THE BUSINESS OF PRIVACY: FROM PRIVATE ANXIETY TO COMMERCIAL SENSE? A BROAD OVERVIEW OF WHY PRIVACY OUGHT TO MATTER TO INDIAN BUSINESSES

Malavika Jayaram[*]

Eco warriors and wildlife enthusiasts subscribe to the green credo that, while journeying through wide-open spaces, one should "take nothing but memories and leave behind nothing but footprints". This is getting harder and harder to do in the electronic frontier. Intimate details of one's personal life are being captured, copied, accessed and preserved all the time, everywhere, instantly. The corporate greed for capturing personal data, coupled with increasing surveillance by governments, makes privacy a critical theme for public discourse. This paper hopes to provide a broad sweep of key developments on the legislative front, particularly in India and Europe, while placing the big picture concerns in a global context. It hopes to transcend the narrow "privacy as a human right" rhetoric and explain why caring about privacy is as much a corporate concern as a private anxiety. It sets out some of the key drivers for taking it seriously and the rationale for why privacy makes good business sense.

I. INTRODUCTION

Never mind Orwell's dystopian vision of a surveillance society, a future where an authoritarian "other" tracked and monitored one's every move. The other is often us, as we live in a present where we are co-opted and shaped, knowingly or unknowingly, into what Microsoft Research's Gordon Bell, among others, terms "Little Brothers" – where the threat lies in "democratised surveillance, carried out not by one omnipresent authority but by millions of individuals".[1]

Lifelogging, an unusual activity that most people outside of the computer science fraternity will likely not be familiar with, involves wearing a SenseCam, "…a camera about the size of a cigarette packet, which is worn

[*] B.A.LL.B (Hons.), 1994, National Law School of India, Bangalore; LL.M, 1995, Northwestern University School of Law, Chicago; Partner, Jayaram & Jayaram, Bangalore; Fellow at the Centre for Internet and Society. The author is a PhD scholar working on issues of privacy, data protection and identity. Email: malavika@jjlawindia.com.

[1] Simon Cox, *Memories are Made of Disks*, The Sunday Times September 11, 2011.

around the neck and can be set to take photographs when triggered by such things as changes in the light, ambient temperature or body heat, or be primed to take a snapshot, say, every 30 seconds. It has no viewfinder or display, but is fitted with a fish-eye lens to capture almost everything in the wearer's view."[2] A phenomenon that resembles the love child of Facebook, Flickr, Blogger and a plethora of health monitoring apps, lifelogging aims not just at documenting and archiving every detail of one's life in a 24-7-365 way, but at creating "perfect digital memory". [3]

Bell's lifelogging is the focus of Microsoft Research's MyLifeBits project, which was inspired by Vannevar Bush's[4] imaginary Memex machine. MyLifeBits is one of many attempts at capturing entire lives, not just the curated parts of it that most people in the information age regularly document. Other experiments in continuously recording physiological information through wearable technology have given rise to terms such as "lifecasting",[5] "lifecaching",[6] and "sousveillance"[7]. While the exact methods of each of these logging experiments are beyond the scope of this paper, it is worth mentioning that as early as 1945, Bush hypothesized about his desire to reproduce, or at least to assist, the associate trails that the mind uses. Stating the limitations of record retrieval by mechanized means, and the "… ineptitude in getting at the record […] largely caused by the artificiality of systems of indexing",[8] Bush expressed his fascination with the fact that "… the human mind does not work

---

2 *Id*.

3 *Id*.

4 Director of the US Federal Office of Scientific Research.

5 Lifecasting is a continual broadcast of events in a person's life through digital media. *See* http://en.wikipedia.org/wiki/Lifecasting_(video_stream) for background and details. Technopedia, *Lifecasting*, available at http://www.techopedia.com/definition/27100/lifecasting (Last visited on January 8, 2012).

6 Lifecaching is the "collecting, storing and displaying one's entire life, for private use, or for friends, family, even the entire world to peruse" *Lifecaching*, available at http://trendwatching.com/trends/LIFE_CACHING.htm (Last visited on January 8, 2012).

7 Jascha Hoffman, *Sousveillance*, The New York Times December 10, 2006: "Surveillance, from the French for 'watching over' refers to the monitoring of people by some higher authority — the police, for instance. Now there's sousveillance, or 'watching from below.' It refers to the reverse tactic: the monitoring of authorities […] by informal networks of regular people, equipped with little more than cellphone cameras, video blogs and the desire to remain vigilant against the excesses of the powers that be."; Aarhus University, *Sousveillance: The Art of Inverse Surveillance*, available at http://www.digitalurbanliving.dk/sousveillance/ (Last visited on January 8, 2012): "Sousveillance, original French, as well as inverse surveillance are terms coined by Steve Mann (Toronto, Canada) to describe the recording of an activity from the perspective of a participant." "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments", in which the terms' inventors state: "One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in society." *See also* Steve Mann, Jason Nolan & Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1(3) Surveillance and Society 331 (2003).

8 Vannevar Bush, *As We May Think*, available at http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/3881/ (Last visited on January 8, 2012).

that way. It operates by association. With one item in its grasp, it snaps instantly to the next that is suggested by the association of thoughts, in accordance with some intricate web of trails carried by the cells of the brain. It has other characteristics, of course; trails that are not frequently followed are prone to fade, items are not fully permanent, memory is transitory. Yet the speed of action, the intricacy of trails, the detail of mental pictures, is awe-inspiring beyond all else in nature." While acknowledging that "man cannot hope fully to duplicate this mental process artificially" and that "…one cannot hope thus to equal the speed and flexibility with which the mind follows an associative trail…", he anticipated that it "should be possible to beat the mind decisively in regard to the permanence and clarity of the items resurrected from storage." His hypothetical Memex machine would function as an "enlarged intimate supplement to […] memory".

Bell and fellow lifelogger Jim Gemmell believe that "society at large is on an inexorable path to total-recall technology and it is going to transform the world around us… and change what it means to be human".[9] There are obvious privacy concerns that have been raised in relation to the passive, indiscriminate logging of information. Apart from the unfiltered sharing of intimate information, not just of oneself, but of everything in one's "field of vision", there is huge risk in third parties, and especially governments getting hold of such data. Martin Dodge and Rob Kitchin, geographers specialising in digital technologies, have studied the effects of lifelogging and the potential of pervasive computing to create widespread sousveillance.[10] Warning of the dangers of third parties indulging in "invasive profiling and social sorting" and the potential for the life-log as a marketer's dream, they point out that "… when every action is recorded for in perpetuity, in a seemingly objective manner, Bentham's panopticon[11] is realized. This is particularly the case if life-logs

---

[9] Gordon Bell & Jim Gemmell, *Total Recall: How the E-Memory Revolution will Change Everything*, available at http://www.youtube.com/watch?v=WZwoAgSMFME (Last visited on January 8, 2012).

[10] Martin Dodge & Rob Kitchin, *Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting*, 34(3) Environment and Planning B: Planning and Design 431-445 (2007).

