Executive Summary at paras. 2.1-2.3.

97 See *supra* note 80; *PDPA*, *supra* note 65.

98 Sing., Ministry of Information, Communications and the Arts, *Public Consultation Issued by Ministry of Information, Communications and the Arts: Proposed Personal Data Protection Bill* (Consultation Paper) (19 March 2012), online: Ministry of Information, Communications and the Arts <http://app.mica.gov.sg/Default.aspx?tabid=487> [M.I.C.A. March 2012 Public Consultation].

99 See *e.g.*, *ibid*. at para. 2.7 (the proposed definition "is one that the industry is already familiar with").

100 *Ibid.* at para. 2.134 ("sunrise period of no less than 18 months").

101 *PDPA*, *supra* note 65, s. 3.

Such explicit balancing of the rights of individuals and the "need[s]" of organisations is hard to reconcile with a rights-based approach to privacy; it is better understood as a pragmatic attempt to regulate the flow of information, moderated by the touchstone of reasonableness.

This Part outlines the scope of the Act by reference to the data covered, the entities affected, the conduct regulated, and the mechanisms for enforcement. The inclusion of a Do Not Call registry is somewhat anomalous in the context of a data protection law—in that it does not matter how the telephone numbers are acquired[102]—but its inclusion again highlights the pragmatic approach to the governance of information flows more generally rather than a notion of privacy *stricto sensu*.

### A. *Personal Data*

Personal data is defined in the *PDPA* as:[103]

> data, whether true or not, about an individual who can be identified
> (a) from that data; or
> (b) from that data and other information to which the organisation is likely to have access.

"Individual" is in turn defined as "a natural person, whether living or deceased".[104]

This definition is similar to that used in the Model Code, but no longer limited to data in electronic form or to data concerning a living individual.[105] Paper records had been excluded for reasons of practicality,[106] but both in principle and in recognition of the amount of personal data routinely collected—for example, in the form of lucky draw and other competitions—it made sense to include such personal data in the Act.[107]

The inclusion of the personal data of deceased persons is more interesting. The E.U. lacks such a protection, which appears to be modelled on Canadian legislation.[108] Such a provision calls into question the reason for data protection in the first place. Is personal data a property interest to be protected? If so, why is it protected for only 10 years?[109] Or is data protection linked to protection of individual rights that pass with the individual? There is a legitimate interest in preventing the personal details of recently deceased persons from being made public, or the health details of relatives from being sold to one's insurance company, but it is not clear that addressing these potential harms is best done through general inclusion in a data protection law. Again, the legislation suggests that it is best understood not with

---

[102] *Cf.* Daniel J. Solove & Chris Jay Hoofnagle, "A Model Regime of Privacy Protection" (2006) 2006 U. Ill. L. Rev. 357 at 370.

[103] *PDPA*, *supra* note 65, s. 2(1).

[104] *Ibid*.

[105] *Cf.* Model Code, *supra* note 84 at para. 2.

[106] As the N.I.A.C. Report observed, paper records range "from the systematic to the shambolic": N.I.A.C. Report, *supra* note 66 at para. 8.19.

[107] M.I.C.A. March 2012 Public Consultation, *supra* note 98 at para. 2.9.

[108] *Cf. Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 7(3)(h)(ii) [*PIPEDA*] (disclosure without knowledge or consent is permitted, *inter alia*, "twenty years after the death of the individual whom the information is about").

[109] *PDPA*, *supra* note 65, s. 4(4)(b).

reference to protection of individualised rights to privacy so much as an attempt to govern information flows more generally. (The legislation is also interesting for the compromise that was struck between those who supported coverage for 20 years and those who opposed coverage entirely—resolved by a Solomonic decision to cover the personal data of deceased persons for 10 years only.)

