Data is your organisation's core business: Are you prepared to govern it?[1]

Received: 4th March, 2018

Annelies Moens
is a widely recognised global privacy expert and thought leader, trusted by business executives, government and privacy professionals. She is Managing Director of Privcore and formerly Deputy Managing Director at Information Integrity Solutions, the largest privacy consulting company operating within the Asia Pacific region, providing privacy advisory services to both the private and public sectors. Annelies co-founded the International Association of Privacy Professionals in Australia and New Zealand in 2008. She held elected roles during her six year board term, including as president. Over the last 17 years, she has held senior leadership roles predominately in privacy and related fields, including at the Australian privacy regulator. She has an MBA in general international management (distinction) from the Vlerick Business School in Belgium, is a qualified lawyer, and has undergraduate degrees in computer science and law (first class honours) from The University of Queensland, Australia. Annelies is a fellow of the Australian Institute of Company Directors, a chartered manager and fellow of the Australian Institute of Managers and Leaders and is a certified information privacy professional (information technology) through the International Association of Privacy Professionals.

Managing Director, Privcore Pty Ltd, Level 14, 5 Martin Place, Sydney, NSW 2000 Australia
E-mail: amoens@privcore.com

Abstract This paper explains why data and its governance as part of corporate governance are important to most, if not all, organisations, and is something that leaders and directors need to embrace. The paper highlights some key themes affecting the governance of data, such as trust and social licence, mass customisation, an increasing number of data breaches and technology. It then follows with a call for leaders and directors to help shape and influence the direction technology takes by providing examples played out in the media of innovation that have privacy at their core, as well as those that provide more challenges and grey areas. The final part of the paper provides guidance to readers on what leaders and directors can do to help build trust. This will include looking at culture, risk management frameworks, accountability, monitoring key indicators, working and collaborating with regulators.

KEYWORDS: governance, data, leaders, directors, trust, customers

WHY LEADERS AND DIRECTORS SHOULD TAKE CARE

Data are an asset or a liability depending on how it is managed[2] and in this sense, every organisation (business, government and not-for-profit) is a data business.[3] As an asset or a liability, data are a core topic with which directors must make themselves comfortable and familiar, and are an essential component of corporate governance.

Furthermore, a lot of data in organisations are about people, their lives, what they do, where they go, what they buy, what they like, what they say, what they look for, what they do for entertainment and so on — it is personal information and thus in many instances is subject to privacy and data protection requirements. Data are so integral to organisations, that it must be treated as core business. Data protection and privacy also have the added dimension of being considered a human right in some jurisdictions.[4]

Some of the top-valued companies globally, including Amazon, Apple, Facebook, Alphabet (Google) and Microsoft are individually worth billions and collectively made more than US$900bn in the past year.[5] As these companies are data businesses relying on personal information, they understand the value of their customers' data.[6]

In order to lead successful organisations, leaders and directors need to develop a vision that enables their organisations to make decisions which build trust with their customers.[7] Customer trust and customer privacy go hand in glove and the governance of data is not something that can be relegated effectively to compliance and IT functions without board oversight and direction.

THEMES AFFECTING THE GOVERNANCE OF DATA

Trust and social licence

The 2018 Edelman Trust Barometer reveals that trust is in crisis around the world. In 20 of the 28 economies surveyed, business, government, NGOs and media are generally not trusted.[8] Yet for innovation to flourish, trust is vital[9]; and innovation depends increasingly on the use and sharing of data.

In Australia, the Office of the Australian Information Commissioner's Community Attitudes to Privacy Survey 2017 shows that 'one in six [citizens] (16%) would avoid dealing with a government agency because of privacy concerns, whilst six in ten (58%) would avoid dealing with a private company'.[10] Boards need to think about how their organisations communicate with stakeholders. How do they build and shape expectations with customers? It is certainly not shaped by the terms and conditions of products and services.[11]

Mass customisation

The term 'mass customisation' refers to our present-day era where we have taken the handmade bespoke aspects of the pre-industrial era and the mass production capability of the industrial revolution era to be able to produce customised items at scale.[12]

In our mass customisation era there is a need for customer centricity, where we need to understand our customers at an individual level in order to provide for their bespoke needs. Yet at the same time, ensuring an organisation has a 360-degree view of a customer is NOT a customer-centric approach, as customers may not want to fully reveal themselves to organisations. Customers may want to be able to choose what they share.