[11] Caspar Bowden, *Ever have the Feeling You're being Watched*, available at http://www.gqindia.com/content/ever-have-feeling-youre-being-watched (Last visited on January 8, 2012):

> "The capacity of the state to watch what everyone is reading and saying online also is nothing like the old spy novel world of crocodile clips and the microphone in the martini olive. A small number of specialist companies produce compact supercomputers which can scan flows of data at fibre-optic speeds, looking for patterns, recording population-wide dossiers immensely broader than could possibly be proportionate for specific law enforcement investigations.
>
> Neither commerce nor government want you to think about the political implications of turning the Internet into a vast Panopticon, the novel design for a prison proposed by the 18th century English philosopher Jeremy Bentham. From a central control tower a single warder could observe (without being observed) the behaviour of all inmates incarcerated in cages around a circular periphery. Bentham wanted not just prisons built this way, but hospitals, schools, factories – he thought every social institution would benefit

are interlinked to create collective profiles". They also suggest that an ethics of ethics of forgetting needs to be developed and built into the development of life-logging technologies."[12]

While life-logging may be considered an extreme activity, the issues it raises contain some important lessons. It portends the intrusive effects of dataveillance performed by third parties, whether governments or private companies. There are those, like Lyndsay Williams, the lifelogger and software engineer who invented the SenseCam, who say that only what she calls "people without integrity" should fear scrutiny of their personal data.[13] This brings us to the old chestnut beloved of the privacy universe – the "if you have nothing to hide, you have nothing to fear" rhetoric. Privacy law expert, Daniel Solove, having encountered this logic so frequently, decided to ask the readers of his blog, 'Concurring Opinions,' for good responses to the nothing-to-hide argument. Amongst the flurry of responses that he received, he recounts a few in his article "Why Privacy Matters Even if You Have Nothing to Hide":[14]

- My response is "So do you have curtains?" or "Can I see your credit-card bills for the last year?"
- So my response to the "If you have nothing to hide..." argument is simply, "I don't need to justify my position. You need to justify yours. Come back with a warrant."
- I don't have anything to hide. But I don't have anything I feel like showing you either.
- If you have nothing to hide, then you don't have a life.
- Show me yours and I'll show you mine.
- It's not about having anything to hide; it's about things not being anyone else's business.
- Bottom line, Joe Stalin would [have] loved it. Why should anyone have to say more?

---

from an unrelenting disciplinary gaze. Bentham had no time for human rights, describing them as "nonsense on stilts. But today the human right to privacy is recognized in all societies worthy of the name democracy. Freedom is incompatible with watching everybody all the time."

12 Dodge & Kitchin, *supra* note 10.

13 Cox, *supra* note 1.

14 Daniel Solove, *Why Privacy Matters Even if You Have 'Nothing to Hide'*, available at http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/ (Last visited on January 8, 2012).

Solove attempts to unpack the "nothing-to-hide" argument in his new book *Nothing to Hide: The False Tradeoff Between Privacy and Security.* A key point he makes is that it the "…argument focuses on just one or two particular kinds of privacy problems—the disclosure of personal information or surveillance—while ignoring the others. It assumes a particular view about what privacy entails, to the exclusion of other perspectives." He explains how the argument anticipates a certain visceral kind of injury.[15] But others have previously critiqued Solove's taxonomy of privacy itself for being on the other extreme. Ann Bartow argues that it "…suffers from too much doctrine, and not enough dead bodies. It frames privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease." In his new book, Solove references Bartow's view that privacy needs more "dead bodies" and that privacy's "lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other [types of harm]". He even concurs, "…people respond much more strongly to blood and death than to more-abstract concerns". He, however, deviates from her view making the convincing argument that "…if this is the standard to recognize a problem, then few privacy problems will be recognized. Privacy is not a horror movie, most privacy problems don't result in dead bodies, and demanding evidence of palpable harms will be difficult in many cases."

Someone who has suffered palpable harm, if not the spilling of actual blood and guts, is Hasan Elahi- a Bangladeshi-born new media professor, he was falsely accused by a neighbour of being an accomplice to 9/11. Having been detained at a Detroit airport in 2002 by FBI agents (who subsequently released him and admitted their mistake), he was conscious that getting on the terrorist watch list was not just a one-time problem. After months of scrutiny, including a series of lie detector tests, he was finally cleared, but he suspected that his travel schedule as a professor and artist might continue to raise suspicions in the future. He decided to document the minutiae of his life, partly as an alibi to prove his whereabouts at all times (and avoid being packed off to Guantanamo), but largely as an audacious art project to question and parody surveillance. His website Tracking Transience[16] is a triumphantly magnified and twisted co-opting of the nothing-to-hide logic. "Elahi photographs his meals before he eats them, toilets before he uses them, and a GPS tracker (updated several times a day) shows his precise location. Elahi's montages made from the snapshots of the banal details of everyday life create a statement about erosion of privacy in our daily lives."[17] Another intriguing feature of his work is that the "embrace of surveillance for its subject's own protection; Elahi has protected himself from unwanted scrutiny by making his entire life and whereabouts publicly

[15] Daniel Solove, *A Taxonomy of Privacy*, 142(3) U. Pa. L. Rev. 477 (2006).
[16] *See* http://www.trackingtransience.net/.
[17] *See* http://www.coolhunting.com/culture/hasan-elahi-1.php.

accessible".[18] Elahi's project is best captured by his wry yet profound observation: "I've decided that if the government wants to monitor me that's fine. But I could do a much better job monitoring myself than anyone else."[19]

Part-II of this paper sets the context for privacy concerns in India. Noting the enhanced threat to privacy in light of increasing digitisation of information, this part explores basic attitudes towards privacy in the country. Apart from tracing the legislative efforts aimed at protecting privacy, this part examines the steps taken by industry bodies on matters relating to cyber security and data protection. Part-III argues that in the backdrop of legislative slackness, businesses have hitherto failed to provide anything more than the basic minimum standard of privacy necessitated by the market. In addition to an analysis of recent data protection and privacy reform in the UK, the EU and Canada, this part sets forth the case for greater investment in privacy protecting technology by industries. Finally, Part-IV concludes.

II. THE CONTEXT FOR PRIVACY CONCERNS

We clearly live in a strange new world where States, and indeed private actors, can monitor and record the lives of individuals to an unprecedented extent. More than ever before, it is possible to know an astonishing amount of information about people through the use of surveillance. The increasing ease of digitizing content and the ubiquity of information sharing are factors that contribute to a dizzying amount of personal information residing with third parties.

Unlike a simpler yesterday, where the only Kafkaesque scenario involved a sinister government, today attacks on one's privacy and personal space can emanate from seemingly benign private operators as easily as from obviously fascist overlords. Due to the complexity of legal and market drivers relating to data collection, processing and retention, regulatory authorities as well as private entities are stockpiling more and more data. In an economy where information is currency, there is huge pressure to be adequately monetized with data.

The fact that digitization of content has led to ease of transactions and enhanced communication is undeniable, and yet the threat of surveillance, the re-use of data for purposes other than those originally intended by owners and the lack of protection for the public-private divide are some of the less salutary features of modern life. There is an argument, though, that if there is too much connectedness and number crunching going on, it is only because there is consumer demand for it. There is certainly merit to the view that the appetite

[18] *See* http://www.einsteinforum.de/index.php?id=167.

[19] Jacob Resnick, *Hasan Elahi:Tracking Transcience*, available at http://www.coolhunting.com/culture/hasan-elahi-1.php (Last visited on January 8, 2012).

for being connected and up to date is so insatiable that people are more indifferent about how information is obtained. By offering up information voluntarily through Facebook or Twitter, everyone is collectively contributing to the death of privacy. An interesting statistic (perhaps an urban myth?) is that more personal information is put into the public domain voluntarily than was ever extracted during the worst excesses of the Hoover era and McCarthyism. This does not, however, imply that consumers are valuing privacy less, or are in fact agnostic as the use of their data: it may well be that they are unaware of how intrusive the data gathering actually is, what end use their information might ultimately be put to, or what the long-term implications of such public sharing might be. The trade-off that people seemingly make, in the interests of ease, or of distributing news in a one-to-many manner (rather than individual emails to friends) or a host of other reasons, might largely be a result of information asymmetry or a lack of transparency as to the secondary use of their personal data. This is too nuanced a matter to explain away with glib statements about the devaluing of privacy in the modern era.