1. *Existing Data*

The Act is prospective, meaning that organisations may continue to use personal data collected prior to its entry into force for the same purposes. That implied consent can be withdrawn by subsequent action, but another exception covers situations in which an individual has "otherwise indicated", before or after the legislation enters into force, that he or she does not consent to the use of the personal data.[110]

The limited protection offered is the ability to withdraw consent for the on-going use of previously collected data. This applies only to organisations in possession of those data, including their agents and data intermediaries[111]—meaning that withdrawal of consent must be communicated to each organisation and would not affect other parties with which those data had been shared. Nor does such a provision imply the ability to request that such data be deleted (or "forgotten"), only that its future use and disclosure may be limited.

2. *Publicly Available Data*

Business contact information is largely excluded,[112] as are personal data that are "publicly available".[113] This is defined as meaning personal data that are:[114]

> generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event?—
>
> (a) at which the individual appears; and
>
> (b) that is open to the public[.]

A key question is likely to be whether the posting of data on social networking sites such as Facebook makes those data "generally available".

3. *Sensitive Personal Data*

The *PDPA* does not distinguish between different forms of personal data. Without using the word, the *E.U. Data Protection Directive* provides stronger protections for data regarded as 'sensitive'. The U.K. implementing legislation established a special category of "sensitive personal data". Both require a higher threshold of consent before such data may be processed.[115]

---

110 *Ibid.*, s. 19.

111 *Ibid.*, s. 16.

112 *Ibid.*, s. 4(5).

113 *Ibid.*, 2nd Sch. at para. 1(c); 3rd Sch. at para. 1(c); 4th Sch. at para. 1(d).

114 *Ibid.*, s. 2(1).

115 *E.U. Data Protection Directive*, *supra* note 51, art. 8; *Data Protection Act 1998* (U.K.), 1998, c. 29, s. 2 [*U.K. Data Protection Act*].

There are on-going debates over the appropriate definition of sensitive personal data.[116] Malaysia's *PDPA* defines sensitive personal data as including medical history, political opinions, religious beliefs, and the commission or alleged commission of any offence.[117] Notable differences from the E.U. approach include the exclusion of racial or ethnic origin and sex life.[118] Singapore's Model Code drew heavily on the Canadian precursor to the *Personal Information Protection and Electronic Documents Act*, and merely provided that when determining the form of consent appropriate to the processing of data, the sensitivity of those data should be taken into account.[119] In general, express consent should be required when the data in question are sensitive.[120] "Sensitive" was not defined in the Model Code, but the explanatory notes used the examples of medical and financial records as data that are almost always regarded as sensitive.[121]

The decision not to create a category of sensitive personal data in the *PDPA* was justified in part by the novelty of the regime being implemented and the possibility of sector-specific frameworks to address particular concerns.[122] This would include, for example, the *Banking Act* and existing codes for medical professionals.[123]

### 4. *Children's Data*

Whereas it is arguable that sensitive personal data enjoy some measure of sector-specific protection, a significant gap exists in the protection of the personal data of children.

This is an area in which the United States actually provides greater protection than Europe. The *E.U. Data Protection Directive*—like the *PDPA*—does not refer to children specifically, meaning that the protections in place are the same as for their parents. Two implicit assumptions are that parents are aware of their children's activities online and are in a position to help guide them in making appropriate decisions. Neither assumption withstands much scrutiny when compared to the actual online behaviour of children. Some jurisdictions within Europe have adopted codes of conduct intended to regulate the activity of marketing, but these are generally

---

116 Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, 3rd ed. (Oxford: Oxford University Press, 2009) at 83.

117 Malaysia's *PDPA*, *supra* note 46, s. 4.

118 *E.U. Data Protection Directive*, *supra* note 51, art. 8(1).

119 Model Code, *supra* note 84 at para. 4.3.3. *Cf. PIPEDA*, *supra* note 108, 1st Sch. at para. 4.3.4; EU, Data Protection Working Party, Doc. 5109/00/EN WP39, *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act* (26 January 2001) at 3, online: European Commission <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp39en.pdf>.

120 Model Code, *ibid.* at para. 4.3.6.

121 *Ibid*. at para. 4.3.3, Implementation and Operational Guidelines.

