THE DATA PROTECTION PARADIGM FOR THE TORT OF PRIVACY IN THE AGE OF BIG DATA

It will be argued in this article that the legal scholarship on the common law tort of privacy in the US and some Commonwealth countries have not produced any meaningful concept of privacy appropriate for the age of big data. Due to the nature of digital information, a better paradigm for protection can be found in the European Union data protection regime. This article will also evaluate the Singapore Personal Data Protection Act (Act 26 of 2012) in this regard.

Hannah **LIM** Yee Fen
BSc, LLB, LLM (Hons) (University of Sydney);
Advocate and Solicitor (Singapore);
Associate Professor of Business Law, Nanyang Technological University, Singapore.

1 As legal scholar Raymond Wacks has commented, "the discourse on 'privacy' is anything but coherent".[1] Furthermore, "the voluminous literature on the subject has failed to produce a lucid or consistent meaning of a concept".[2] Indeed, Wacks has aptly summed up the current legal landscape. The impetus and framework focus of this article is big data and how big data forces a rethink of the traditional discourse on the common law tort of privacy. The generally accepted concepts of privacy as it is known at common law in the US and in some of the major Commonwealth countries will be considered. These will show the challenges of legal scholars and courts trying to grapple with a massive tort that seems to have no conceivable boundaries. This will be followed by a comparison with the key features of the 1995 European Union ("EU") Data Protection Directive ("Data Protection Directive" or "the Directive").[3] It will attempt to show that the Directive covers many of the areas that common law privacy has been grappling with; it also provides a workable and sensible blueprint for a restructuring of privacy law in the age of big data. It is the unifying legislation that can more appropriately deal with privacy encroachments than the current

1 Raymond Wacks, *Law, Morality, and the Private Domain* (Hong Kong University Press, 2000) ch 8.
2 Raymond Wacks, *Law, Morality, and the Private Domain* (Hong Kong University Press, 2000) ch 8.
3 Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data).

jurisprudence. Finally, the article will consider the position in Singapore.

2 It should be highlighted at the outset that in the age of big data, consideration of privacy is not merely academic, nor does it only have a place in high theory. The issues at stake here are associated with the facilitation of cybercrime and criminal activities in the physical world. In order to elucidate this, this article will begin by examining what exactly big data is and its potential contribution to criminal activities.

I. Big data

3 With endless and rapid advancements in technology, the law must adapt to new possibilities made available by innovation. In this regard, the privacy of individuals has been at stake since the advent of computers and computing networks, especially the Internet, but never before has the privacy of individuals been at greater risk than now with the rise of big data.

4 Data has always been collected even well before the invention of the computer and digital technology but computer hardware and software technologies and computer networks, and the increasing power and speed of all of these, have given unprecedented opportunities for data to be combined, matched, analysed, used and disclosed in ways unimaginable. There has also been an exponential growth in the volume of data collected, much greater data storage capacity and the increased ability to connect previously discrete data networks.

5 There is no precise definition of "big data" but it generally refers to the collection and analysis of unusually large datasets. The data is both structured and unstructured data generated from diverse sources in real time, in volumes too large for traditional technologies to capture, manage and process in a timely manner.[4] The datasets typically come from a variety of industries and settings, and the sources are often consumer and social media related with tracking technologies allowing the datasets to be combined and often matched. Some of the sources include websites, blogs, news feeds, social media, and public and private databases.[5]

6 Jules Berman describes big data as being characterised by "the three Vs". First, there must be *volume*, meaning large amounts of

4 Maureen Errity & John Lucker, "The Real Deal with Big Data" *Wall Street Journal* (6 November 2013).

5 Maureen Errity & John Lucker, "The Real Deal with Big Data" *Wall Street Journal* (6 November 2013).

data. Secondly, there must be *variety*, meaning that "the data comes in different forms, including traditional databases, images, documents, and complex records".[6] Lastly, there must be *velocity*, which means:[7]

> … the content of the data is constantly changing, through the absorption of complementary data collections, through the introduction of previously archived data or legacy collections, and from streamed data arriving from multiple sources.

7 Vast amounts of data are being created and collected everyday by the interactions of billions of people using computers, mobile phones and other electronic devices. Online or mobile financial transactions, social media traffic and global positioning system co-ordinates now generate over 2.5 quintillion bytes of big data every day.[8] Even the humble cash card and In-Vehicle Units used in Singapore-registered cars are amassing data every day and, within the next few years, these In-Vehicle Units can be used to track the whereabouts of cars at all times.[9]

8 When all such large datasets are collected and combined, big data reveals information about individuals that simply was not knowable in previous generations. It reveals who a person talks to, what is said, where he goes, where he works, who he works for, who his family members are, where he eats, what he eats, what he purchases and so on. It gives insight into likes and dislikes, hobbies, financial statuses, employment, and even criminal histories. Most activities involving electronic equipment can be traced and tracked. The metadata from mobile phones, for example, can reveal the location and time of a call, text message, or e-mail.[10] Location data can be then used to identify where a person sleeps, where he works, whether he is in fact working at the office as he claims or on the golf course, who he drinks beer with, what medical professionals he visits and what political or religious gatherings he attends. Since 2010, in addition to metadata, Apple iPhones have also been collecting data through Siri, the talking, question-answering application. Apple has been feeding it data since 2010, and now, with people supplying millions of questions each day,

---

6 Jules J Berman, *Principles of Big Data: Preparing, Sharing, and Analyzing Complex Information* (Morgan Kaufmann, 2013) at pp xv and xx.

7 Jules J Berman, *Principles of Big Data: Preparing, Sharing, and Analyzing Complex Information* (Morgan Kaufmann, 2013) at pp xv and xx.

8 World Economic Forum, *Big Data, Big Impact: New Possibilities for International Development* (2012) <http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf> (accessed 29 March 2015).

9 See Christopher Tan, "New ERP Could Track Vehicles at All Times" *The Straits Times* (25 March 2015) at p A6.

10 Dionne Searcey & Anne Marie Squeo, "More Phone Firms Fight Claims They Supplied Call Data to NSA" *Wall Street Journal* (17 May 2006) at p A3.

Siri has been learning and it is becoming an increasingly adept personal assistant, and even a "friend" for those who are autistic.[11]

9 The advances of facial recognition software and biometric identification technologies have made it even easier to collect information about individuals. Facial recognition software can identify a person by comparing the person's face to a database of stored faces.[12] As sources of photographs proliferate, especially on social networking sites such as Facebook, the utility and ease of the technology will expand more rapidly. Biometric identification technologies essentially utilise individuals' biological characteristics to identify them, so they rely on features such as irises, tattoos, scars, shape of people's ears and the gait they may have.[13] Like facial recognition software, once a scan is done, comparison is made with a database of stored biometric data.[14] Once a person is identified, other information about him can be added to give a fairly comprehensive profile of that person.

10 A recent invention that is a rising cause for privacy concerns is the domestic drone, or unmanned air vehicle. Hobbyists can purchase drones relatively easily as they are now widely available and affordable. Drones can fly at high altitudes, be fitted with high-power zoom lenses with recording facilities, and also have night vision.[15] Thus, drones have the capacity to fly outside the window of an apartment on the 26th floor looking in at unsuspecting residents in various states of undress.[16]

11 In short, big data can create a revealing profile of the person one is. Personal information is extremely valuable, and has become even more so in the era of big data.[17] This information can, of course, be used commercially by firms for strategic or marketing purposes. Indeed, companies like Facebook have, as their business model, the acquisition and sale of personal data. Some have bluntly asserted that Facebook's users are really Facebook's product because Facebook sells information

11 Judith Newman, "To Siri, With Love: How One Boy with Autism Became BFF with Apple's Siri" *New York Times* (17 October 2014).