Privacy is all about giving the customer control of what happens with their data — making them the driver and the reason for our products and services. As such, customer service and managing failure, including data breaches, are becoming increasingly crucial touchpoints in determining the level of engagement and goodwill customers have towards brands and institutions.

Increasing number of data breaches

Being able to manage failure is increasingly important as more and more organisations are subjected to data breaches owing to either their own inadequate security practices, system/human failures or unfortunate external attacks against which they cannot fully protect themselves.[13]

The more data that leave controlled and protected environments, the more we are polluting our data ecosystem. Identity fraud increases, trust diminishes (both ways between customers and organisations) and billions of dollars are wasted.[14] Indeed, an Australian expert on data breaches recently testified before the US Congress on the impact of such breaches on identity verification, and outlined that static knowledge-based authentication is becoming increasingly risky in a post-breach data world.[15] Focus on cybersecurity to ensure organisations have control of the data for which they are custodians is becoming increasingly crucial.

Technology

Technology is rapidly dictating our policies as legislatures and policy makers struggle to keep up. We are in a world where it is easier to keep data than delete it[16] and it is easier to create systems that retain data.[17] An increasing amount of data will be collected about people as more devices become connected to the Internet of Things, which saturates our lives.

We have new technologies that are affecting massively the handling of individuals' personal information:

- Automated driverless cars and the collection of masses of data from sensors, voice and behaviour.
- Automated algorithmic decision making and artificial intelligence affecting our day-to-day lives.[18]
- Social credit scoring.[19]
- Biometrics and facial recognition in private and public spaces.[20]
- Digital identity management.[21]
- Cloud services through which data storage and processing is outsourced.

While none of these technologies are inherently bad, they can rapidly lead to massive increased individual risk, through over-collection of data, data breaches and misuse, or out of context use. These issues can be minimised with appropriate governance, which will be needed in order to retain customer trust.

LEADERS NEED TO HELP SHAPE AND INFLUENCE THE DIRECTION TECHNOLOGY TAKES

We are at a pivotal point in history — how we lay our foundations now will determine the kind of society we will live in. Technology is changing our lives rapidly both for good and bad. We need to build core human values and ethics into our products and services. We must keep individuals at the centre and build technology that respects human values, including privacy and security. Outlined below are examples of innovation where privacy is at their core, as well as those that provide us with a few more challenges and grey areas.

Examples of innovation that have privacy at the core

- Trade Me — Transparency Report: In 2017, Trade Me published its fifth Transparency Report to give insight into how it works with law enforcement and government agencies to help keep its website trusted and safe.[22] The Transparency Report helps keep law enforcement and government accountable for their requests for customer data and deters customers from criminal activity on Trade Me.
- Tresorit: End-to-end encryption cloud service, where only customers can see their data.[23]
- Startpage — Anonymous searching: Google search results with privacy protection — no collection of personal information or what you search for.[24]
- Wire: Secure conversations and video calls with end-to-end encryption.[25]

Examples of innovation, but without privacy at the core?

Great technology can be implemented badly without security and privacy by design. Some of the examples below are for illustrative purposes only and are now being rectified by the companies themselves, regulators or being litigated.

- Vtech Electronics: Connected toys, apps and platforms collecting personal information without notice and consent, and not taking reasonable steps to secure the data.[26]

- Vizio, internet-enabled TV: Collecting what viewers watch and selling it to advertisers without viewers knowledge or consent through snooping pixels.[27]
- Uber, ride sharing: Collecting information about customers' mobile phone battery life and identifying that customers are willing to pay more for rides when their battery is running low on charge[28] and Uber admitting that it actively concealed data breaches.[29]
- Bose, headphones: Allegedly collecting the music you listen to and selling it without permission.[30]

WHAT LEADERS AND DIRECTORS CAN DO TO BUILD TRUST

Develop a culture of respect

The importance of culture cannot be underestimated. In an independent review of the Accident Compensation Corporation (ACC) in New Zealand following a data breach that occurred in 2012, culture was the biggest transformational issue for ACC.[31] It had had inconsistent practices around respecting personal information, which led to numerous incidents of inappropriate handling of personal information. Today, New Zealand government agencies have privacy maturity assessment frameworks in place and a chief privacy officer who operates across the whole government as a result of that independent review, so that confidence and trust in New Zealand government can grow.[32]

Make privacy part of risk management frameworks

According to the World Economic Forum's 2018 Global Risk Report, alongside extreme weather events and natural disasters, cyberattacks and data fraud/theft are the top three and four likely risks to occur.[33] As such, privacy needs to be part of risk management and assurance processes.