122 M.I.C.A. March 2012 Public Consultation, *supra* note 98 at para. 2.8. But see *PDPA*, *supra* note 65, 4th Sch. at para. 1(r) (allowing for disclosure without consent for archival or historical purposes "if a reasonable person would not consider the personal data to be too sensitive to the individual").

123 See Sing., *Parliamentary Debates*, vol. 87 (16 September 2010) (Lui Tuck Yew); also available as Notice Paper No. 116 of 2010, Question No. 462 for Written Answer (Singapore: Parliament, 19 July 2011), online: Ministry of Information, Communications and the Arts <http://app.mica.gov.sg/Default.aspx?tabid=477>.

regarded as weak or ineffectual.[124] (The draft Regulation now under discussion in the E.U. would include a new article on the personal data of children.[125])

The United States, by contrast, adopted legislation in the form of the *Child Online Privacy Protection Act*, which came into force in 2000.[126] It applies to commercial websites and online services directed at children aged under 13 and other websites that have actual knowledge that children aged under 13 are sharing personal information.[127] *COPPA* provides, among other things, requirements for the privacy policies of such sites, the circumstances in which "verifiable parental consent" must be obtained, and limitations on the use of any data collected. Though it is still possible to collect data, many sites now prohibit users under 13 completely—most prominently Facebook.

It is not clear that reliance on parental intervention is realistic, nor does the U.S. experience suggest that the costs to business of restricting collection of children's data are prohibitive. Nevertheless, accounts of parents tolerating or assisting their children creating Facebook accounts despite being under 13 are indicative of the relaxed attitude towards children's data protection in Singapore,[128] periodically tempered by scandals of abuse.[129]

It is possible that this will be revisited in the future.[130] One approach would be to require verifiable parental consent for the collection of the personal data of children, based on the U.S. law. Such consent can be verified in the United States through the submission of a credit card number or email, though these may be easily obtained by an enterprising child.[131] Alternative means of verification include provision of a handphone number, perhaps with some confirmation being sent via S.M.S., though an increasing number of children have their own phones. The most effective means of bypassing the media dominated by children may in fact be via "snail mail"—a letter.

### B. *Entities Affected*

The *PDPA* applies to "organisations", defined as meaning "any individual, company, association or body of persons, corporate or unincorporated".[132] It covers organisations that collect, use, or disclose data in Singapore whether or not those organisations have a physical presence in Singapore. The decentralisation of modern

---

124 Emmanuelle Bartolia, "Children's Data Protection vs Marketing Companies" (2009) 23 Int'l Rev. L. Comp. & Tech. 35.

125 *Proposal for a General Data Protection Regulation*, *supra* note 61, art. 8.

126 *Children's Online Privacy Protection Act*, 15 U.S.C. § 6501 (1998) [*COPPA*].

127 *Ibid*., §§ 6501, 6502.

128 Jamie Ee Wen Wei & Teo Wan Gek, "Kids Getting Internet Savvy at a Younger Age" *The Straits Times* (14 June 2009).

129 Elizabeth Soh, "Most Severe Court Case of Underage Sex; Growing Danger from Young Kids Going Online, Say Social Workers" *The Straits Times* (30 December 2010).

130 M.I.C.A. March 2012 Public Consultation, *supra* note 98 at para. 2.88. The Minister has the power, for example, to make regulations concerning the application of the Act to minors: *PDPA*, *supra* note 65, s. 65(2)(c).

131 Bartolia, *supra* note 124 at 39.

132 *PDPA*, *supra* note 65, s. 2(1). Confusingly, however, the offences section distinguishes between offences that are committed by "a person" and "an organisation or person": *ibid.*, s. 51.

telecommunications frequently gives rise to jurisdictional barriers to enforcement, but treating such organisations differently from those in Singapore might adversely affect local businesses.[133] Individuals acting in a personal or domestic capacity, or as employees of an organisation, are excluded.[134] Public agencies (the Government and tribunals appointed by law) are excluded entirely,[135] with the Minister empowered to designate any statutory body to be a public agency for the purposes of the *PDPA*.[136]