Helen Nissenbaum, in a prescient 1998 article,[20] explained why the then prevailing wisdom of privacy being a private concern was a limited one. In describing what she calls "the problem of privacy in public", she expressed her concerns around data harvesting. More critically, she spoke of the problematic nature of shifting information gathered from diverse sources, which is then collated, combined and enriched into rich profile information, from one context to another. In placing context at the centre of the discourse, she talks of how theories of privacy must adequately address such data mining and context shifting, especially if "...those who engage in these practices seem to assume that the information in question has been dislodged from its contextual attachments and therefore "up for grabs". She suggests that the discomfort with the practices shows that people deem contextual integrity, and therefore privacy, to have been violated even when the information in question is not sensitive or intimate.[21] She goes on to raise an additional consideration, key to the business of profiling, which is that "…while isolated bits of information […] are not especially revealing, assemblages are capable of exposing people quite profoundly."

A. PRIVACY (OR THE LACK OF IT?) IN INDIA

The legal, sociological and philosophical concerns thrown up by emerging technologies have been the subject of discourse in the West for some

[20] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17(5) Law & Philosophy 559 (1998).

[21] *Id*.: "… the process of compiling and aggregating information almost always involves shifting information taken from an appropriate context and inserting it into one perceived not to be so. That is, the violation of contextual integrity is part of the reason critics find data aggregation to be morally offensive".

time now. From an ideological standpoint, grassroots activity and civil rights movements have served to push the notion of privacy and identity into the public domain. In the legal sphere, the development of data protection law and practice is one response to the need for safeguarding personal information. From a commercial perspective, codes of practice and self-governing initiatives/policies within businesses and within industry sectors engender customer goodwill and loyalty.

Whether one subscribes to the Scott McNeally "You have zero privacy anyway, get over it"[22] view of the world, or sees resonance in the growing tribe of people who mutilate their fingerprints in tangible protest against identity schemes, privacy can no longer be ignored. Even in India, where the popular yet simplistic view is that Indians simply don't care about privacy - a limited, if compelling, argument being that for those without access to the basics of food, shelter, healthcare, education and employment, it is seen as a luxury or an urban preoccupation - there is an increasing and perhaps long overdue politicisation of the debate, triggered largely by a slew of e-governance initiatives that impact identity, security and privacy. While this alleged cultural bias against privacy as a value[23] and a web of complex socio-economic factors may have rendered it, legitimately or otherwise, a less pressing concern than others, the increasing modernizing impetus has changed this substantially by bringing privacy to the public discourse. This shift has been effected in part through a raft of measures aimed at digitization (to make all manner of information recordable and searchable), transparency (to make the state visible and accountable, as also to stifle corruption and fraud), enumeration (to make the individual and the whole visible to the state) and service delivery (to improve access to goods, services and benefits).

B. THE "INDIANS ARE NOT VERY PRIVATE" TAUTOLOGY

When Lorrie Cranor, Ponnurangam Kumaraguru and others from Carnegie Mellon carried out what might be the only contemporary study on

---

[22] This statement was made by McNealy in 1999, while he was Sun Microsystems' CEO, at an event to launch Sun's (then) new Jini technology. Stating that consumer privacy issues were a "red herring", he went on to make this now infamous statement to a group of reporters and analysts, much to the horror of several privacy alliances and consumer coalitions that Sun was part of.

[23] Jana Diesner, Ponnurangam Kumaraguru & Kathleen M. Carley, *Mental Models of Data Privacy and Security Extracted from Interviews with Indians*, available at http://www.andrew.cmu.edu/user/jdiesner/publications/diesner_kumaraguru.pdf (Last visited on January 8, 2012); Ponnurangam Kumaraguru, Lorrie F. Cranor & Elaine Newton, *Privacy Perceptions in India and United States: An Interview Study*, available at http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf (Last visited on January 9, 2012); Ponnurangam Kumaraguru & Lorrie F. Cranor, *Privacy in India: Attitudes and Awareness*, available at http://www.cs.cmu.edu/~ponguru/PET_2005.pdf (Last visited on January 9, 2012).

Indian attitudes to privacy, their research findings led them to highlight a few critical observations:[24]

1. General Understanding and Concerns about Privacy: It would appear that Indians largely saw privacy in terms of personal space, not information as such.[25]

2. Awareness of and Concerns about Privacy and Technology: Indians were not as aware of the risks arising out of technology, such as threats from biometrics or the online environment, as their US counterparts.

3. Comfort Level of Sharing Different Types of Data: The study indicated "significant differences in comfort level across the nine types of personal information surveyed (postal mail address, email address, phone number, age, health & medical history passport number, annual household income, credit card number and passwords of email/ATM). It would appear that respondents were largely comfortable sharing their age, email address, and health information with websites, in contrast with U.S. attitudes to similar sharing.

4. Trust in Business and Government: As might have been expected, the study underlined the significant differences between trust levels – Indians exhibited an overwhelming willingness to trust organisations and the State with personal information. Research in the West has shown that "privacy-concerns levels tend to be correlated with distrust in companies and government."

5. Posting Personal Information: The study also confirmed that respondents were not as perturbed about personal information, such as university grades being posted on public notice boards on campuses, or traveller information being publicly displayed at Indian railway stations and in train compartments. The posted information includes personally identifiable information, including first and last names, age, gender, point of boarding the train, destination, seat number, etc. There were low levels of concern about these sorts of practices.

The study offers some insight into the basic attitudes to privacy in India, as part of an ongoing attempt to study this further. Without justifying the absence of strong legislative protections for data, it does highlight, with some

---

[24] *See* Ponnurangam Kumaraguru, *Privacy in India*, available at http://www.cs.cmu.edu/~ponguru/iaap_nov_2005.pdf (Last visited on January 8, 2012) (briefly summarizing the key findings).

[25] *Id*.: "The survey found that 48 percent of those surveyed related privacy to physical, home and living space. U.S. studies indicate that Americans relate privacy to health and financial information".

amusing and depressing anecdotal evidence, that the Indian perceptions of the public and the private are, if not less developed than their western counterparts, certainly less well-informed.

Until recently, there was little legal protection accorded to information, and privacy jurisprudence came through the backdoor of assertion of fundamental rights accorded by the Indian Constitution. The battleground for privacy struggles was largely located in the citizen-State sphere, and more often than not concerned the body rather than information.[26] Apart from the constitutional arena, several pieces of legislation touched on privacy, and together they formed a piecemeal attempt to address limited concerns, but this was very much a vertical approach (much like the US, where privacy has largely been dealt with on a sectoral basis), unlike the European Union style of horizontal protection by way of an overarching directive. Some of the key instruments that tackled privacy and data protection are the Consumer Protection Act, 1986, the Credit Information Companies (Regulations) Act, 2005, The Public Financial Institutions Act, 1983, the Information Technology Act 2000, the Indian Telegraph Act, 1885, the Indian Contract Act, 1872 and the Specific Relief Act, 1963. More recently, in particular over the last year or so, there have been several attempts to regulate and address privacy (like the old chestnut about waiting for a bus, and then three coming along at once).

When a data protection law was mooted a decade or so ago, largely to stem the concerns of overseas companies who were nervous about offshoring data to a country without an adequate level of protection for data, several key players within Indian industry, such as NASSCOMM, took the view that doing business in India was a complicated enough thing, with a host of laws and regulations to ensure compliance with. They felt that adding yet another law to the list would disincentivise cross-border trade and adversely affect the IT industry. They took the view that the provisions of the Information Technology Act, 2000 ('IT Act') were more than enough to handle issues around data. They echoed the market preference for papering over the gaps through the use of EU model contract clauses (to achieve equivalence through contract rather than a strong data protection law), arguing that enacting a new law would be counter productive. Strengthening the provisions of the existing law was seen by most to be a more business friendly approach.