12 Laura K Donohue, "Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age" (2012) 97 Minn L Rev 407 at 447–448.

13 "Types of Biometrics" Biometrics Institute website <http://www.biometricsinstitute.org/pages/types-of-biometrics.html> (accessed 29 March 2015).

14 Zach Howard, "Police to Begin iPhone Iris Scans Amid Privacy Concerns" *Reuters* (20 July 2011).

15 Canada, Office of the Privacy Commissioner of Canada, *Drones in Canada* (March 2013) at p 4 <https://www.priv.gc.ca/information/research-recherche/2013/drones_201303_e.pdf> (accessed 29 March 2015).

16 Erin Mizraki, "Seattle Police Investigate Possible Peep Drone outside Woman's Apartment" *ABC News* (24 June 2014).

17 Steve Lohr, "The Age of Big Data" *New York Times* (12 February 2012) at p SR1.

about its users to advertisers.[18] Further, with Facebook's acquisition of the instant messaging application company WhatsApp in 2014, Facebook can easily build almost perfect profiles of individuals without recourse to external sources of data.

12 A much greater risk of big data is when vast amounts of personal information fall into the hands of criminals. Unlike physical property, once personal information has been disseminated, it cannot be "recovered" or taken back. This in particular poses long-lasting privacy implications because some kinds of personal information cannot be changed, like one's height, date of birth or irises. Much damage can result from the criminal misuse of personal information, in terms of personal bodily harm, monetary loss, and even psychological harm. It is all these harms that are at the centre of privacy in the 21st century. Personal information and profiles can be used for impersonation, fraud and identity theft which are largely monetary harms. They can also be used to harm the physical, psychological and emotional well-being of individuals if the personal information is used to, for example, stalk a victim or to bully or harass a victim. In effect, having intimate and vast knowledge about an individual gives the perpetrator control and power over the victim as he knows the victim's every move and his every like and dislike.

II. In the beginning: The Warren and Brandeis conception of privacy

13 A precise definition of privacy is elusive as the concept encompasses various different meanings. The concept has been the subject of much academic discussion and writing since the influential article by Samuel D Warren and Louis D Brandeis was published in 1890.[19] The article was reportedly inspired by the rise of newspapers, photography and other technologies with the potential to publicise people's images and personal information, and, in particular, by the unwanted attention that Warren himself received from the Boston newspapers about his personal life.[20]

18 See Erin Bernstein & Theresa J Lee, "Where the Consumer Is the Commodity: The Difficulty with the Current Definition of Commercial Speech" (2013) Mich St L Rev 39 at 40 and Olivia Solon, "You Are Facebook's Product, Not Customer" *Wired* (21 September 2011) <http://www.wired.co.uk/news/archive/2011-09/21/doug-rushkoff-hello-etsy> (accessed 29 March 2015).

19 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193.

20 Neil M Richards, "The Puzzle of Brandeis, Privacy, and Speech" (2010) 63 Vand L Rev 1295.

14 The article noted that the common law had in the past found ways to protect individuals' person and property, even extending to the protection of reputation in the tort of defamation, so that with political, social and economic changes, common law can also be flexible enough to protect privacy interests as well.[21] Warren and Brandeis thus articulated the need for the common law to recognise and provide protection for individual privacy.[22]

15 They proceeded to call for the creation of a tort action for wrongs such as the circulation of unauthorised pictures of private persons.[23] The essence of privacy was to them "the right to be let alone",[24] a phrase coined by Judge Thomas Cooley in his famous treatise on torts.[25] Warren and Brandeis, however, also defined the tort variously as the right to "an inviolate personality",[26] the "immunity of the person",[27] the right to "one's personality",[28] "rights as against the world",[29] or "the privacy of a private life".[30] They explained that the general object was to:[31]

> … protect the privacy of private life, and to whatever degree and in whatever connection a man's life has ceased to be private, before the publication under consideration has been made, to that extent the protection is to be withdrawn.

16 Two important points should be noted about the right to privacy conceived by Warren and Brandeis. First, "the right to be let alone" placed a reliance on the public/private distinction which encompassed the distinction between private facts *versus* public facts as

21 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 213.
22 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 196.
23 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 195.
24 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 193, 195 and 205.
25 Thomas M Cooley, *A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract* (Callaghan, 2nd Ed, 1888) at p 29.
26 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 205.
27 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 207.
28 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 207.
29 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 213.
30 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 215.
31 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 215.

well as the scope of legitimate use of those facts. Their proposed tort would only protect facts "concern[ing] the private life, habits, acts, and relations of an individual"[32] but would not "prohibit any publication of matter which is of public or general interest".[33] Thus, their proposed tort would not prohibit the publication of information with a "legitimate connection" with the fitness of a candidate for public office or any actions taken in a public capacity.[34] Their summary position is that:[35]

> … [s]ome things all men alike are entitled to keep from popular curiosity, whether in public life or not, while others are only private because the persons concerned have not assumed a position which makes their doings legitimate matters of public investigation.

The public and private distinction is not as easily resolved as Warren and Brandeis seemed to believe. As some of the cases below show, courts have had to grapple with what would constitute a private fact. So, for example, would the fact that a celebrity was leaving a Narcotics Anonymous meeting be a private fact when it is in a public street?[36]

17 Secondly, the right to privacy proposed by Warren and Brandeis was a right that protected individuals from intrusion by other people or organisations, in particular the media. Their main concerns were indeed "recent inventions and business methods",[37] referring to the invention of instantaneous photography and newspaper enterprises. It is interesting to note, however, that when the US Supreme Court eventually took up the cause in its decisions, the right to privacy was treated as a protection against state or governmental intrusion – by 1965, the privacy threat in the US from the Government was perceived to be more insidious than from the private sector.[38] That, however, may be a US-centric approach as it is clear that the private sector has in the 21st century outpaced and out-resourced the public sector in privacy intrusions.[39]

---

32 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 216.

33 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 214.

34 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 216.

35 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 216.

36 *Campbell v MGN Ltd* [2004] UKHL 22 at [14].

37 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 195.

38 See *Griswold v Connecticut* 381 US 479 (1965).

39 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at pp 130–132.

III. Prosser's conception of privacy torts

18 The early conception of a privacy tort by Warren and Brandeis took shape some 70 years later in the US with the work of William Prosser[40] in 1960 when he encompassed the notion into four privacy torts. These four torts are still recognised in one form or another as law in the US today[41] and they are:

> (a) intrusion upon the plaintiff's seclusion or solitude, or into private affairs;
>
> (b) public disclosure of embarrassing private facts about the plaintiff;
>
> (c) publicity which places the plaintiff in a false light in the public eye; and
>
> (d) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[42]

19 Prosser himself noted that the:[43]

> … four distinct kinds of invasion of four different interests of the plaintiff … are tied together by a common name, but otherwise have nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone'.

These four torts may well provide the individual with some shreds of privacy protection but in reality, the last three of these torts are relatively narrow and have specific requirements or prerequisites that would not be helpful in protecting information privacy in the modern digital world of big data.

20 The tort of public disclosure of embarrassing private facts requires disclosure of facts that are private so this tort would not, for example, protect information about one's name, gender, and home address. In the tort of a false light in the public eye, a defendant needs to spread falsehoods about a plaintiff that would be considered objectionable by the average person. So if the information that is disseminated – for example, salacious information – is true, this category of the tort cannot be used. Lastly, the tort of appropriation occurs when a defendant uses a plaintiff's name, likeness, or image

40 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383.
41 American Law Institute, *Restatement (Second) of Torts* (American Law Institute Publishers, 1977) § 652A(2).
42 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 389.
43 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 389.

without the plaintiff's permission for "his own use or benefit",[44] usually for commercial benefit. Thus, if the defendant's use is not for his own use or benefit or if the appropriation is not commercial, but, for example, is intended to harass, then this tort is also of little use.

