Justice vs Control in Cloud Computing: A Conceptual Framework for Positioning a Cloud Service Provider's Privacy Orientation

Valerie Lyons

Abstract The continued rise in frequency and magnitude of cloud-based privacy breaches brings to the fore the challenges experienced by cloud service providers (CSPs) in balancing the need to maximize profit with the need to maintain data privacy. With a backdrop of the ineffectiveness of regulatory approaches to protecting privacy, this chapter explores privacy from a non-regulatory perspective—instead exploring a CSP's approach to privacy as dynamics of control and justice. We apply control theory to represent the CSP's compliance with privacy legislation and power over data, and we apply justice theory to represent the CSP exceeding compliance. Control theories, such as social contract theory, have frequently

V. Lyons (✉)
The Linc Centre, BH Consulting, Blanchardstown Technology University,
Dublin, Ireland
e-mail: valerie.lyons3@mail.dcu.ie

been applied to explore privacy challenges between organizations and consumers, as too have justice theories e.g. procedural and distributive justice. However, few studies have combined these theoretical concepts to provide a balanced view of these tensions in the cloud computing landscape. Integrating concepts from these theories, we construct a framework that can help to explain and position a CSP's privacy orientation. Four key privacy orientations emerge in our framework, namely: Risk Managers, Integrators, Citizens and Warriors. We discuss the implications of each privacy orientation for CSPs. Our framework will enable future research to further understand, explore and compare the impact and effectiveness of each privacy orientation.

Keywords Cloud computing • Data privacy • Data protection • Control theories • Justice theories • Procedural justice • Distributive justice

5.1 INTRODUCTION

The high cost of maintaining internal IT systems that are scalable, robust, and fast enough to keep pace with the speed of business, has ushered in the era of cloud computing services. Global cloud market revenues are predicted to increase from US\$180b in 2015 to US\$390b in 2020, attaining 17% annual average growth (Forbes 2017). All indicators for the growth of cloud computing, such as data traffic, the number of data centers or the amount of cloud service providers (CSPs) are also predicted to grow exponentially (Cisco 2018a). Whether applied to enterprise management systems, email systems or mobile computing, cloud computing both increases efficiency and reduces information technology costs by allowing on-demand access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort (Mell and Grance 2011). However, although cloud computing's benefits are tremendous, security and privacy concerns continue to be the primary obstacles to wide adoption (CSA 2009).

Cloud computing presents particularly challenging issues for privacy as it involves the dispersal of data across servers in geographically dispersed locations that often cross national and legislative boundaries, together

with shared use of resources, making privacy incidents difficult to determine and detect (Ren et al. 2012). This was evidenced by a recent case in 2019, when Rubrik, the cloud data management giant, exposed a large cache of customer information improperly stored in an Amazon Elasticsearch database (Techcrunch 2019). With the rise in high-profile privacy incidents, such as Cambridge Analytica in 2018, and Capital One's data breach on AWS (Fortune 2019), cloud service customers (CSCs) have also become more aware of the potential risks associated with the processing of data outside the traditional on-premise models. There are additional tensions arising from the costs of detection, prevention and/or remediation of privacy incidents versus the value that can be derived from data services (Acquisti 2008; Chen et al. 2012).

Governments, regulators and policymakers respond to such incidents by enhancing the specificity and stringency of compliance regulation, however the pace of change in cloud computing and the exponential growth in data is fast outpacing the legislative lifecycle. Instead of focusing on regulation as a response, focusing on privacy from a non-regulatory perspective may yield more sustainable solutions for CSPs to address the balance of these tensions more effectively. Reflecting this—in this chapter, we draw on control theories of privacy (Fried 1984; Moor 1997) to explain how CSPs comply with privacy law and exact power over data and systems, and we draw on theories of procedural justice (Allan and Tyler 1988) to explain how CSPs can 'loosen the leash' to enable the CSC have more control.

It would be highly complex to map cloud computing issues across the full panoply of regulatory privacy architectures, such as the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR), the United Nations Declaration of Human Rights (UDHR), the Health Insurance Portability and Accountability Act (HIPAA) etc. However, given the broad reach of GDPR (it jurisdictionally applies to all EU CSPs, and to any non-EU CSP processing data of EU residents, or to any data processing within an EU territory) and its position as the strongest data protection regime in the world (Consumers-International 2019), we focus on GDPR in this chapter as the common reference for privacy regulation.

Applying these concepts of control and justice to privacy, we present a proposed privacy orientation framework describing the key privacy orientations of CSPs. This framework can help explain different approaches to privacy, and to understand their implications. Our framework extends

research from Greenaway et al. (2015) to posit a new dimension to privacy orientations, which we call the Philanthropic Privacy dimension, where organizations undertake privacy activities with the aim of resolving privacy as a social issue. This privacy dimension is important, as organizations taking actions beyond their corporate obligations have been found to experience less privacy incidents (Accenture and Ponemon 2015).