C. IT ACT AMENDMENTS

Certain measures effected by the Information Technology (Amendment) Act, 2008 were thus intended to address data privacy and security. The main "data protection" provision, §43A, which imposes liability

[26] *See* Graham Greenleaf, *Promises and Illusions of Data Protection in Indian Law*, 1(1) International Data Privacy Law 47 (2011). *See also* Prashant Iyengar, *Limits to Privacy*, available at http://ssrn.com/abstract=1807733 (Last visited on January 8, 2012).

on a "body corporate" that fails to implement reasonable security procedures and thereby causes wrongful loss or wrongful gain, is considered by many to be a weak provision. In the absence of detailed rules being promulgated, the exact impact of the section was debatable. There were additional concerns that the Rules made under this, namely the Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data or Information) Rules, 2011 would adversely affect the Indian outsourcing industry. The new Rules "…oblige organizations to notify individuals when their personal information is collected via letter, fax or email. They require covered organizations to make a privacy policy available, to take steps to secure personal information, and to offer a dispute resolution process related to the collection and use of personal information."[27]

After some furore in the local and international media on this issue, the Indian government felt compelled to issue a clarification. The clarification itself is of somewhat dubious standing, given that it was issued in a Press Note! Legal basis and effect apart, it is broadly intended to exempt outsourcers from the new rules, and keep the personal data sent from overseas to India for processing out of the purview of the new requirements. Briefly, this exempts them from the otherwise onerous effect of the rules, which was to require companies to seek consent in writing from individual data subjects. The clarification attempts to communicate the Indian government's current view that the companies sending the data offshore, and not the Indian companies providing services, are responsible for procuring consent, according to their own national laws. Drilling down to the detail of statutory provisions of the current legal framework for data privacy is not the crux of this paper, and readers are directed towards other analyses that do more justice to this particular theme.[28]

D. A NEW PRIVACY LAW

The other development on the Indian privacy law horizon was the drafting of a Privacy Bill. The original intent was that data protection provisions under the draft National Identification Authority of India Bill, 2010 (the "UID Bill", which would cover, albeit retrospectively, the functioning of the authority managing the unique identity or "Aadhaar" project).[29] A decision

---

[27] Thomas Claburn, *India Adopts New Privacy Rules*, Information Week May 5, 2011.

[28] Graham Greenleaf, *India's U-turns on Data Privacy*, November 8 (University of New South Wales Faculty of Law Legal Studies Research Paper Series, Paper No. 42, 2011); *See also* Greenleaf, *supra* note 26.

[29] The Unique Identity (UID) scheme, now re-christened Aadhaar (meaning foundation in Hindi), is the world's most ambitious biometric identity project. It is intended to record not just citizens but residents too, and promises to establish "uniqueness" by collecting all 10 fingerprints, scans of both irises, photographs and demographic information and carrying out a process of de-duplication before issuing a unique identifier. For various reasons, this is intended to be a number rather than a physical card. The federated architecture of the system, whereby a network of public and private "registrars" can enroll applicants into the system,

was, however, taken to create a statutory right of privacy that went beyond a law that merely regulated data collected under particular project. At the time of writing, the status of this bill is still uncertain (an unofficial copy of a "third working draft" dated April 19, 2010 has been floating around), but its complexity and potential overlap with other provisions under Indian law impacting privacy would indicate that it will be significantly amended before progressing through the legislative process. A detailed analysis of this document is beyond the scope of this paper.

E. DATA PROTECTION COURTESY THE UID PROJECT

What is, however, critical to note is that the UID Bill presented before Parliament was rejected by the Standing Committee on Finance on December 9, 2011. In its 42nd Report, the Standing Committee on Finance (2011-2012) of the Fifteenth Lok Sabha ("Standing Committee") expressed in fairly robust language its reservations about the proposed UID Bill. The Standing Committee did not just reject it as drafted: it went even further by advising the government to "…reconsider and review the UID scheme" itself. In its report, it set out its objections to the UID Bill, and it highlighted several causes for grave concern, such as the lack of due process, the collection of biometric information and its linkage with personal information being "beyond the scope of subordinate legislation", the executive action that was "unethical and violative of Parliament's prerogatives", the persistence of the present problem of identification despite the Aadhaar number, the lack of a comprehensive feasibility study, the potential for fraud and the limitations of technology that make it unlikely that "the proposed objectives of the UID scheme could be achieved".

All of these developments – the new §43A rules finally being enacted, the draft privacy bill and the draft UID Bill (and the last in particular) – have resulted in the subject of privacy finally finding its way into the mainstream public discourse. What started out as a matter of concern only to certain sections such as civil society, technology professionals, academics and legal theorists, among others, is now recognized in national and international media as a pressing issue that Indians should be concerned with. Reports of the world's biggest biometric identity project being derailed (or at the very least, being challenged) due to the rejection of the UID Bill are intensifying the larger debate on the necessity for the identification scheme in the first place, as also on the finer points of its conception, implementation and risks.

with neither clear guidelines nor an overarching set of data protection principles that regulate their collection, storage, use, sharing, transfer and processing of biometric and demographic data, poses several privacy and security concerns. There are concerns that, in the absence of a strong data protection law as such, the potential for abuse is enormous. Curiously, the project was rolled out prior to it being sanctioned by the Indian Parliament.

In all of this, what was industry doing? Historically, privacy was a matter businesses were not particularly engaged with, unless they were part of the outsourcing juggernaut, and thereby driven by contractual commitments to provide an adequate level of protection to data being processed on behalf of foreign citizens (who were entitled by applicable law to certain protection even when data was offshored). Privacy was likely perceived as an emotive subject restricted to the personal domain or at best the human rights department; as something that had little to do with commerce, let alone a proposition that made business sense. In parallel with the legislative efforts outlined briefly above, however, industry bodies such as NASSCOMM, the Data Security Council of India (DSCI) and others were issuing approach papers, memos and guides (both to government bodies such as the Standing Committee on Information Technology as well as to industry generally) on cyber security and the right to privacy, on privacy in India, etc.[30] These documents borrowed heavily from global approaches to privacy and placed the nascent Indian framework squarely within the broadly accepted international understanding of privacy emanating from international conventions, APEC guidelines, OECD principles and other relevant guidelines.

These developments indicate that the current context of increasing awareness and sensitivity to issues of privacy is an interesting time for Indian business. There is a growing need for organisations to take stock of their practises and approaches to the gathering, processing, use, storage, retention and deletion of personal data, not just with an eye on achieving compliance with applicable laws and regulations, but also from a business perspective.

III. THE BUSINESS OF PRIVACY

There is a growing sense that we are all complicit in the death of privacy, mediated by the usual suspects like Facebook and Google, and an increasing awareness of the sobering fact that people largely trade privacy for convenience.[31] In the information economy, with all its clichés of data as the new currency and the insatiable governmental, corporate and private "greed" for more of it, there are suggestions that the privacy equivalent of the seatbelt

---

[30] *See Cybersecurity and Right to Privacy*, Memorandum from Data Security Council of India to the Standing Committee on Information Technology (July 9, 2010) available at http://www.dsci.in/paper/2 (Last visited on January 8, 2011); *See also* Vinayak Godse, *RISE Project - Policy Paper: Privacy in India*, available at http://www.dsci.in/sites/default/files/Policy%20Paper%20-%20Privacy%20in%20India.pdf (Last visited on January 8, 2011).