### 1. *Data Intermediaries*

One area in which the E.U.'s approach to data protection had come to be seen as unnecessary or unhelpful was the distinction made between data controllers and data processors. In the *E.U. Data Protection Directive*, as well as implementing legislation such as Britain's *Data Protection Act*, data controllers determine why and how personal data are processed; data processors act on behalf of controllers.[137] The distinction was intended to be the degree of autonomy that an entity exercises over the processing operations, but in practice this distinction can be difficult to ascertain.[138] It is also somewhat at odds with modern information technology practices, particularly as increasing amounts of data are stored "in the cloud" and content is user-generated.[139]

The *PDPA* introduces the new concept of a "data intermediary", which is "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation".[140] It is not clear why the term "data intermediary" was used rather than "data processor", since it is defined in almost identical terms as "processing" includes, *inter alia*, adaptation and alteration of data.[141] This is particularly puzzling since the concept of a "data intermediary" with a significantly reduced role has been mooted in the academic literature and proposed by industry.[142] If the intention is to define this category with reference to the E.U. standard, it might have been more appropriate to use the E.U. term. Otherwise, a narrower definition might have been better.

Data intermediaries have very limited obligations under the *PDPA* with respect to personal data processed for another organisation pursuant to a written contract.[143]

---

133 M.I.C.A. March 2012 Public Consultation, *supra* note 98 at paras. 2.17-2.20.

134 *PDPA*, *supra* note 65, s. 4(1)(a)-(b).

135 *Ibid*., s. 4(1)(c). The M.I.C.A. consultation paper stated that government data protection rules accord "similar levels of protection" to that in the *PDPA*, but as those rules are not public this claim is difficult to evaluate: M.I.C.A. March 2012 Public Consultation, *supra* note 98 at paras. 2.12-2.16.

136 *PDPA*, *supra* note 65, s. 2(2).

137 *E.U. Data Protection Directive*, *supra* note 51, art. 2; *U.K. Data Protection Act*, *supra* note 115, s. 1(1).

138 See Carey, *supra* note 116 at 211, 212; EU, Data Protection Working Party, Doc. 00264/10/EN WP169, *Opinion 1/2010 on the concepts of "controller" and "processor"* (16 February 2010), online: European Commission <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf>.

139 See *e.g.*, Vadim Schick, "Data Privacy Concerns for U.S. Healthcare Enterprises' Overseas Ventures" (2011) 4(2) J. Health & Life Sci. L. 173.

140 *PDPA*, *supra* note 65, s. 2(1).

141 *Cf. U.K. Data Protection Act*, *supra* note 115, s. 1(1).

142 Vodafone, "A Comprehensive Approach on Personal Data Protection in the European Union: European Commission Communication COM(2010) 609", online: Vodafone <http://www.vodafone.com/content/dam/vodafone/about/privacy/vodafone_response_com2010_609.pdf>.

143 *PDPA*, *supra* note 65, s. 4(2).

These obligations are limited to the protection of data "by making reasonable security arrangements"[144] and ensuring that it does not retain those data in a form that can be associated with particular individuals when the purpose for which those data were collected is no longer being served and retention is not necessary for "legal or business purposes".[145] The organisation that has contracted with the intermediary remains fully responsible under the Act in respect of data processed on its behalf.[146]

### 2. *News Organisations*

A potentially interesting category is the limited exemption granted to news organisations. Such organisations are exempted from the requirement to obtain consent for the collection (but not use or disclosure) of personal data "solely for its news activity".[147] The category was originally defined by reference to the type of organisation and activities undertaken, along with a requirement that any organisation must be gazetted as such by the Minister.[148] This was subsequently amended to include an elaborate definition of "news organisation" that limited it to activities carried out "in relation to a relevant broadcasting service, a newswire service or the publication of a newspaper". "Relevant broadcasting service" was in turn defined as a licensable broadcasting service within the meaning of the *Broadcasting Act*.[149] The implication appears to be that online publications are to be excluded from this exemption.