21 As for the tort of intrusion upon the plaintiff's seclusion or solitude, or into private affairs, this tort does have significance in the protection of the individual's personal information but like the other three, the relevance is limited. The US cases cited by Prosser were cases of physical intrusions such as intrusion into a home or a hotel room, as well as non-physical intrusions such as eavesdropping on private conversations by means of wiretapping and microphones and "peering into the windows of a home".[45] Prosser also cited a case in which a creditor "hounded the debtor for a considerable length of time with telephone calls at his home and his place of employment"[46] and another case of "unauthorized prying into the plaintiff's bank account".[47]

22 The accompanying commentary to § 652B of the US *Restatement (Second) of Torts*[48] ("Restatement") explains that the tort arises in three kinds of scenarios. First, the invasion may be by physical intrusion into a place in which the plaintiff has secluded himself. Secondly, the invasion may be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs. Thirdly, it may be by some other form of investigation or examination into his private concerns. The first scenario will have limited application because it will only apply where the individual has secluded himself, either in the home or some other setting. Still, there are questions of what constitutes seclusion. Would, for example, being inside a public toilet but not locked inside a cubicle be regarded as seclusion? As already mentioned, a lot of data obtained through big data analytics will be captured in all sorts of situations, whether or not the individual is secluded. The second scenario is equally limited as it requires the individual to be secluded in terms of being "sensed" by others. So, for example, can friends whispering in the corner of a café be considered to have secluded themselves? The last situation requires an invasion into the private affairs of another. Thus, if the intrusion is not into a matter of private affairs, such as the place of work, choice of books read or movies watched, this tort is of little assistance.

---

44 American Law Institute, *Restatement (Second) of Torts* (American Law Institute Publishers, 1977) § 652C.

45 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 390.

46 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 390.

47 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 390.

48 American Law Institute, *Restatement (Second) of Torts* (American Law Institute Publishers, 1977) Commentary on § 652B.

23 Furthermore, subsequent cases and § 652B of the US Restatement[49] have also prescribed the need for the invasion to be highly offensive to a reasonable person, which re-enforces the idea that the matter or situation invaded must be a private one, thereby limiting the scope of the tort. The accompanying commentary in the Restatement clarifies that it is irrelevant if there was any publicity given to the person whose interest is invaded or to his affairs. The tort is grounded in the intrusion itself.[50]

24 In the categorisation of privacy torts in the US, the first two of these torts emphasise the need for the matter or situation to be private or for the facts to be of a private nature. As seen above, in the digital age of big data, the threshold requirement of private matter or facts may be too low because of the ability for all kinds of data to be easily searched, found, matched, combined and subsequently used to cause harm. As for the remaining two torts, the tort of false light is only enlivened when there are falsehoods being disseminated, which borders more upon the tort of defamation. This presents too high a threshold for any meaningful protection of an individual's personal data. The tort of appropriation only applies if a person's name or likeness has been put to the defendant's own use or benefit, so again, this threshold would be too high because it will not catch practices such as harassment.

IV. Adoption of Prosser's conception of privacy in other jurisdictions

25 Despite the relatively early conceptions of privacy by Prosser in an age well before the advent of personal computers and digital technology, his categorisation of privacy torts has been the progenitor of conceptions of privacy in other jurisdictions in the 21st century.

26 In 2012, the New Zealand High Court recognised a tort of intrusion upon seclusion in the case of *C v Holland*,[51] where the defendant installed a recording device in a bathroom to record his female flatmate showering. In this case, Whata J referred to the Ontario Court of Appeal in *Jones v Tsige*,[52] which had earlier in the same year recognised a tort of intrusion into seclusion. Further, in September 2014, the Australian Law Reform Commission published *Serious*

49 American Law Institute, *Restatement (Second) of Torts* (American Law Institute Publishers, 1977) § 652B.

50 American Law Institute, *Restatement (Second) of Torts* (American Law Institute Publishers, 1977) Commentary on § 652B.

51 *C v Holland* [2012] 3 NZLR 672.

52 *Jones v Tsige* (2012) ONCA 32.

Invasions of Privacy in the Digital Era[53] recommending a tort of intrusion upon seclusion that is similar to the tort espoused in New Zealand by Whata J requiring intentional, or reckless, serious and unauthorised intrusion.

27 In the UK, the tort of intrusion upon seclusion is not so clearly recognised. The House of Lords refused to recognise a tort of invasion of privacy in *Wainwright v Home Office*[54] and consequently the case was taken to the European Court of Human Rights which found in *Wainwright v United Kingdom*[55] that Art 8 of the European Convention on Human Rights[56] ("ECHR") had been breached. Article 8 of the ECHR provides, in part, that "everyone has the right to respect for his private and family life, his home and his correspondence". In this case, the applicant had been required to remove all her clothes before she was allowed to enter into a prison to visit her son and this was held to be a breach of her Art 8 rights.

28 It was perhaps with the European Court of Human Rights decision in mind that Eady J stated in *CTB v News Group*[57] that it "is important always to remember that the modern law of privacy is not concerned solely with information or 'secrets': it is also concerned importantly with *intrusion*" [emphasis in original].[58] Similar sentiments were expressed by Tugendhat J in *Goodwin v News Group*.[59]

29 The other multi-jurisdictionally accepted privacy tort is the tort of disclosure of private information which stems from Prosser's tort of public disclosure of embarrassing private facts. The elements of the US tort as set out in § 652D of the Restatement are that publicity is given to a matter concerning the private life of another, and the matter publicised is of a kind that would be highly offensive to a reasonable person, and it is not of legitimate concern to the public. The commentary to the Restatement explains that publicity here:[60]

> … means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.

53 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Final Report* (ALRC Report 123) (September 2014).
54 *Wainwright v Home Office* [2004] 2 AC 406.
55 *Wainwright v United Kingdom* (2007) 44 EHRR 40.
56 European Convention for the Protection of Human Rights and Fundamental Freedoms (213 UNTS 221) (4 November 1950; entry into force 3 September 1953).
57 [2011] EWHC 1326.
58 *CTB v News Group* [2011] EWHC 1326 at [23].
59 *Goodwin v News Group* [2011] EWHC 1437 at [85].
60 American Law Institute, *Restatement (Second) of Torts* (American Institute of Law Publishers, 1977) Commentary on § 652D.

Hence, the communication must be one that reaches, or is sure to reach, the public, and not merely one other person, which suffices in the tort of defamation.

30 In the New Zealand case of *Hosking v Runting*,[61] the New Zealand Court of Appeal recognised the existence of a tort of wrongful publication of private facts. The two fundamental requirements of this tort are (a) the existence of facts in respect of which there is a reasonable expectation of privacy; and (b) publicity given to those facts that would be considered highly offensive to an objective reasonable person.[62] In *C v Holland*, Whata J noted that the intrusion tort was a "logical extension or adjunct"[63] to the tort of wrongful publication of private facts.

31 In the UK, the disclosure of private information has been a settled basis for action since the case of *Campbell v MGN Ltd*.[64] The cause of action confirmed in that case developed out of the equitable cause of action for breach of confidence. Disputes concerning violations of privacy had typically been brought under the cause of action for breach of confidence, and this had led to two general lines of authority, those cases concerning confidential or secret information and those concerning privacy.