[31] Alessandro Acquisiti & Jens Grossklags, *Privacy & Rationality* in Privacy and Technologies of Identity – A Cross-Disciplinary Conversation (Katherine Strandberg & Daniela Stan Raicu eds., 2006): "…individuals are willing to trade privacy for convenience or to bargain the release of personal information for relatively small rewards"; *See also* Patrick Oppmann, *In Digital World*, *We Trade Privacy for Convenience* April 14, 2010, available at http://articles.cnn.com/2010-04-14/tech/oppmann.off.the.grid_1_cell-phone-smart-phone-digital-world?_s=PM:TECH (Last visited on January 8, 2012).

law be effected to foster an ecosystem where the default setting is privacy-respecting.[32] The argument goes that- if people cannot protect themselves and make sensible choices, law and regulation will make up their minds for them. This raises several issues around freedom, choice, informed consent, individualism, trade offs, all of which need to be carefully considered while crafting privacy laws that are "fit for purpose". While developed countries have considered these issues for some time now, I would venture that Indian industry has not tackled them with the same level of rigour and seriousness, for various reasons. In the absence of a statutory right to privacy, or strict legal provisions requiring the protection of data, businesses have been left largely to their own devices, offering no more than the basic protection required by the market standard privacy policy (in all likelihood, a cut and paste job from similar policies on their competitor's sites) or standard terms and conditions (likely drafted without a real focus on privacy issues).

Recent surveys have indicated the pressing need to take privacy seriously. In the list of privacy trends forecast by the well-known Technocrati blog for 2012, the top trend was that "Consumers choose convenience over privacy". In an interesting example of a popular blog post highlighting a conclusion made by academics five years earlier,[33] their editorial described this top trend thus:[34]

> "Geolocation data, mobile device tracking, RFID chips, grocery store loyalty cards, toll booth EZ-Pay transponders, and other portable devices track our location and other pertinent data attributes, while data analytics firms' enhanced algorithms turn meaningless data points into money making opportunities. "I have no idea what they do with this data. It was probably detailed in the "terms and conditions" I didn't read when installing the mobile application."

Ernst and Young's summary of privacy trends for 2012 included (a) the expanded reach of regulation, laws and enforcement, (b) the imposition globally of additional breach notification requirements, (c) organizations expanding governance, risk and compliance (GRC) initiatives, (d) the risks posed

---

[32] In a recent Internet Society workshop I attended ("Mapping the Identity Ecosystem" - Amsterdam, December 14-15, 2011), there was a vigorous debate about terminology, with very definite views about the relative merits of "privacy-friendly", "privacy-enhancing" (which implies improvement over a given condition of privacy - this is relative and therefore not very meaningful), "privacy-preserving" (implies prior existence of privacy to start with, which may not be true) and other terms in use. The term "privacy-respecting" emerged as the one most were comfortable with.

[33] Acquisiti & Grossklags, *supra* note 31.

[34] *See* Brian Dean, *Top 10 Privacy Trends for 2012*, December 22, 2011 available at http://technorati.com/blogging/article/top-10-privacy-trends-for-2012/page-2/#ixzz1iJEUbi1d (Last visited on January 8, 2012).

by cloud computing and mobile devices, (e) the increased investment in governance and tools for privacy and data protection (mandated by regulation as well as risks), (f) more privacy assessments, (g) service standard reporting standards (due to changes to SAS70), (h) privacy by design (regulators recognizing the need to embed privacy into new technologies upfront), (i) social networking (need for policies to govern social interactions) and (j) evolving privacy professional expectations (certifications and the like).

In 2008, the Information Commissioner's Office ('ICO') in the UK commissioned a study and report on privacy by design. The idea was to explore why, after more than 20 years of data protection legislation being introduced in the UK, not enough was being done by organizations to address privacy. One of the findings from this report was the "need for a clear articulation of the business case for proactive privacy protection". In response to this point, the ICO commissioned a further study and brought out a report in 2010 titled "The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection".

These are three examples of privacy concerns crossing over from academia and policy land into the business arena; of the threats to privacy becoming pervasive and commonplace enough that they are being debated and actioned outside of just the legislative realm. The above three paragraphs are very simple examples of how techies, consultants and regulators, respectively, are all engaging with issues of privacy. In order to make out a case for why it matters to business in particular, it is worth reviewing the Privacy Dividend exercise carried out by the ICO.

A. THE PRIVACY DIVIDEND

The Privacy Dividend report ('the Report') was the outcome of a study commissioned by the ICO. The discussion document that launched the study[35] is in itself a document worth perusing, as it raises many of the questions that business should be engaged with. In soliciting feedback from professionals with some experience in implementing privacy protection, as well as business leaders whose organisations handle a lot of data, it is a good resource for Indian businesses that have little experience of what the key concerns are, and may trigger some internal reflection on an organisation's culture of privacy protection.

In a nutshell, the Report concludes that protecting privacy makes good business sense for those organisations that process personal information regardless of their sector or size. While setting out that privacy consists of

[35] *See* Information Commissioner's Office, The Privacy Dividend: The Business Case for investing in Proactive Privacy Protection available at https://www.watsonhall.com/methodology/privacy-protection.pl (Last visited on January 8, 2011).

several components, such as physical privacy, spatial privacy, relational privacy and informational privacy,[36] it largely focuses on the last category in a business context and describes the benefits that can accrue from protecting personal privacy.[37]

The Report makes a few critical observations:

1. The protection of informational privacy is not solely about protecting personal information from *being lost*; privacy failures can take many forms, including the gathering of excessive personal information (over and above what it necessary for the purpose of data gathering), processing personal information unfairly, using inaccurate information with uncomfortable consequences or failing to inform people in the event of a breach.

2. The legitimate expectations of customers as to the handling and use of their data should inform the manner in which companies treat data – this cannot be subservient to the organisation's own view of its needs in relation to that data.

3. Privacy is not contrary to efficiency, wealth creation, data sharing or freedom of information. The Report suggests that such competing goals can be met by "…performing data sharing according to a privacy-protecting code of practice, or recognising that providing a public or consumer good (e.g. convenience) is not sufficient on it own to justify unnecessary data capture or to presume the individual's consent."[38]

4. While 'value' might be a nebulous thing when it comes to personal information, organisations should be aware that it goes beyond the commodity value that it has to the organisation processing it, and also includes the harm resulting from the loss of information, it being rendered unavailable or unusable, and the larger societal harm if privacy were violated.

---

[36] A. Westin, Privacy and Freedom (1968) (arguing that there are several ways of categorising and thinking about privacy and describing four states of privacy: solitude, intimacy, anonymity and reserve): "Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives". Solove, *supra* note 15 focuses in activities that invade privacy and cause problems, and creates a taxonomy that focuses on 4 primary groups of harmful activity: information collection, information processing, information dissemination and invasion, which he breaks down further.

[37] The second volume of the Report breaks down the main components of the business case, and offers practical guidance to enable companies to formulate their own business cases that are appropriate for their contexts and systems, but this level of detail goes beyond the scope of this paper.

[38] Information Commissioner's Office, *supra* note 35, 6.

5. Although people largely care about their privacy, the value they place on it might not be clear, *including to them*, until it is actually violated and they are affected by the harm.

The Report sets out a neat rubric for viewing the value of privacy: it suggests that organisations consider 4 dimensions or perspectives of personal information:

1. Its value as an asset used within the organisation's operations;

2. Its value to the individual to whom it relates;

3. Its value to other parties who might want to use the information, whether for legitimate or improper purposes; and

4. Its societal value as interpreted by regulators and other groups.[39]

The study underlines the fact that not respecting privacy is not just an end-user concern; the harm caused can backfire on or be squarely attributed to the organisation responsible, causing reputational loss as also monetary loss from customers taking their business elsewhere. Trying to play the blame game by pointing fingers at external entities to whom data handling activities have been delegated is no excuse: it does not absolve the organisation of accountability, and managing such assurance-related risks is (or ought to be) a key business strategy.