Make leadership accountable

What gets measured gets done. If no person at senior executive level or board level is responsible for the decisions their organisation makes with respect to what happens to customer data, the direction the organisation takes will likely be dictated by factors other than core values, such as respect for personal information.

Monitor key indicators such as input from customers, suppliers and employees

Listen not just to senior executives, but also to customers, suppliers and a broad set of employees. Consider how fast bad news travels to the board and whether privacy is a regular board agenda item. How are failures and complaints managed within the organisation?

Collaborate with the regulator

Regulators with collaborative approaches[34] tend to have more successful regulated outcomes (plus most complaints are negotiated settlements). The New Zealand Privacy Commissioner, as an example, is taking an innovative regulatory approach by introducing a Privacy Trustmark, whereby it is willing to indicate services or products that take data protection seriously and give customers confidence their personal information will be respected and protected.[35]

SUMMARY

It is incumbent on leaders and directors to know what goes on in their organisation in terms of the handling of personal information; only then can they steer their organisation to adopt and develop innovations that respect one of their most valuable assets. Failure to do so is likely to lead to customer dissatisfaction and loss, regulatory intervention, fines, shareholder and customer litigation and class actions, and decline in share value and profits.

References and Notes

1. Based on an article and presentation prepared for the Australian Institute of Company Directors' Australian Governance Summit, 1st to 2nd March, 2018, Melbourne, Australia.
2. World Economic Forum (2011) 'Personal data: The emergence of a new asset class', available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed February 2018) and Sidgman, J. and Crompton, M. (2016) 'Valuing personal data to foster privacy: A thought experiment and opportunities for research', *Journal of Information Systems*, Vol. 30, No. 2, pp. 169–181.
3. Moens, A. and Roberts, N. (2017) 'Not just and IT issue: Why governance of data should be on the agenda of every board director', *Governance Directions*, March, pp. 104–106.
4. Privacy is a fundamental human right recognised in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional treaties.
5. Levy, A. (2017) 'The big five tech giants added $181 billion in market value on Friday', *CNBC*, 27th October, available at: https://www.cnbc.com/2017/10/27/amazon-alphabet-microsoft-facebook-apple-added-181b-to-value.html (accessed February 2018).
6. 'The world's most valuable resource is no longer oil, but data', *The Economist*, 6th May, 2017, available at: https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (accessed February 2018).
7. Selby, J. (2017) 'How can company boards build trust when faced by cybersecurity risk?', *Optus Macquarie University Cyber Security Hub*, p. 3.
8. '2018 Edelman Trust barometer global report', available at: https://www.edelman.com/trust-barometer (accessed February 2018).
9. Botsman, R. (2016) 'We've stopped trusting institutions and started trusting strangers' [online video], available at: https://www.ted.com/talks/rachel_botsman_we_ve_stopped_trusting_institutions_and_started_trusting_strangers (accessed February 2018)
10. Office of the Australian Information Commissioner (2017) 'Australian community attitudes to privacy survey 2017', p. I, available at: https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017 (accessed February 2018).
11. Berreby, D. (2017) 'Click to agree with what? No one reads terms of service, studies confirm', *The Guardian*, 3rd March, available at: https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print (accessed February 2018).
12. See, as an example, Shoes of Prey: Design Custom Made Shoes, available at: https://www.shoesofprey.com/ (accessed February 2018).
13. According to the 2017 'Cost of data breach study Australia', Ponemon Institute LLC (sponsor IBM), 52 per cent of data breaches are due to negligence or system glitches in Australia.
14. Equifax, Yahoo and Target are examples of companies that paid or will pay tens to hundreds of millions of dollars owing to data breaches either through devaluations, litigation, brand damage or customer and supplier costs.
15. Hunt, T. (2017) 'Here's what I'm telling US Congress about data breaches [web blog]', 30th November, available at: https://www.troyhunt.com/heres-what-im-telling-us-congress-about-data-breaches/ (accessed February 2018).
16. Mayer-Schonberger, V. (2011) 'Delete: The Virtue of Forgetting in the Digital Age', Princeton University Press, USA.
17. See, for example, Australia's metadata retention scheme whereby telecommunications service providers are required by law to retain at least two years' of customer metadata so that criminal law enforcement agencies and authorities that can investigate serious contraventions of domestic law can find out what, where, when and with whom customers e-mailed, messaged or spoke: *Telecommunications (Interception and Access) Act 1979 (Cth)*.
18. Moens, A. (2016) 'Book review: *Weapons of Math Destruction* 2016, Cathy O'Neil, Data Scientist iappANZ, *Privacy Unbound*, Issue 76.
19. Botsman, R. (2017) 'Big data meets Big Brother as China moves to rate its citizens', *Wired*, 21st October, available at: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion (accessed February 2018). And in Australia there are moves to set up social scoring for those who would find it otherwise difficult to obtain credit; see www.lodex.co and Redrup, Y. (2018) 'How social data could help you get a loan', *Australian Financial Review*, 27th December, 2017 to 1st January, 2018, p. 19.
20. Dingwall, D. (2017) 'Facial recognition technology to replace passport scans at airports', *Canberra Times*, 28th July, available at: http://www.canberratimes.com.au/national/public-service/facial-recognition-technology-to-replace-passport-scans-at-airports-20170726-gxjd5v.html (accessed February 2018) and deAgonia, M. (2017) 'What is face ID? Apple's new facial recognition explained', *ComputerWorld*, 1st November, available at: https://www.computerworld.com/article/3235140/apple-ios/what-is-face-id-apples-new-facial-recognition-tech-explained.html (accessed February 2018).
21. Hendry, J. (2017) 'How the DTA plans to manage your digital identity', *itnews*, 16th November, available at: https://www.itnews.com.au/news/how-the-dta-plans-to-manage-your-digital-identity-477751 (accessed February 2018).