32 In *Campbell v MGN Ltd*, Naomi Campbell, an actress, claimed that Mirror Group Newspapers had breached the duty of confidence because they published photographs of her leaving a Narcotics Anonymous meeting. The House of Lords stated that the cause of action for breach of confidence "has now firmly shaken off the limiting constraint of the need for an initial confidential relationship" and that in doing so "it has now changed its nature".[65] Lord Nicholls of Birkenhead stated that:[66]

> Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information.

61 [2005] 1 NZLR 1.
62 *Hosking v Runting* [2005] 1 NZLR 1 at [117].
63 *C v Holland* [2012] 3 NZLR 672 at [86].
64 [2004] UKHL 22.
65 *Campbell v MGN Ltd* [2004] UKHL 22 at [14].
66 *Campbell v MGN Ltd* [2004] UKHL 22 at [14].

With this, the tort of misuse of private information was born and tortious damages are now available whereas previously under actions for breach of confidence, damages (being an equitable remedy) were at the discretion of the judge. The tort was also no longer limited to disclosure but encompassed any kind of misuse. This has been confirmed in both the High Court[67] and Court of Appeal[68] decisions in *Judith Vidal-Hall v Google Inc*. This recent development in the UK could be connected to the English Human Rights Act 1998,[69] which incorporates elements of the ECHR.[70] Admittedly, Art 8 is not confined to private information, but the right of "respect" referred to in Art 8 would certainly encompass not just non-disclosure but also any other kind of misuse.

33 The Australian Law Reform Commission, in September 2014,[71] also recommended the introduction of a tort of misuse of private information.

V. Other privacy taxonomies

34 Whilst the work of Prosser has been expanded upon by courts and law reform bodies in various jurisdictions, some legal scholars have also lent their weight to the discourse. These taxonomies, however, do not actually add anything new to the discourse, especially when they are compared with the Data Protection Directive. As will be elucidated in the next part,[72] the Data Protection Directive had already set out the major harms and laid down a comprehensive framework that would protect privacy covering all the scenarios that courts and commentators have been dealing with over the past century. This part will consider the two main taxonomies cited by the Australian Law Reform Commission in its September 2014 report[73] because they represent the current scholarship. One of these[74] is more commonly accepted in Commonwealth jurisdictions and has been relied upon by some of the courts. However, the first represents the more recent discourse in the US. The following part will make a comparison of these taxonomies with the Data Protection Directive.

67 *Judith Vidal-Hall v Google Inc* [2014] EWHC 13.
68 *Google Inc v Judith Vidal-Hall* [2015] EWCA Civ 311.
69 c 42.
70 See also *Google Inc v Judith Vidal-Hall* [2015] EWCA Civ 311 at [18].
71 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123) (September 2014) ch 5.
72 See paras 46–71 below.
73 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123) (September 2014) ch 5.
74 The second to be considered at paras 40–45 below.

A. Solove's taxonomy

35 An extensive taxonomy of privacy was presented by US scholar Daniel Solove[75] in 2006 and was cited by the Australian Law Reform Commission in 2014.[76] Solove noted that Prosser focused only on tort law.[77] Privacy law according to Solove is "significantly more vast and complex, extending beyond torts".[78] Solove's analysis returned to the original Warren and Brandeis article as he focused on the harms to individuals and the activities that create problems.[79]

36 Solove noted that the harm Warren and Brandeis referred to was an incorporeal injury rather than a physical injury, which is easy to understand and to compensate for. Warren and Brandeis noted that the law in the 1890s was beginning to recognise nonphysical harms and that:[80]

> … modern enterprise and invention have, through invasions upon his privacy, subjected [the individual] to mental pain and distress, far greater than could be inflicted by mere bodily injury.

They felt privacy concerned "injury to the feelings".[81]

37 Solove opined that the harms Warren and Brandeis spoke of are dignitary harms, of which reputational injury is the classic example and to which defamation law has already responded.[82] Solove's view is that there are other kinds of dignitary harm beyond reputational injury, these being the harms of incivility, lack of respect and causing emotional angst.[83] In addition to these dignitary harms, Solove also put forth what he calls "architectural" problems and these involve the creation of or enhancement of the risk that a person might be harmed in the future.[84] To illustrate, Solove explained that activities involving a person's information "might create a greater risk of that person being victimized by identity theft or fraud" which increase the chances of dignitary, monetary or physical harms.[85] As will be seen below,[86] the creation of or

75 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477.
76 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123) (September 2014) at p 75.
77 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 483.
78 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 483.
79 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 485.
80 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 196.
81 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193 at 197.
82 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 487.
83 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 487.
84 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 487–488.
85 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 488.
86 At paras 46–51 below.

enhancement of risk was one of the very evils that the European Commission sought to address when it began to draft the *Data Protection Directive*.[87] What Solove suggested was not new.

38 Solove set out four basic groups of harmful activities, each of which "consists of different related subgroups of harmful activities".[88] These are:

> (a) information collection which would include surveillance and interrogation;
>
> (b) information processing activities such as aggregation, identification, secondary use, carelessness in protecting stored information from leaks and improper access, and failure to allow the individual to know about the data that others have about the individual and to participate in its handling and use;
>
> (c) information dissemination, meaning activities that involve the spreading or transfer of personal data or the threat to do so. This would include breach of confidentiality, disclosure, increased accessibility, blackmail, appropriation and dissemination of false or misleading information about individuals; and
>
> (d) invasion which would encompass intrusion upon seclusion and decisional interference, which is a largely US legal construct that resulted from the 1965 US Supreme Court case of *Griswold v Connecticut*[89] that concerns the Government's incursion into individuals' decisions regarding their private affairs.

While these four groups are fairly thorough in scope, the first three groups are taken extensively from the Data Protection Directive and its foundation principles. The first three groups of activities and examples thereof that Solove outlined are the exact same three categories of activities that the Data Protection Directive sought to curb and regulate, namely, collection, processing defined in the widest manner and form, and disclosure or dissemination.

39 Furthermore, the level of protection sought in the Data Protection Directive is extremely comprehensive and strict, much more so than Solove's taxonomy. In fact, the Data Protection Directive sets the bar so high that many jurisdictions around the world, in attempting to

87 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at pp 137–154.

88 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 489.

89 381 US 479 (1965).

meet the "adequacy" requirement in Art 25 of the Directive for the purpose of enabling cross-border transfer of personal data from the EU, were unable to meet the stringent privacy protection standard of the Directive. As for the last category that Solove outlined, intrusion upon seclusion, the jurisprudence and discourse have been plentiful since Prosser's original formulation in 1960 and as will be seen below,[90] this was also envisaged in the drafting of the Data Protection Directive.

B. The commonly accepted taxonomy

40 On the other side of the Atlantic, and in some of the other major Commonwealth jurisdictions, the development of a theory or tort of privacy has been slower. Unsurprisingly, many commentators have classified privacy more or less along the lines of the two Prosser privacy torts that the Commonwealth jurisdictions discussed above[91] have recognised or are proposing to recognise.[92] One of the most recent works in the area is that by Nicole Moreham and it will be used as the anchor for discussion. Moreham's work was also cited by the Australian Law Reform Commission.[93]

41 Moreham begins her analysis of the theoretical conceptions of physical privacy in much the same way as Solove, by listing the many and varied examples of what is or could be understood as common intrusions into privacy.[94] She then notes that although:[95]

> … each of X's privacy breaches is effected differently, they all prevent the subject from choosing, on his or her own terms, the extent to which he or she is accessed by others.