To sum up some of the benefits of protecting privacy and having a carefully considered approach to it at an organisational level, it is very clear from the Report that whether the driver is a desire to "do the right thing" with regard to privacy, (which involves creating and maintaining trust, being transparent and being respectful of people's privacy), a decision to embed this as part of the culture of the organisation, a marketing strategy to project a privacy-friendly ethos to its public or any number of other "soft" reasons, these do not negate the existence of several "hard" factors – what the Report calls "mission-enhancing benefits" and "risk-reducing benefits"- that make privacy critical. These include better compliance with laws and regulation (especially as regulators are getting increasingly focused on issuing rules and guidelines in this space), increased take up of services by customers (especially those who reward enhanced trust), cost reductions (which arise out of improved efficiencies in managing data, as customers provide more accurate information, as also from the lack of penalties imposed for privacy violations and data breaches, which again, are on the rise and becoming hefty amounts rather than nominal ones) and greater resilience. The Report also cautions that "the legal costs, plus the need to address the root cause of non-compliance in a manner and

[39] *Id*., 8.

timeframe not of the organisation's choosing, can also prove expensive." It highlights the finding that "61% of private organisations now believe that the DPA[40] adds value to their business, and 83% believe that it improves customers' trust – these are critical messages for a commercial operation." The figures are higher – 77 percent and 92 percent respectively - for public organisations.[41]

B. EUROPE ON THE CUSP OF DATA PROTECTION REFORM

Organisations are increasingly appreciative of the value derived from data protection, rather than resenting it as a cost to business. Their comfort level with the status quo, however, is likely to be challenged as the landscape appears to be shifting. Further, those organisations that may not have taken it too seriously thus far, preferring to take the risk of fairly weak enforcement action or relatively small penalties, will find themselves confronting a more stringent regime with greater regulatory enthusiasm for fining privacy offenders.

Viviane Reding, as European Commissioner for Information Society and Media, is credited with laying the foundations for Europe's Digital Agenda (a remit now managed by her colleague Neelie Kroes). In her current roles as Vice-President of the European Commission and EU Justice Commissioner, she is embarking on a series of reforms of the data protection regime. In a recent speech,[42] she spelt out the main aims of her reform, which are:

1. Putting citizens in control of their data;
2. Ensuring security in the cloud;
3. Creating a right to data portability;
4. Creating a level playing field and a more business-friendly regulatory environment;
5. Rethinking international data transfers; and
6. Encouraging innovation and trust.

[40] The Data Protection Act, 1998 of the UK implements the EU Data Protection Directive, *infra* note 46.

[41] SMSR, Report on the Findings of the Information Commissioner's Office- Organisations-Annual Track (2008) available at http://www.ico.gov.uk/Global/Search.aspx?collection=ico&keywords=Annual+Track+2008+–+Organisations+Report (Last visited on January 8, 2012).

[42] Viviane Reding, Vice-President, European Commission, EU Justice Commissioner, *Privacy in the Cloud: Data Protection and Security in Cloud Computing Roundtable*, Sppech/11/859 at the High Level Conference on Mobilising the Cloud organised by GSMA Europe, Brussels (December 7, 2011) available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/859 (Last visited on January 8, 2012).

Elaborating on each of these, she highlighted, firstly, the need for companies to ensure transparency and empower citizens to make informed decisions about how their data is used. Not only does this require companies to tell citizens what data is collected and for what purposes, whether it will be available to third parties, what their rights of redressal are, etc. all of this information must be in simple and understandable language. Secondly, while recognising that security is also a problem when information is stored locally, she wishes not to underestimate the risks where the data of millions of people is stored and therefore and she wants "business [having] to pay utmost attention to security of information and privacy by design".

Thirdly, she wishes to ensure that users should have total freedom as to the mobility of their data when they leave a cloud service, and to "leave no digital traces behind". She is intent on companies not erecting barriers to change, and stifling competition by locking in people to their services. More importantly, she warns against users being deprived of "…their effective right to freely choose and freely change the best privacy environments for their personal data". This data portability is intended to be key feature of her proposed legislative reform.

Her fourth point about a level playing field is largely concerned with simplifying the regulatory environment: conscious of inefficient data protection rules and administrative burdens, she is keen to encourage business to operate successfully across borders and achieve economies of scale. The fifth limb of her reform agenda is closely linked to this; mindful of the fragmentation in the EU and the need for a "single online market for online services", she states that "the free flow of data will be guaranteed" and that transfer of personal data to third countries (historically a fairly cumbersome and fraught area) will be covered by a single set of instruments and rules, rather than the extra conditions imposed on a national level by various countries. These in particular are of huge significance to Indian business, and, if implemented by the proposed legislation, will result in potentially driving down the cost of international data transfers both for the outsourcer and the service provider.

Her last point, about fostering innovation and trust, is aimed at ensuring a competitive edge for those companies that respect privacy, yet creating a level playing field for all businesses (as between European companies and their competitors elsewhere).

Although this presentation was made in the context of cloud computing,[43] she underlines the broader reach of her legislative reform, and confirms that "many of the issues (of cloud computing) are similar to any outsourcing service, in particular to cross-border outsourcing" and that she intends

[43] She also confirmed in this speech that Neelie Kroes would propose a European Cloud Computing Strategy in 2012.

to lay a sound legal foundation by "removing fragmentation, reducing red tape and rationalising the instruments for international transfers of personal data".

This speech is a curtain raiser of the types of legislative reform that we might see coming out of Europe this year. All of these have implications for Indian business, not just in the outsourcing realm for companies processing the data of European citizens, but also for companies offering online services, particularly cloud based platforms and applications. Companies would be well advised to stay abreast of these developments, as they have a wider impact than within Europe, and, to the extent that they are effective in harmonizing the legal and regulatory environment that Indian companies ensure compliance with (whether driven by law, contract, binding corporate rules, marketing strategy or otherwise), they may ring in some changes that will benefit Indian business operating in the technology and service industries.

There has already been some activity in this sphere: the European Commission has already sent the proposed "Data Protection Framework for the EU" for a period of consultation. This framework is the reform that Viviane Reding refers to (as part of a legislative package that she will propose in January, 2012) and is intended to introduce a General Data Protection Regulation (meant to update the current directive that was adopted in 1995[44]) and a new Police and Criminal Justice Data Protection Directive (an analysis of which is beyond the scope of this paper). The objective of this new proposal is largely to fulfill the European Commission's ambitions of harmonising the European data protection regime, and of enhancing the rights of individuals.

The draft regulation in relation to the General Data Protection Directive was "unofficially" released online in December, 2011[45] (the official version is due for publication in January, 2012). There have already been some criticisms of the draft document that is under consultation. Commentators and legal experts have pointed out that "while one of the stated objectives is also "cutting red tape for businesses", it is difficult to see how this objective has been met in the draft documents, given the increased burdens on industry."[46]

---

[44] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (Last visited on January 9, 2012).

[45] European Commission, *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 of such Data* ('Draft Regulation'), November 29, 2011 available at http://epic.org/privacy/intl/EU-Privacy-Regulation-29-11-2011.pdf (Last visited on January 9, 2012).

[46] Reed Smith, *European Commission's Proposed Change to the EU Data Protection Laws: Detailed Analysis*, available at http://www.reedsmith.com/publications/search_publications.cfm?widCall1=customWidgets.content_view_1&cit_id=32923 (Last visited on January 8, 2012).

Some of the key elements of the proposed framework are that:

1. It clearly underlines the extraterritoriality of European data protection law, something that was legally ambiguous and debated thus far (Art. 2 now explicitly extends the scope of the regulation to anyone who processes personal data of EU citizens, *i.e.*, to data controllers regardless of whether they are established within or outside the EU).