## C. *Rules on Collection, Use, and Disclosure*

The basic obligations under *PDPA* are that collection, use, and disclosure of personal data are permissible only with the actual or deemed consent of the individual, or where required by law.[150] Actual consent is only possible if the individual has been informed as to the purpose for which the personal data is being collected, used, or disclosed.[151]

An organisation cannot require an individual's consent to wider disclosure than is required for providing a given product or service, or procure it through misleading conduct.[152] There was significant discussion, however, as to whether consent can be deemed if an individual has failed to "opt-out" of a data collection scheme.[153] The Act now limits deemed consent to circumstances in which an individual voluntarily provides the personal data and it is reasonable that he or she *would* provide the data.[154]

---

144 *Ibid*., s. 24.
145 *Ibid*., s. 25(b).
146 *Ibid*., s. 4(3).
147 *Ibid.*, 2nd Sch. at para. 1(h).
148 See the M.I.C.A. March 2012 Public Consultation, *supra* note 98 at Annex D for the March 2012 Draft of the *Personal Data Protection Bill* released for consultation, s. 2 [March 2012 Draft of *PDPA Bill*].
149 Cap. 28, 2012 Rev. Ed. Sing. See *PDPA*, *supra* note 65, 2nd Sch. at para. 2.
150 *Ibid*., s. 13.
151 *Ibid*., ss. 14(1)(a), 20.
152 *Ibid*., s. 14(2).
153 See M.I.C.A. March 2012 Public Consultation, *supra* note 98 at paras. 2.49, 2.50.
154 *PDPA*, *supra* note 65, s. 15(1).

It is arguable that the E.U. requirement of unambiguous consent requires an opt-*in* approach—that is, the default position should be that data will not be shared with third parties or used other than for the purposes for which it is given.[155] (This is also the position taken in the draft Regulation that may soon supplant the *E.U. Data Protection Directive*.[156]) In any case, based on the past decade's experience with the Model Code and the—at best—partial success of the *Spam Control Act*, the decision to require an opt-in approach with very limited provision for deemed consent is appropriate. Consent, however given, can be withdrawn with reasonable notice.[157]

In complying with these obligations, organisations are required to develop policies for implementation, including a process to respond to complaints.[158] Organisations are also required to "consider", when meeting those obligations, "what a reasonable person would consider appropriate in the circumstances."[159] How an organisation would engage in such contemplation is unclear, but there is separate provision that the purposes for which personal data is collected, used, or disclosed must be purposes "that a reasonable person would consider appropriate in the circumstances".[160]

These reasonableness caveats may aid in addressing one of the most basic problems in data protection regimes, which is analogous to the problems confronting privacy discussed earlier:[161] in theory, consent can regulate the appropriate flow of personal data; in practice, consent routinely fails to do so either because consumers do not understand the options or companies do not give them a meaningful choice.[162]

Another provision that highlights the focus on information flows rather than privacy-type rights concerns access to and correction of personal data. Organisations are obliged to "make a reasonable effort" to ensure that personal data are "accurate and complete", if those data are likely to be used "to make a decision that affects the individual" or shared with another organisation.[163] An individual has a limited right to request access to personal data and request the correction of errors or omissions in personal data concerning him or her.[164]

All organisations are required to protect personal data in their possession or control by "making reasonable security arrangements" to prevent unauthorised access.[165] When "it is reasonable to assume" that the purpose for which the data were collected no longer requires retention and there is no business or legal requirement to retain the data, the organisation must "cease to retain its documents containing personal data" or remove the means by which those data can be associated with

---

155 See generally Michael E. Staten & Fred H. Cate, "The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA" (2003) 52 Duke L.J. 745 at 749.

156 *Proposal for a General Data Protection Regulation*, *supra* note 61.

157 *PDPA*, *supra* note 65, s. 16.

158 *Ibid.*, s. 12.

159 *Ibid.*, s. 11(1).

160 *Ibid.*, s. 18(a).

161 See *supra* note 55 and accompanying text.

162 See generally Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA" (2006) 56 U.T.L.J. 181; Matthew S. Kirsch, "Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising" (2011) 18 Rich. J.L. & Tech. 2.