90 At paras 46–71 below.

91 At paras 25–33 above.

92 See, for example, Ruth Gavison, "Privacy and the Limits of the Law" (1979) 89 Yale LJ 421; Judith Wagner DeCew, "The Scope of Privacy in Law and Ethics" (1986) 5 Law & Phil 145; Rachael Mulheron, "A Potential Framework for Privacy? A Reply to Hello!" (2006) 69 MLR 679; Chris Hunt, "Conceptualizing Privacy and Elucidating Its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011) 37 Queen's LJ 167; and Kirsty Hughes, "A Behavioural Understanding of Privacy and Its Implications for Privacy Law" (2012) 75 MLR 806.

93 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123) (September 2014) at p 76.

94 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 352.

95 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 352.

Furthermore, all of them "also lead to feelings of affront, violation and indignity".[96]

42 Moreham notes that the examples listed reveal two types of overlapping but distinct privacy interference: the misuse of private information ("informational privacy") and unwanted sensory access ("physical privacy").[97] She also acknowledged that many scholars also divide the concept along similar lines.[98] The informational privacy examples involve first discovering something about a person; secondly, the retention of private records or information about the person; and third, disclosure of private information about the person such as passing on gossip or uploading information onto the Internet.[99] These three activities are along the same lines as Solove's first three sets of harmful activities.

43 The second category of physical privacy concerns unwanted access to the physical self. Moreham states that:[100]

> The interference in these cases is *sensory*: the intruder interferes with your physical privacy by watching, listening to or otherwise sensing you against your wishes. It is this aspect of the interest which is at stake when X spies on Y in the shower, hacks Y's telephone calls, or videos Y in his or her bedroom. [emphasis in original]

According to Moreham, in these situations:[101]

> … the concern is primarily physical: the observer is, through the use of the senses, physically experiencing something of you against your wishes and/or allowing others to do the same.

44 Moreham admits that there is overlap between the two categories. So a person who installs a camera in a tenant's bathroom will find out what the tenant does there as well as see the tenant naked. However, her view is that both these components of the privacy interest,

96 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 352.
97 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 353.
98 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 353.
99 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 354.
100 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 354.
101 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 355.

physical and informational, need to be recognised if privacy is to be comprehensively protected.[102] She continues:[103]

> This is because it is possible to commit a serious breach of privacy without obtaining any meaningful information. Little 'information' is obtained, for example, when a person is spied on in the shower, watched in a toilet … even if some meaningful information is obtained, it is unlikely to be the sole reason for the subject's objection.

45 Moreham then agrees with Raymond Wacks where he said:[104]

> What is essentially in issue in cases of intrusion is the frustration of the legitimate expectations of the individual that he should not be seen or heard in circumstances where he has not consented to or is unaware of such surveillance. The quality of the information thereby obtained, though it will often be of an intimate nature, is not the major objection.

Moreover, as will be seen below,[105] the two categories suggested by Moreham are, in essence, covered by the Data Protection Directive. The first category of informational privacy and the three ways in which it can be compromised are, as already mentioned with respect to Solove's taxonomy, the exact same three types of activity that the Directive sought to restrict. The second category of physical privacy, as will be seen below,[106] is also in essence encompassed by the Directive.

VI. The Data Protection Directive

A. The context of the Data Protection Directive

46 Not long after the personal computer became a mass market technology, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[107] ("Convention") was adopted in 1981 and all the EU members were

102 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 355.

103 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 355.

104 Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989) at p 248, referred to in Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 355.

105 At paras 52–71 below.

106 At paras 52–71 below.

107 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Eur TS No 108) (28 January 1981; entry into force 1 October 1985).

signatories.[108] This Convention required the signatories to protect the privacy rights of individuals in circumstances where information about them was to be processed automatically. There was also a further desire that there be the facilitation of a common international standard for the protection of individuals' privacy so that the free flow of information could proceed without impediment.[109] Indeed, one of the items in the Preamble to the Convention stated the necessity "to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples".[110]

47 The object of the Convention was to strengthen data protection, which focused on the legal protection of individuals with regard to automatic processing of personal information relating to them. At that time, it was already perceived that there was a need for such legal protection in light of the increasing use of computers for administrative purposes. It was not difficult to see that automated files, when compared with manual files, have a vastly superior storage capability and offer possibilities for a much larger variety of transactions, all of which can be performed at high speed. It was also foreseeable back then that there would be further growth of automatic data processing in the administrative field.

48 Another goal of the Convention was to provide a level playing field within the EU to ensure all member states afforded the same level of protection. However, with the many different cultures, legal systems and priorities in the various EU member states, the road to achieving this outcome was not easy. Some countries such as Germany and France saw significant human rights issues. Others, such as the UK, were concerned primarily with ensuring that minimum standards were met. As a result, there were many and varied data protection laws among the signatory countries, the exact opposite of the original intention.[111]

49 By 1990, it became clear that the inconsistency was a serious impediment to attaining a common market, exacerbated by the increased use of information technology within the EU. It was feared that countries with strict privacy laws would restrict the movement of

108 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at p 137.

109 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at pp 137–138. See further the Preamble to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Eur TS No 108) (28 January 1981; entry into force 1 October 1985).

110 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Eur TS No 108) (28 January 1981; entry into force 1 October 1985) Preamble.

111 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at p 138.

information into those whose laws were less so, or that companies would relocate to countries within the EU with the more lax laws. It was these fears that gave rise to the Data Protection Directive. The main purpose of the Data Protection Directive was to harmonise the level of protection given to personal data within all member states. It was also in part designed to prevent the erection of trade barriers based on the protection of personal privacy.[112]

50 The first draft of the Data Protection Directive was presented in 1990 but it took several more drafts before consensus was reached in 1995.[113] Some member states were not willing to reduce the level of protection whilst other member states maintained that no directive was required.[114] Importantly, the final draft adopted applies where data is processed, whether or not by automatic means.[115] This ensures that the directive applies regardless of whether technology or equipment is used, and whether the information is in electronic form. It applies to written, Internet, and even oral communications.

51 The Data Protection Directive is a framework legislation in that it requires each EU member state to enact its own domestic laws adopting or transposing the Directive's articles. The text of the Directive therefore offers a blueprint for data privacy laws across Europe. Whilst it is true that given any specific privacy issue that arises within Europe, the statute of the relevant country that adopts or enacts the Directive will determine data privacy rights and responsibilities, the purpose of examining the Directive here is to elucidate its key features. In doing so, the parallels between common law privacy and the protection afforded by the Directive will become clear. Furthermore, it will be seen that the level and scope of the protection under the Directive is far more comprehensive and superior than the protection given by current privacy torts at common law in many jurisdictions and proposals by law reform commissions and scholars. In fact, much of the privacy discourse at common law is replicating what is already protected under the Directive.

112 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at p 138.

113 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at p 138.

114 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at p 138.

115 Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data) Art 2(b).

B. The provisions of the Data Protection Directive

52 The Data Protection Directive requires each member state to enact general data protection laws that cover both government and private entities. This is vastly different from the divergence model in the US[116] where sectoral privacy laws apply to distinct categories of data such as medical records and credit records.[117] It is perhaps for this reason that much of the jurisprudence and much of the tort law on privacy in the US did not make connection with data protection law until only very recently.[118]

53 The Data Protection Directive can be said to have grown out of a foundation that was economic but it evolved into a human rights construct. One of the main objectives of the Directive set out in Art 1(1) is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of data". A number of the EU member states have long viewed personal data as something that belonged to the individual, like property. It is unsurprising then that the Directive imposes tight restrictions on what kinds of activity are permissible with respect to personal information. In line with this, in 2014, the Court of Justice of the EU ruled that a person has a right to be "forgotten" on the Internet under the Directive.[119] It is not the purpose of this part to give a comprehensive analysis of the Directive; instead, its key features will be highlighted to show its connections with common law privacy and hopefully to shape the common law's future direction.