2. It will apply to individuals who post other people's personal data online (the text refers to individuals who make "the personal data of other natural persons accessible to an indefinite number of individuals").[47]

3. Certain definitions have been added, such as "personal data breach" (which now includes data whether in transit, storage or processing), and others have been reworked, such as health data now becoming "data concerning health" and including two new definitions for "biometric data" and "genetic data".

4. It introduces new rules with regards to consent (data controllers will now have to prove that they were provided with consent - which may not be relied upon in the event that there is a "significant imbalance in the form of dependence between the position of the data subject and the controller"[48] – and prohibits direct marketing without consent).[49]

5. It clarifies the principle of data minimization (data collection should be adequate, relevant and limited to the minimum necessary for the purpose of processing and should only be processed if it is not possible to do so in a manner that does not identify the data subject). [50]

6. It introduces the much debated "right to be forgotten"[51] (which extends the previous right of objection and erasure).

---

47 Draft Regulation, Art. 2(5)(d).

48 Draft Regulation, Art. 7(4).

49 Opt-outs are only possible for marketing for non-commercial purposes that are "recognised as being in the public interest".

50 Draft Regulation, Art. 4(1)(c).

51 John Armstrong, Emma Burnett, Sarah Cole & Rachel Sherratt, *A First Glimpse of the New General Data Protection Regulation* December 16, 2011 available at http://www.mondaq.com/x/157618/Privacy/A+First+Glimpse+Of+The+New+General+Data+Protection+Regulation: "Article 15 gives the data subject a right to be forgotten and to erasure. The data subject has the right to erasure of his/her personal data where: the data is no longer necessary in relation to the purposes that it was collected or processed for; the data subject withdraws consent or the storage period has expired; the data subject objects to the processing of the data; or the processing does not otherwise comply with the Regulation. If the data is in the public arena, there is an obligation on the controller to erase or restrict the processing of that data, including where links to or copies of the data can be found on the internet."

7. It introduces the right of portability that Reding referred to in her speech.

8. It embeds the concepts of "privacy by design" and "privacy by default".[52]

9. It imposes limits on profiling ("organisations would potentially be barred from profiling individuals based on automatic processing that seeks to predict a person's performance to work, creditworthiness, economic situation, location, health, personal preferences, reliability or behaviour; unless done so in the course of performing a contract, consent has been obtained or is expressly authorised under law"[53]).

10. It revises third country data transfer rules (transfers may be made so long as they are "not frequent, massive, or structured, and adequate safeguards are in place"[54]).

11. It imposes rigorous new sanctions and remedies and sanctions (this made headline news as the draft Regulation provides three tiers of sanctions for negligent or intentional breaches of 1 percent, 3 percent or 5 percent of annual worldwide turnover of an enterprise[55]).

As the official version is not yet available, it is hard to predict to what extent these provisions will change. The draft does, however, provide a sense of the concerns and preoccupations in relation to data protection reform, and it is probably safe to say that a fair number of provisions will find their way into the official proposal and eventually be enacted. Once the new measures are finalized they will need to be adopted by the European Council and the European Parliament.[56] Although there does not seem to be any indication of whether the currently accepted methods of cross-border data flows, such as the model contractual clauses, the US Safe Harbour framework, the list of countries approved as providing adequate protection and the use of Binding Corporate Rules, will be affected significantly, it is worth keeping an eye on these aspects as they will have an impact on Indian businesses providing data processing and online products and services into the EU.

---

[52] Draft Regulation, Art. 27(3) (Security of Processing) empowers the Commission to further specify the criteria for the technical and organisational measures that are necessary to ensure security, and specifically references the need to take into account key developments in the areas of "privacy by design" and "privacy by default".

[53] Smith, *supra* note 46; Draft Regulation, Art. 18(1).

[54] Smith, *supra* note 46.

[55] For details of when the sanctions are triggered, *see* Draft Regulation, Art. 70 (Administrative Sanctions).

[56] The Electronic Privacy Information Centre, *EU Data Protection Directive*, available at http://epic.org/privacy/intl/eu_data_protection_directive.html (Last visited on January 9, 2012).

C. A BRIEF PAUSE FOR A PRIVACY BY DESIGN PRIMER

Without intending to derail the discourse, it is probably worth taking a step back to set out exactly what privacy by design means. It has come up several times in this paper, as various entities and people have referenced it, but for those who are not familiar with the concept, a brief overview might be in order. What started out as a term of art beloved to data protection geeks has now extended not just to policy wonks and regulators, but has also found its way into the mainstream through the publications and industry analyses put out by consultants and technology companies. This crossover from regulator-speak into (relatively) common parlance is largely credited to Ann Cavoukian, the Information and Privacy Commissioner of Ontario. Her work contested the assumption largely prevalent in the 90s that regulation was the answer to ensuring privacy: her view that embedding privacy upfront while designing systems, so as to make it an organisation's default position, has gained a lot of traction.[57] Her original work focused on the technology of privacy by design ('PbD'), but she later extended this to business practices as well as physical design and infrastructure.[58] Subsequently, she also tackled the idea of privacy by redesign[59] (to reengineer existing and legacy systems to be privacy friendly even if their original design was not mindful of or sensitive to privacy concerns).

Her articulation of classic PbD focused on seven guiding principles.[60] These principles are:

1. Proactive not Reactive: Preventative not remedial (the aim is to prevent privacy invasions, not to fix them after the fact).

2. Privacy as the default (not as something the user needs to configure or select).

3. Privacy embedded into system design (it is integral to the architecture, as something considered up front).

4. Full functionality – Positive Sum not Zero Sum (one of her key contributions was to challenge the zero-sum approach which pitted privacy

---

57 *See* http://privacybydesign.ca/.

58 Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada, *Privacy by Design*, available at *http*://www.ipc.on.ca/images/Resources/privacybydesign.pdf (Last visited on January 9, 2012).

59 Ann Cavoukian & Claudiu Popa, *Privacy by Redesign: A Practical Framework for Implementation*, available at http://privacybydesign.ca/content/uploads/2011/11/PbRD-framework.pdf?search=search (Last visited on January 9, 2012).

60 These principles were discussed and widely adopted as a resolution by regulators and policy makers at the 32nd Annual International Conference of Data Protection and Privacy Commissioners meeting in Israel in October, 2010.

against other interests such as security; her focus was to show that it was possible to accommodate various interests and not have to make trade-offs between legitimate concerns).

5. End-to-end security – Lifecycle Protection (to ensure that data is protected from "cradle to grave").

6. Visibility and Transparency.

7. Respect for User Privacy.

While it is heartening to see the language of PbD find its way into regulator-speak and techie-speak, a word of caution is necessary. There are some criticisms, particularly from the engineering world, that the jargon is reflexive and ambiguous; that there is a lack of clarity about exactly what PbD means. Some have commented, "most of the principles include the term "privacy by design" in the explanation of the principle itself. For example, the definition of Principle (3), Privacy Embedded into Design, states that: "Privacy by design is embedded into the design and architecture of IT systems (…). It is not bolted as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system without diminishing functionality". This recursive definition – privacy by design means applying privacy by design – communicates to the reader that something needs to be done about privacy from the beginning of systems development, but it is not clear what exactly this privacy matter is nor how it can be translated into design."[61]

Computer scientists are mindful that PbD is a complex engineering task, and warn of the dangers of "…reducing such methodologies to "privacy by design check lists" that can easily be ticked away for compliance reasons while not mitigating some of the risks that privacy by design is meant to address."[62] There is also a concern that merely treating it as an engineering problem ignores many of the learnings from the social sciences.[63]

---

[61] Seda Gürses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design* available at https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf (Last visited on January 9, 2012).

[62] *Id*.