163 *PDPA*, *supra* note 65, s. 23.

164 *Ibid*., ss. 21, 22.

165 *Ibid*., s. 24.

particular individuals.[166] This replaced an earlier requirement to destroy personal data,[167] though the breadth of the category "business purposes" will likely reduce the significance of this provision.

### 1. *Exceptions to the Requirement for Consent*

The *PDPA* allows for the collection, use, or disclosure of personal data without consent in specified circumstances, elaborated in the Second, Third, and Fourth Schedules[168]—which may be amended by the Minister by order published in the *Gazette*.[169] The three schedules run to some nine pages, but there is significant overlap. Collection, use, or disclosure is permitted, for example, where it is "clearly in the interest of the individual" and consent cannot be obtained in a timely way; in response to an emergency; necessary in the national interest, or for an investigation or legal proceedings; for the collection of a debt; for the provision of legal services; or otherwise authorised by law.[170]

A further exclusion is made for "evaluative purposes", including decisions related to employment, admission to educational institutions, and contractual and insurance matters.[171] Exemptions are also made for "news organisations" discussed earlier,[172] and where collection—but not use or disclosure—is solely for "artistic or literary purposes".[173] Personal data may not be collected, but it may be used or disclosed without consent, for certain research purposes.[174] And a general exclusion allows for disclosure—but not collection or use—to a public agency if necessary in the public interest.[175]

### 2. *Transborder Transfers*

The original draft of Singapore's Model Code included an eleventh principle, said to be "optional", that covered transborder transfers of data and was loosely based on art. 25 of the *E.U. Data Protection Directive*.[176] In its place, the Model Code as adopted provided only that organisations transferring data to any third party should "take reasonable steps to ensure that the data... will not be processed inconsistently" with the Code.[177]

The *PDPA* does not embrace the E.U. approach of making adequacy determinations as to jurisdictions to which personal data may be transferred, but it does now prohibit the transfer of personal data outside Singapore without ensuring that

---

166 *Ibid*., s. 25.
167 March 2012 Draft of *PDPA Bill*, *supra* note 148, s. 27(2).
168 *PDPA*, *supra* note 65, s. 17.
169 *Ibid*., s. 64(1).
170 *Ibid*., 2nd Sch. at para. 1; 3rd Sch. at para. 1; 4th Sch. at para. 1.
171 *Ibid*., s. 2(1).
172 See *supra* notes 147-149.
173 *PDPA*, *supra* note 65, 2nd Sch. at para. 1(g). Use and disclosure were covered in the draft legislation: March 2012 Draft of *PDPA Bill*, *supra* note 148, 4th Sch. at para. 1(i); 5th Sch. at para. 1(k).
174 *PDPA*, *supra* note 65, 3rd Sch. at para. 1(i); 4th Sch. at para. 1(q).
175 *Ibid*. at 4th Sch. at para. 1(g).
176 N.I.A.C. Report, *supra* note 66 at paras. 8.12, 8.47-8.50.
177 Model Code, *supra* note 84, s. 4.1.1.

organisations receiving the data provide a "standard of protection… comparable to the protection under" the *PDPA*.[178]

Some of the uncertainty may be removed by the new Personal Data Protection Commission, which is empowered to exempt organisations from the requirements concerning the transfer of personal data outside Singapore.[179]

### 3. *Data Breach Notification*

The Act does not include a provision requiring organisations to notify customers in the event that personal data is compromised. In 2008, the Australian Law Reform Commission ("A.L.R.C.") recommended creating a new obligation to notify the Privacy Commissioner and affected individuals when an unauthorised person acquires personal data and there is a real risk of serious harm.[180] Similar requirements were debated in the United States, in the wake of Citigroup's revelation that personal data from 200,000 credit card holders were stolen by hackers.[181]

A blanket obligation to report every breach could be excessively onerous. A recent proposal by the White House would have limited the obligation to organisations that collect personal data of 10,000 people in any 12-month period.[182] The A.L.R.C. threshold of "real risk of serious harm" would clearly encompass possible identity theft, but limit the need to report on data breaches that do not include identifying information.