54 The Data Protection Directive applies to all kinds of "processing" which is very widely defined, as will be seen below.[120] Importantly, Art 7(a) stipulates that personal data may be "processed" only if the data subject has unambiguously given his consent. Implied consent is insufficient, which means any breach of the Art 7(a) requirement of explicit consent would catch all cases ever envisaged of common law privacy intrusion, for if a person has given explicit consent, then there can be no complaint of any invasion of privacy. The other situations set out in Art 7 where personal data may be processed are when the processing is necessary: for the performance of a contract

116 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at pp 136–137.

117 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at pp 154–156.

118 Yee Fen Lim, *Cyberspace Law: Commentaries and Materials* (Oxford University Press, 2002) at pp 154–156.

119 *Google Spain SL v Agencia Española de Protección de Datos* Case C-131/12 (13 May 2014).

120 At para 57 below.

to which the data subject is party; for compliance with a legal obligation; in order to protect the vital interests of the data subject; to perform a task carried out in the public interest or to facilitate the exercise of official authority; or to further the legitimate interests pursued by a party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection under Art 1(1).

55 It should be stressed that except for explicit consent, all the other situations that fall under Art 7 mandate the element of necessity. Therefore, in Europe, processing ordinary personal data is presumed illegal, unless the processing has been explicitly consented to or is "necessary" for any of the listed limited purposes. These together, if complied with, would ensure robust protection for an individual's privacy. It is true that in the cases that come under "necessity", the individual concerned may not even be aware of the processing. However, the situations of necessity listed are self-limiting; they are also for legitimate purposes and some are for the benefit of the individual. The head of necessary for the performance of a task carried out in the public interest may appear to be rather broad; it is, however, a head that would not be upheld lightly given the overall tenet of the Directive to protect fundamental rights, so there must be a genuine convincing public interest and the processing must be necessary for the performance of the task.

56 To appreciate the full meaning of the general prohibition, the definitions will now be discussed. The definitions contained in the Data Protection Directive are crucial to understanding the breadth and depth of coverage. Article 2(a) defines "personal data" to mean "any information relating to an identified or identifiable natural person" who is known as the data subject. An identifiable natural person is a person who:

> … can be identified, directly or indirectly, in particular by reference to an identification number or by one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

With this very broad definition, personal data encompasses many things. A person's face is personal data, as is a photo of a person's face, an employee number, and even a birthmark. A mobile phone number or a car number plate can also identify a person so they too are personal data. A person's voice is also personal data, as are medical records, diaries and many other things. Because the definition includes "one or more factors", this is where anonymisation of personal data may not always render an individual unidentifiable because it is often still

possible to ascertain a person's identity where there is a set of facts about the individual.[121]

57 Article 2(b) defines "processing of personal data" equally broadly and it extends well beyond the common understanding of the notion of processing. "Processing of personal data" means:

> … any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction …

This extremely comprehensive list of what is considered to be "processing" in effect places the *doing of anything* with personal data as coming within the purview of the Data Protection Directive. It includes the first three groups of harmful activities outlined by Solove, namely collection, processing (which would come under "use" here), and dissemination and many more activities. The explicit inclusion of "storage" in the definition of "processing" makes the mere *act of holding personal data* a regulated activity under EU law. This in fact was one of the original rationales behind the Directive. Those nations in Europe under fascist governments during and after World War II were acutely aware of the occurrences of the secret police misusing personal information in classified files for nefarious purposes, including whom to send off to concentration camps. This legacy in these countries has instilled a healthy scepticism of anyone amassing data banks with personal information that can be used for yet unknown purposes. As a result, during the drafting process of the Directive, countries such as Germany were insistent that the level of protection not be lowered.[122]

58 Solove's fourth group of harmful activities, that of invasion or intrusion upon seclusion, would also be caught by this expansive definition of "processing". The reason for this is that "processing" is not limited to the electronic realm ("whether or not by automatic means") and an intrusion upon seclusion would certainly be collecting personal data of some sort, even if the collection is in one's head to be possibly later recorded, revealed or otherwise used in some way. For example, observing someone in the shower would certainly be collecting

121 Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques* (0829/14/EN) (10 April 2014).

122 This fear of nefarious purposes and activities is also the reason for the presence of Arts 25 and 26 of the Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data) restricting the transfer of personal data to countries outside the European Union.

information about the data subject, whether it is his physical attributes or how long he takes to shower, what soap he uses and so on. Since the spying is on a human being who is clearly identifiable, there is no doubt that it is personal data. This mere collection and holding of information would be regarded as "processing" under the Data Protection Directive unless it is excepted in the statutes of individual EU member states.

59 One objection to the above analysis is that in effect, every human being is collecting personal data as they go about their daily business. Is this true? Yes and no. Yes in the sense that one is always constantly seeing and observing but no in the sense that many a time, one forgets what he has seen because it is not his intention to be collecting and storing it in his memories. In the case of a purposeful spying of someone in the shower, it can be said that there is a clear intention to observe; hence, there is a clear inference that what was observed will be retained and remembered.

60 Similarly, when one considers the two broad categories put forth by Moreham, that is, the misuse of private information (informational privacy) and unwanted sensory access (physical privacy), both of these are also activities caught by the "processing" definition in Art 2(b). What Moreham meant by informational privacy is clearly covered by the "processing" of personal data because she had in mind the discovery ("collection"), retention ("storage") and disclosure ("dissemination") of private records or information about the person. If anything, Moreham's formulation is narrower as she is only concerned with private record or information about a person whereas the Data Protection Directive catches any "personal data" which is any information from which a person can be identified, directly or indirectly, by one or more factors. As previously mentioned, this can be a photo of a person's face or an employee number which would not normally be considered as private information about a person.

61 Moreham's second category of physical privacy is very similar to Solove's fourth group of harmful activities, that of invasion. Moreham stated that the interference in these cases is sensory, through watching, listening to or otherwise sensing a person against his or her wishes. The primary means of interference through sensing would be watching through the eyes or the listening through the ears. It would seem difficult to interfere with a person's privacy through smelling. As for the two remaining senses, if there is any touching or tasting of another person, these would already be actionable under other torts. Watching or listening to a person under the Moreham formulation would both constitute "processing" under the Directive as personal data is collected. Eyes can see many things that can identify a person directly or indirectly. As for listening to a person, apart from the content of the

communication which can contain personal data, the voice of a person is personal data which can be used to identify an individual.

62 The broad definitions of "personal data" and "processing", coupled with the general prohibition on the processing of personal data unless explicit consent is given, means that almost every collection, every use, every secondary or further use, every combination and every disclosure of personal data requires the explicit consent of the individual. In fact, the Data Protection Directive would render most if not all of the activities discussed by Solove and Moreham illegal. Certainly, acts such as those carried out in *C v Holland*[123] and *Jones v Tsige*,[124] where Tsige, a bank employee, had used her work computer to access Jones' banking information almost 200 times over a period of four years, would fall foul of the Directive. Similarly, in *CTB v News Group*,[125] an injunction case brought by a footballer to prevent publication of the fact of, and details about, his extramarital affair with a lingerie model would come under the protective umbrella of the Directive, there being no public interest that could be advanced with the dissemination of his name.