22. Trade Me (2017) 'Transparency Report', available at: https://www.trademe.co.nz/trust-safety/2017/7/25/transparency-2017-1/ (accessed February 2018).
23. See: https://tresorit.com/.
24. See: https://www.startpage.com/.
25. See: https://wire.com/en/.
26. The Federal Trade Commission's first enforcement outcome against a connected toy manufacturer came out early this year against Vtech Electronics. See: https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated (accessed February 2018).
27. Roberts, J. (2017) 'Is your smart TV spying on you?', *Trusted Reviews*, 8th February, available at: http://www.trustedreviews.com/news/smart-tv-privacy-problems-vizio-samsung-lg-sony-panasonic-2952175 (accessed February 2018).
28. Grenoble, R. (2016) 'Uber knows when your iPhone battery is dying and you're getting desperate', *Huffington Post*, 21st May, available at: https://www.huffingtonpost.com/entry/uber-surge-pricing-battery-life_us_573f2057e4b0613b512a0130 (accessed February 2018).
29. Grubb, B. (2017) 'Thousands of Australians affected by Uber hack cover-up', *The Sydney Morning Herald*, 22nd November, available at: http://www.smh.com.au/technology/consumer-security/thousands-of-australians-affected-by-uber-hack-coverup-20171122-gzqmhj.html (accessed February 2018).
30. Stempel, J. (2017) 'Bose headphones spy on listeners: Lawsuit', *Reuters*, 20th April, available at: https://www.reuters.com/article/us-bose-lawsuit/bose-headphones-spy-on-listeners-lawsuit-idUSKBN17L2BT (accessed February 2018) and Davies, W. (2017) 'Bose urges judge to dismiss privacy law suit', *Digital News Daily*, 4th August, available at: https://www.mediapost.com/publications/article/305378/bose-urges-judge-to-dismiss-privacy-lawsuit.html (accessed February 2018).
31. Information Integrity Solutions and KPMG (August 2012) 'Independent review of ACC's privacy and security of information', available at: https://www.iispartners.com/s/22-August-2012-ACC-Independent-Review-FINAL-REPORT.pdf (accessed February 2018).
32. New Zealand Privacy Maturity Assessment Framework, available at: https://www.ict.govt.nz/assets/Guidance-and-Resources/Privacy-Framework-August-online.pdf (accessed February 2018).
33. World Economic Forum (2018) 'Global Risks Report 2018', available at: https://www.weforum.org/reports/the-global-risks-report-2018 (accessed February 2018).
34. Hodges, C. and Steinholtz, R. (2017) 'Ethical Business Practice and Regulation', Hart Publishing, CH Beck and Nomos, UK.
35. Privacy Commissioner New Zealand (2017) 'Making a trust mark for privacy', available at: https://www.privacy.org.nz/news-and-publications/statements-media-releases/making-a-trust-mark-for-privacy/ (accessed February 2018).