Additional questions include identifying where data resides and who should be obliged to make the report: the organisation that collected the information in the first place and has a relationship with the customer, or the service provider who stored the data? In the U.S., state legislation generally puts the onus on the former.[183] To whom should such a report be made? Where serious harm might follow, the customer should be advised. But more generally it would be desirable to have the supervisory authority—the Personal Data Protection Commission—informed. Taiwan recently adopted amendments to its *Data Protection Act* (which came into force on 1 October 2012) that would include a modest data breach notification requirement for violations of the Act, though it has been criticised for not having a supervisory body.[184]

An alternative approach to data breach notification is not to make it a mandatory obligation, but to consider any such notification to those who might be injured by

---

178 *PDPA*, *supra* note 65, s. 26(1).

179 *Ibid*., s. 26(2)-(4).

180 Austl., Commonwealth, Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No. 108) (Canberra: Australian Government Publishing Service, 2008), recommendation 51-1, online: Australian Law Reform Commission <http://www.alrc.gov.au/publications/report-108>.

181 Eric Dash, "Citi Data Theft Points Up a Nagging Problem" *New York Times* (9 June 2011), online: New York Times <http://www.nytimes.com/2011/06/10/business/10citi.html?pagewanted=all&_r=0>.

182 Elizabeth Montalbano, "White House Seeks National Data-Breach Notification Law" *InformationWeek* (13 May 2011), online: InformationWeek <http://www.informationweek.com/government/policy/white-house-seeks-national-data-breach-n/229500626>.

183 Jacqueline May Tom, "A Simple Compromise: The Need for a Federal Data Breach Notification Law" (2010) 84 St. John's L. Rev. 1569.

184 Shamma Iqbal, "Taiwan Introduces Enforceable Data Breach Notification Requirements", *Inside Privacy* (9 March 2011), online: Inside Privacy <http://www.insideprivacy.com/international/tawain-introduces-enforceable-data-breach-notification-requirements/>.

the data breach as a mitigating factor in enforcement proceedings. If this is the case, reference to data breach notifications should be included in penalty guidelines that are drafted for enforcement purposes.[185] This is useful both in ensuring fairness and telegraphing to organisations that it is in their interest to notify customers of data breaches.

### 4. *Do Not Call Registry*

The slightly odd fit of the Do Not Call Registry within the *PDPA* is suggested by having its own interpretive clause.[186] The obligations created are additional to those in the *Spam Control Act*, on the basis that whereas that Act puts conditions on the sending of unsolicited commercial messages sent in bulk, the Do Not Call Registry determines whether a specified message may be delivered to a specific telephone number. "Specified message" for this purpose is defined by reference to the content, presentation, or linked information; a message is covered by the provision if, having regard to that information, "it would be concluded" that one of the purposes of the message is to advertise or otherwise offer to supply goods or services, an interest in land, or a business or investment opportunity.[187]

Such messages may not be sent to a Singapore telephone number that has been entered on a Do Not Call Register.[188] The legislation as adopted significantly narrows the scope of this obligation, which had originally applied regardless of whether the sender or recipient were in Singapore at the time the message was sent or accessed.[189] It is now limited to circumstances in which at least one party was in Singapore.[190] Unlike the rest of the *PDPA*, the Do Not Call provisions apply to a "person" who sends such messages, who is under an obligation to check the Do Not Call Registry within a period to be prescribed.[191] Failure to comply is an offence punishable with a fine of up to £10,000.[192]

## D. *Enforcement*

The *PDPA* establishes a Personal Data Protection Commission consisting of three to seventeen members appointed by the Minister.[193] Its mandate includes enforcing the Act but also promoting awareness, conducting research, and advising the Government on data protection generally.[194] Provision is made for the Commission to produce non-binding guidelines, which will likely play an important role in implementation of the Act.[195]

---

185 *Cf.* M.I.C.A. March 2012 Public Consultation, *supra* note 98 at para. 2.112.
186 *PDPA*, *supra* note 65, s. 36.
187 *Ibid*., s. 37.
188 *Ibid*., s. 43(1).
189 March 2012 Draft of *PDPA Bill*, *supra* note 148, ss. 42, 47(1).
190 *PDPA*, *supra* note 65, s. 38.
191 *Ibid*., s. 43(1).
192 *Ibid*., s. 43(2).
193 *Ibid*., s. 5(1).
194 *Ibid*., s. 6.
195 *Ibid*., s. 49.