63 Similarly, the facts of the New Zealand case of *Hosking v Runting* and the UK case of *Campbell v MGN Ltd* would also fall under the Data Protection Directive as they involve the disclosure or dissemination of personal data that was not consented to nor necessary under any of the permitted situations where personal data may be processed listed in Art 7, as already discussed above.[126]

64 If the protection granted under the Data Protection Directive is compared with Prosser's conception of privacy,[127] as already discussed,[128] it would cover intrusion upon the plaintiff's seclusion or solitude as well as the public disclosure of embarrassing private facts about the plaintiff. Prosser's third kind of invasion, publicity which places the plaintiff in a false light in the public eye, would also be caught by the Directive. Publicity is the disclosure element of processing and there is obviously personal data involved if the plaintiff is identified. As long as the individual is identified, it is personal data and it is immaterial if the contents are true or false.

65 Regarding Prosser's fourth class of privacy invasion, that of appropriation for the defendant's advantage of the plaintiff's name or

123 [2012] 3 NZLR 672.
124 (2012) ONCA 32.
125 [2011] EWHC 1326.
126 At paras 54–57 above.
127 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 389.
128 At paras 18–24 above.

likeness,[129] this too comes within the ambit of the Data Protection Directive. The mere fact that there is appropriation, meaning some kind of "use" which is "processing", and that the appropriation is of a person's name or likeness, which would undeniably constitute personal data.

66 The Data Protection Directive also contains extensive provisions on ensuring only adequate, relevant and accurate personal data is held, safeguarding the security of whatever personal data is held as well as destruction of personal data when no longer needed. These are far more comprehensive and give a stronger cloak of protection than what Solove or Moreham proposed.

C. Exceptions

67 In the actual implementation of the Data Protection Directive, Art 8(2) gives member states some leeway to grant certain exceptions, such as for national security, defence, criminal investigations and the like. Article 9 allows member states to carve out limited exceptions for "journalistic purposes" and "artistic or literary expression" purposes but only to the extent "necessary" to reconcile the right of privacy with "the rules governing freedom of expression". Some countries such as Germany[130] have continued to adhere to the strict standard as set out in the Data Protection Directive, while other countries such as the UK have allowed some exemptions, for example, if the processing was for domestic purposes only.[131]

D. The Data Protection Directive taxonomy

68 Moreham admitted that there is overlap between the two categories of informational privacy and physical privacy. She distinguished the two categories by saying that "it is possible to commit a serious breach of privacy without obtaining any meaningful information" and explained that little information is obtained when a person is spied on in the shower or watched in a toilet.[132] This, in her view, would be an example of why physical privacy is needed because no meaningful information was obtained which would have placed it under the category of informational privacy.

129 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 389.

130 Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Federal Data Protection Act) (BGBl I 1990 S 2954).

131 Data Protection Act 1998 (c 29) (UK) s 36.

132 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 355.

69 It appears that Moreham distinguished the two categories by whether or not "meaningful" information was or can be obtained. Furthermore, Moreham regarded her two categories as two overlapping but distinct sets.[133] Both of these lines of thought are not helpful in the big data age.

70 First, as already expounded, any single piece of personal data can become meaningful, especially when combined with other personal data. It was with the foresight of the European Commission in the 1980s that both the Convention and the Data Protection Directive were aimed at reducing or preventing the risk of harm arising in the future, for example, when the information is stored, combined, disclosed or otherwise used, the very same risks that Solove referred to.[134] Thus, it should be emphasised that the very object of the Directive is to protect even the most mundane and seemingly meaningless personal data.

71 Secondly, following from the vigorous protection of all personal data, if one were to classify how the Data Protection Directive structures the protection of personal data, it would group all personal data, whether meaningful or not, into one large set that needs to be protected and not two distinct overlapping sets. Within this one large set, the Directive has carved out a smaller subset of "special categories of data" in Art 8(1) which prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life unless an express exception applies. Some very narrow exceptions are set out in Art 8(2). The choices of some of the categories in Art 8(1) were no doubt influenced by the events of World War II. However, regardless of the motivations, this taxonomy is far more cognisant of the inherent dangers of collecting and combining personal data and provides extensive protection for the individual, not just in the protection of their feelings, reputation or dignity but also in the protection of their assets, their emotional well-being and even their lives. This taxonomy would form a sound basis for a statutory tort of privacy and it is this taxonomy that is to be preferred for protecting privacy in the 21st century of big data.

VII. Singapore

72 Singapore has not yet recognised a common law tort of privacy although the Protection from Harassment Act[135] does give some

133 Nicole Moreham, "Beyond Information: The Protection of Physical Privacy in English Law" (2014) 73(2) Camb LJ 350 at 353.

134 Daniel Solove, "A Taxonomy of Privacy" (2006) 154 U Penn L Rev 477 at 487–488.

135 Cap 256A, 2015 Rev Ed.

protection for a victim who is stalked or harassed.[136] However, Singapore does have data protection legislation in the form of a light touch regime. Its Personal Data Protection Act[137] ("PDPA") was not modelled on the Data Protection Directive but it does possess some similarities to its EU counterpart. The major difficulty with the Singapore model lies in the extensive exceptions that dilute many of the positive rights given, in particular, under the s 17 exemptions.

73 The PDPA applies to all "organisations",[138] which is defined broadly in s 2 to encompass individuals, corporations and unincorporated associations. In essence, the PDPA applies to all non-government organisations as well as individuals acting in non-domestic and non-personal capacities such as sole traders.

74 The PDPA does not apply to the public sector because it has its own internal data protection rules. However, the lack of transparency in these rules has been a cause for alarm most recently when a school accidentally sent out the personal data of 1,900 primary school-aged students.[139] Whilst an apology was made, the fact remains that the names and birth certificate numbers of the pupils; and the names, phone numbers and e-mail addresses of their parents are now publicly available. Furthermore, it should be noted that in Singapore, the birth certificate numbers become their National Registration Identity Card ("NRIC") numbers when the children reach 15 years of age. The NRIC number is the universal common identifier for citizens of Singapore and is thus a number of especial importance.

75 Personal data is defined in s 2 of the PDPA to mean data, whether true or false, or any combination of data from which an individual can be identified. The form in which the data is stored is unimportant as the PDPA covers both personal data in electronic and non-electronic forms. This definition is in line with the Data Protection Directive.

76 The PDPA, however, excludes from the operation of the new data protection regime data that is business contact information.[140] "Business contact information" is defined to mean an individual's name, position or title, business telephone number, business address, business

136 See further Goh Yihan & Yip Man, "The Protection from Harassment Act 2014 – Legislative Comment" (2014) 26 SAcLJ 700 and Goh Yihan, "The Case for Legislating Harassment in Singapore" (2014) 26 SAcLJ 68.

137 Act 26 of 2012.

138 Personal Data Protection Act 2012 (Act 26 of 2012) s 4.

139 Irene Tham, "1900 Pupils' Personal Data Leaked by Accident" *The Straits Times* (24 March 2015) at p A1.

140 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(5).

e-mail address or business fax number, and any other similar information about the individual not provided by the individual solely for his or her personal purposes.[141] This exclusion from the operation of the whole data protection regime leaves an enormous gap in the protection of personal data. It also gives the mandate for the creation of databases of individuals' names and their jobs. These databases would form the basic foundation block on which to build a complete profile by adding other kinds of personal data.

77 The key activities regulated by the PDPA are collection, use and disclosure of personal data[142] but unlike the Data Protection Directive, none of these words are defined which leaves them open to interpretation by the courts.