[63] *Id*. (They outline some of the dangers from data mining in particular, highlighting the information contained in the gaps and silences as much as in actual activity. For example, "Even though inferences can be very positive from a business perspective, their consequences can be devastating from a privacy point of view. Data mining increases the risk of discriminatory social sorting (31) with its corresponding disadvantages for citizens. A lot of the information that can be inferred from location data traces fall into what is considered highly sensitive information about customers. The trajectories followed by an individual reveal health information, political affiliation, or religious beliefs. A person visiting frequently an oncology clinic exposes her medical condition. A similar risk affects users whose location record reveals that they regularly visit a Catholic church or a mosque, thus disclosing their religion. We also note

This word of caution is worth bearing in mind. Sound bites from industry leaders, trend forecasts from business analysts and media reports about the business of privacy all bandy about the term without really engaging with what it truly means or does. As such, it does run the risk of becoming a term of art beloved of industry, a way of displaying organizational commitment to privacy, while perhaps merely paying it lip service. Plainly, the risk is of co-option merely of the term by the business community, without referencing or having a sense of its origins or its philosophy. Having said that, a world where privacy is a significant enough concern for business leaders to be discussing it, is a better alternative than an environment of indifference.

D. BACK TO THE BUSINESS OF PRIVACY

Harriet Pearson, Chief Privacy Officer at IBM, describes a third scenario that lies between "…the extremes of total transparency and total public withdrawal"; a zone that she refers to as "trusted balance".[64] Her vision is that enterprises continue to gather data and even deal in it (buying, selling, transferring) but they do so in a transparent, responsible manner that is often controlled by the individual. She envisages that "…governments and businesses inform the public about how they collect, store and use personal information. And people have the choice to opt out or opt in as they see fit (except in cases where that right is superseded by a compelling public need, such as law enforcement or public health). These rules are enforced at the organisational, industry and governmental level and are protected by strong security protocols." This raises several red flags around how the contentious issue of informed consent (simplistically, in a world where you cannot negotiate terms with service providers, and need a PhD in parsing privacy policies and fine print, can it really be informed, and is it even consent?) and the precarious future of the opt-in/opt-out approach to privacy (and indeed other online and offline choices). That apart, some of the examples she mentions – she cites "Hippocratic database technology" as an example of privacy by design – give some assurance that systems and processes can be embedded with technical solutions that are privacy friendly and that do not necessarily require user intervention or choice.

She describes the IBM project where "individual fields within medical records can be obscured as necessary to protect patient's privacy. A clerk or an admitting nurse, for example, would see only limited information, whereas an emergency room doctor would be able to view an entire medical history. Hippocratic databases are designed from the beginning with special tags denoting the level of confidentiality attached to each field. The tags, in

that although the locations frequented by a person encode a lot of knowledge, they are not the only car usage data that leak personal information. For instance, not driving the car on Saturdays may disclose as much information as praying at the synagogue").

64 IBM, *Privacy is Good for Business*, available at http://www-07.ibm.com/innovation/in/customerloyalty/harriet_pearson_interview.html (Last visited on January 9, 2011).

effect, carry the hospital's privacy policy along with them. The patient's name is less private and can be shown to any member of staff, but the patient's history of drug use is strictly confidential and can be shown to medical personnel only. This makes it possible to write programs that can translate privacy policy directly into secure IT."

There are several such attempts to preserve privacy without derailing legitimate business interests, and this is an area there will hopefully be continual innovation and growth. As the world moves towards stronger regulations governing privacy, it is a no-brainer for industry to invest in technologies that are mindful of privacy, without pushing all the risk and choice onto users. At the end of the day, the user experience and the interface between people and technology is still required to be as simple and unobtrusive as possible. While certain people with a high degree of sensitivity of privacy concerns (I plead guilty to falling squarely within that camp) will make the effort to fiddle with privacy controls and default settings, most will not, preferring instead to just "get on with it". Given the many reasons why privacy as a value is integral to society, and is part of the both the rights and entitlements package as well as the "my data is my property" logic, businesses – as part of the ecosystem that switches on and maintains solutions for privacy problems – must build it into their value propositions and work cultures.

Speaking about the dangers of a privacy dystopia, Jonathan Raper of Placr Ltd., who is also on the Mayor's Digital Advisory Board in London, England, set out the following key goal:[65]

"Users must be able to reject/modify a privacy transaction without a disbenefit, while still getting a service. To achieve this we need:

1. Strong security on storage of records.
2. Robust authentication of access.
3. Traceable transfers for re-use.
4. Verification of information used for inferencing.
5. Control over tracking/ location."

In his presentation, he went on to explain some of the scandals over cookies, tracking and logging, as indicators that the above goals are not being achieved. He proposed brokering as a solution to certain privacy concerns – the risks arising from the ubiquitous and practically invisible efforts

[65] Jonathan Raper, *Brokering as a Solution to Location Privacy*, Presentation at 'A Fine Balance" Conference, London (December 12, 2011).

to track location data - and described a model where the user and the "broker" could co-monetise the value of data. The argument went that, rather than Facebook or Google or the owners of mobile applications making money off users' data, the user could partner with a "bank" or "broker" to store all their location data, for example, and make informed choices about who could have access to it and for what purpose, and retain control over both the use of their personal data as well as the opportunity to financially benefit from such use.[66]

IV. CONCLUSION

It ought to be clear that, for various reasons, the business of privacy is gaining traction, possibly even at a pace greater than the human rights discourses surrounding it. Due to a combination of, *inter alia*, regulators' zealousness, the growing risks of privacy violations as technologies make government surveillance and private data mining increasingly easy, the escalating awareness of the value of privacy as something sacrosanct in society, and the unassailable benefits of taking it seriously at an organisational level, the year ahead already merits a Dickensian "best of times, worst of times" label.[67] An unlikely analogy perhaps, but the opening passage to A Tale of Two Cities carries tremendous resonance:

> "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to heaven, we were all going direct the other way - in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only."

In a recent conference I attended, Prof Ken Klingenstein used the marvellous phrase "digital asbestos".[68] In our attempts to legislate and govern privacy, or evolve technical safeguards, we need to be mindful of how well or badly we can future-proof these efforts. Businesses are as much key players in empowering user control and decision making as the State, and while there are very strong reasons for privacy to percolate down from the academic realm into the plane of action, we must remain mindful of what Jonathan Margolis calls

---

66 For more information on the idea of a location bank, *see* http://www.firstlocationbank.com/.

67 Charles Dickens, A Tale of Two Cities.

68 Notes from the Internet Society's *Mapping the Identity Ecosystem* meeting in Amsterdam, December 14-15, 2011: "We could suffer from "digital asbestos" like we suffered this wonderful building material asbestos in the past. It took a lot of effort to remove asbestos after we discovered its true nature."

"the arrogance of the present"[69] – the problem of understanding tomorrow with today's mindset, generally, and in particular, the difficulty in assessing "the future potential of new technology when all you have is a mind-set from the "present" from which to make the judgment."[70]

In conclusion, I would urge organisations to question their own practices and approaches to the technology and business of privacy, and to tackle the hard questions about how the notion of identity is changing, whether anonymity is necessary or desirable within an organizational structure, whether the balance of rights between staff (and indeed customers) and employers needs to be revised, how the risks posed by social networking can be managed and what the new battlegrounds for privacy struggles will be going forward. They may just be able to stave off digital asbestosis if they embark on a well-considered fitness program starting now.

[69] Jonathan Margolis, A Brief History of Tomorrow: The Future Past and Present (2000). *See also* http://www.theenvisioners.com/index.php/tag/arrogance-of-the-present/ (Last visited on January 9, 2012).

[70] The Envisioner, *Never Predict Anything, Especially the Future*, available at http://www.theenvisioners.com/index.php/2011/03/18/back-to-the-arrogance-of-the-present/ (Last visited on January 9, 2012).