The basic model of enforcement is largely complaints-based rather than audit-based, or what is sometimes termed "fire-alarm" rather than "police-patrol" regulation.[196] Where the Commission is satisfied that an organisation is not complying with the Act, it may direct the organisation to stop collecting, using, or disclosing personal data; to destroy personal data; and/or to pay a financial penalty of up to $1 million.[197] This is separate from the offences created, which include requesting access to personal data without authority; evading an individual's request for access to personal data; and obstructing or misleading the Commission.[198] Where no other penalty is provided for, the maximum penalty is a fine of up to $10,000 and up to three years in prison.[199]

Britain's Information Commissioner has a similar power to issue "enforcement notices"—requiring a data controller to take (or to refrain from taking) specified actions if the Commissioner is satisfied that the controller has contravened the data protection principles.[200] Beginning in April 2010, if there is a serious contravention that is likely to cause "substantial damage or substantial distress", and the controller knew or ought to have known that there was a risk of such an outcome, the Commissioner has also been able to impose monetary penalties of up to £500,000.[201]

The *PDPA* also provides that an individual who suffers "loss or damage directly as a result" of a contravention of the Act may also bring a civil suit against the organisation responsible.[202]

## VI. Conclusion

The digital revolution has transformed the way we think about information. That transformation has in turn challenged our conceptions of privacy and the legal tools available to defend it. In some ways this is not new: efforts to defend privacy have always been forced to react to new threats, new technology, and the changing cultural context. Yet the new paradigm of information sharing and dissemination—illustrated for the purposes of this article by Facebook and WikiLeaks—makes it harder than ever to assert a right to privacy in a meaningful sense.

These practical considerations have exacerbated the tensions that bedevil any attempt to articulate a general theory of privacy. That task remains difficult, but does not remove the need for robust norms of data protection. Competing models broadly reflect the tensions in the theoretical approaches to privacy, but the impetus for reform is not always a desire to protect privacy as such. In Singapore, at least, reform is not being driven by the desire to defend the rights of data subjects; rather, it is based primarily on economic considerations, as well as the desire to position Singapore as a leader in the region for data storage and processing.

---

196 *Cf.* Mathew D. McCubbins & Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms" (1984) 28 Am. J. Pol. Sci. 165 at 166-176.

197 *PDPA*, *supra* note 65, s. 29. Decisions of the Data Protection Commission, which are enforceable through the District Court, may be appealed to a new Data Protection Appeal Panel, with further appeal possible to the High Court: *ibid*., ss. 30, 34, 35.

198 *Ibid*., s. 51.

199 *Ibid*., s. 56.

200 *U.K. Data Protection Act*, *supra* note 115, s. 40.

201 *Ibid*., s. 55A.

202 *PDPA*, *supra* note 65, s. 32(1).

Such a pragmatic approach may well make it possible to strike an appropriate balance between the rights-based approach endorsed by Europe and the *laissez-faire*-plus-sectoral-patches approach of the United States. Even while acknowledging the importance of European regulators, this offers an opportunity for Singapore to respond to the transformations in the information economy. Among these transformations is the movement of focus from whether data should be collected in the first place, to how the ever-expanding volume of data already available should be used.

Much of the *PDPA* remains to be worked out in practice. The legislation aspires to be technologically neutral and "future-proof", albeit using traditionally common law touchstones of reasonableness (a term that is used 47 times). Moving forward, how Singapore's new law is implemented—"the concrete, the factual, and the experienced situations"[203]—may offer a lens through which to view the changing debates over privacy and, perhaps, offer the basis for a pragmatic theory of data protection.

[203] See *supra* note 57.