78 There are nine key principles outlined in the PDPA, the first of which is the requirement of notification as to the purpose for the collection, use and disclosure before the actual collection, use or disclosure of personal data.[143] This principle would substantially assist an individual to have some control over their personal data but unfortunately, there are two major exceptions contained in s 20(3) of the PDPA: first, where consent is deemed under s 15;[144] and second, in all the situations listed in the three Schedules referred to in s 17.[145] As will be seen below under the consent principle, the sweeping exceptions granted in the three Schedules mean that this requirement of notification has limited utility because there are many situations where the data subject need not be notified of the collection, use or disclosure of their personal data.

79 Like the Data Protection Directive, consent is also a core principle of the PDPA and the general rule is that consent is required before personal data can be collected, used or disclosed.[146] There is no definition of "consent" in the PDPA, although s 14 provides that, subject to the two exceptions under s 20(3) mentioned earlier, consent that is obtained without first notifying the individual of the purpose(s) is not valid consent;[147] nor is consent valid if false, misleading or deceptive practices have been utilised.[148]

141 Personal Data Protection Act 2012 (Act 26 of 2012) s 2.
142 Personal Data Protection Act 2012 (Act 26 of 2012) s 3.
143 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(1).
144 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(3)(*a*).
145 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(3)(*b*).
146 Personal Data Protection Act 2012 (Act 26 of 2012) s 13(*a*).
147 Personal Data Protection Act 2012 (Act 26 of 2012) s 14(1)(*a*).
148 Personal Data Protection Act 2012 (Act 26 of 2012) s 14(2)(*b*).

80 It is, however, the nature of consent required under the PDPA that is questionable. The Data Protection Directive demands explicit consent, but under the PDPA, consent can even be deemed. Section 15 of the PDPA sets out the meaning of deemed consent, which was intended to minimise the impact of the new data protection regime on organisations in the everyday process of personal data collection. Consent is deemed if an individual, without actually giving consent, voluntarily provides the personal data to the organisation for that purpose, and it is reasonable that the individual would voluntarily provide the data.

81 The problematic issue with deemed consent is how much consent can be deemed; the boundaries of what purposes can be deemed to have been consented to are vague. An example to illustrate this might be found in the booking of a taxi over the phone. Instead of the taxi call centre staff having to enquire explicitly whether one consents to the collection and use of certain information, the consent can be deemed. The call centre can legitimately assume consent for the collection and use of information such as the customer's name to identify him, the customer's phone number in case of a delay in the taxi arriving, and the customer's address for pickup.

82 The question is, does this one transaction also deem consent for the call centre to retain all the information, so that in the name of efficiency, the next time the customer calls for a taxi, all the customer needs to provide is his phone number and the pickup address can be quickly retrieved from the computer, thereby saving time? This would appear to be the current practice and interpretation of the law. If efficiency can be used to deem consent, what are the limits? Could a pizza shop along the same line of argument retain a customer's name, type of pizzas ordered, phone number, address and even credit card number too? If they can, then another company offering some other service or product could do the same and before too long, big data will have produced a combined and thorough profile of the individual, including where he works, what time he goes to work, what pizzas he likes and even his credit card number.

83 All this information might seem innocuous but it can be used to perpetrate crimes. A stalker will be able to discover the victim's home and work addresses to stalk him and the stalker will know roughly at what times to stalk the victim. Worse still, the stalker might even be a rapist or kidnapper. Knowing what kinds of books, videos or pizzas a person likes can be used to taunt, ridicule, embarrass or harass the victim, either online or in the real space. In short, big data is an invader of a person's privacy, and if not properly regulated, can facilitate criminal behaviour.

84 The PDPA allows for consent to be withdrawn, even where it has been deemed.[149] There are a number of exceptions to the withdrawal of consent, such as if the collection, use or disclosure is required by law,[150] or if it is necessary for legal or business purposes.[151] Once a withdrawal of consent has been received by an organisation, it must cease and ensure its data intermediaries and agents also cease collecting, using or disclosing the personal data, as the case may be.[152] However, there are no requirements for the organisation to inform third parties of the withdrawal of consent, meaning that the onus lies on the individual to seek out the other organisations to withdraw consent. This can be in reality an impossible task because one never knows to whom the organisation has disclosed one's personal data as there are so many instances under the Fourth Sched where disclosure is permitted without consent.

85 Section 17(1) of the PDPA provides that personal data can be collected without consent in the circumstances set out in the Second Sched. Sections 17(2) and 17(3) similarly provide that personal data can be used and disclosed without consent in the circumstances set out in the Third and Fourth Scheds respectively. An example of the wide nature of the exemption is where it is necessary for "evaluative purposes".[153] "Evaluative purposes" is defined widely in s 2 to mean for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates in a large variety of situations. Some of these situations include employment or appointment to office; promotion or removal from employment or office; admission to an educational institution; and the awarding or continuation of contracts, awards, bursaries, scholarships, honours or other similar benefits. Just in the employment setting alone, employers are permitted to collect and build a comprehensive profile of their potential employees before hiring and of their employees during the course of employment.[154]

149 Personal Data Protection Act 2012 (Act 26 of 2012) s 16(1).
150 Personal Data Protection Act 2012 (Act 26 of 2012) s 16(4).
151 Personal Data Protection Act 2012 (Act 26 of 2012) s 25(*b*).
152 Personal Data Protection Act 2012 (Act 26 of 2012) s 16(4).
153 Personal Data Protection Act 2012 (Act 26 of 2012) Second Sched, para 1(*f*) (for collection), Third Sched, para 1(*f*) (for use), and Fourth Sched, para 1(*h*) (for disclosure).
154 Hannah Lim Yee Fen, "Data Protection in the Employment Setting" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2014).

86 Another wide exemption contained in these three Schedules is where the personal data is publicly available.[155] The exemption for personal data that is publicly available has serious ramifications when personal data is only publicly available due to error such as in the leakage of the 1,900 pupils' personal data,[156] and in all other cases where it was not through consent. These exemptions appear to have come about through pressure from industry driven by concern about compliance costs. These exemptions, however, are extremely broad and may render the whole data protection regime ineffective in providing individuals with meaningful data protection.

87 In light of the extensive exemptions for consent, the third principle concerning limitation of purpose contained in s 18 of the PDPA[157] was intended to offer some protection to individuals. The current form of s 18 is similar to the Canadian position[158] in that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances. However, just like the provision on deemed consent, s 18 is equally vague. The approach of the Data Protection Directive is to be preferred. The purpose limitation principle set out in Art 6(1)(b) of the Directive requires that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". This is indeed the gold standard to ensure privacy.

VIII. Conclusion

88 The currently recognised common law privacy torts in many jurisdictions do not adequately address the privacy problems presented by big data. Coming full circle, the author returns to the simple words coined by Judge Thomas Cooley, that one should have "a right of complete immunity: a right to be let alone".[159] Although Warren and Brandeis tried to give their own meaning to these words, their conception was too focused on the publicity aspect. The "the right to be let alone" is essentially what the Data Protection Directive seeks to achieve in this age of big data where all and sundry are engaging in collection of personal data to learn as much as possible about the

155 Personal Data Protection Act 2012 (Act 26 of 2012) Second Sched, para 1(*c*) (for collection), Third Sched, para 1(*c*) (for use), and Fourth Sched, para 1(*d*) (for disclosure).

156 See para 74 above.

157 Personal Data Protection Act 2012 (Act 26 of 2012).

158 Personal Information Protection and Electronic Documents Act (SC 2000, c 5) (Canada) s 5(3).

159 Thomas M Cooley, *A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract* (Callaghan, 2nd Ed, 1888) at p 29.

individual, and where the individual has little space to be free from constant tracking. If the framework of the Data Protection Directive is adopted as the basis of a statutory tort, then many of the attendant problems that the courts have struggled with in the public/private matter distinction will also disappear.