The remainder of this chapter is organized as follows: in the next section we discuss the tensions arising from privacy, through the lens of control and justice. Following that section, we provide a brief overview of privacy risks in the CSP environment and outline the boundaries of privacy responsibilities within cloud computing models. We subsequently describe the development of our privacy orientation framework. We conclude this chapter with proposals for application of the framework and suggestions for further research.

5.2 PRIVACY AS A CONTROL OR JUSTICE BEHAVIOR

Dinev (2014) suggests that societal discourse has come to equate privacy and information privacy, so the terms are used here interchangeably. Information privacy is frequently described as a multidimensional concept that is dependent on context (Culnan and Williams 2009; Xu et al. 2012). The multiple dimensions affecting privacy being harm, protection, provision, and scope (Mulligan et al. 2016) and the facets shaping context being information sensitivity, industry sector, political sector and technological applications (Smith et al. 2011).

For over two decades, theories of control or theories of justice have been used to explore privacy challenges. Control theories, such as social contract theory, have frequently been applied to explore privacy challenges between organizations and consumers (Martin 2012, 2016; Wright and Xie 2019) as too have justice theories e.g. procedural and distributive justice (Ashworth and Free 2006; Culnan and Armstrong 1999). However, with the exception of Greenaway et al. (2015) no other study has combined these theoretical concepts to provide a balanced view of the privacy tensions arising between CSPs and CSCs.

5.2.1 *Privacy as Control*

While there is no single concept of information privacy that crosses all disciplines (Smith et al. 2011) ‘control over personal information’ is a

common theme across many privacy studies (Belanger and Crossler 2011; Belanger et al. 2002). Control can refer to the ‘controls’ used to manage privacy (Belanger et al. 2002) or refer to the dynamic of ‘power’ over data (Johnson 2009). Both CSCs and CSPs implement ‘controls’ to manage privacy (Belanger et al. 2002) in the form of privacy enhancing tools, network access controls, authorization and authentication controls, privileged identity management controls etc. When privacy controls fail, a privacy incident is said to occur (a privacy incident is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where an authorized user accesses or potentially accesses personal information (DHS 2017, p. 8)). Johnson (2009) on the other hand refers to control as an organization’s need for power over information, while the consumer has to balance the good achieved through information processing against their need for privacy.

Providing the CSC with increased control over their data can result in the CSP not being able to maximize data storage efficiency, require the implementation of costly technical tools by the CSP, or necessitate costly legal indemnification of risk away from the CSP. Greenaway et al. (2015) describe this tension as the pursuit of interests such as profitability or market share, at the expense of those who provide information or pay for a service. This need for a CSP to dominate control is enshrined in the concept of information ownership, and it is this concept of control and power that we apply in this chapter, as reflected by Xu et al. (2012) who distinguish privacy control between individual and organization, with the organization increasingly becoming the ‘control agent’.

However, privacy is not solely about control but also about information being authorized to flow to specific agents at specific times (Moor 1997). Moor (1997) argues that in a highly digital culture it is simply not possible to control all information. Therefore, he argues, the best way to protect privacy is to ensure the right people have access to relevant information at the right time, giving individuals as much control over their data as realistically possible (labelling his theory the “control/restricted access” theory of privacy). With the emerging complexity of organizational networks, such as those constructed by CSPs, such levels of control are not realistically possible. Greenaway et al. (2015) classify organizations who provide little control to their consumers as ‘low control’. However, aligning to the concepts of control that we draw on in this paper, we would classify these organizations as ‘high control’, as they essentially dominate ‘power’ over the consumers’ information.

5.2.2 *Privacy as Justice*

The power-responsibility equilibrium (PRE) model, developed by Davis et al. (1980), states that power (which Lacznia and Murphy (1993) define as ‘the ability to control’) should be in equilibrium, where the partner with more power also has the responsibility to ensure an environment of trust and confidence. If an organization chooses a strategy of great power and less responsibility, it might benefit in the short-term but will lose control in the long-term e.g. from increased regulation (Caudill and Murphy 2000). Organizations can re-balance the control-equilibrium by returning a level of control to the consumer. For instance, in 2019, Apple updated its privacy website with a revised declaration of the company’s position on privacy.¹ This included a new section titled ‘*Control*’ with a subsection titled ‘*Take Charge of Your Data*’ which outlines:

To give you more control over your personal information, we are rolling out a set of dedicated privacy management tools.

This relinquishing of control by an organization is enshrined in the concept of information stewardship. Information stewardship implies that no matter what an organization does with stakeholders’ information (for example, selling it to third parties) the organization always remains responsible and retains oversight of the processing of that information (Rosenbaum 2010). Apple offer opportunities to their consumers that return a level of transparency and control to the consumer—by providing clear and simple explanations of what privacy options are available and how to implement them—they provide opportunities to their consumers that score highly on the Fair Information Practice Principles (FIPPs) scales. The principles of FIPPs are transparency, preference, purpose, minimization, limitation, quality, integrity, security, and accountability (DHS 2008, p. 4). Information privacy and FIPPs have been linked to procedural justice (Culnan and Bies 2003), where an organization’s control over personal information is noted as ‘just’ when the information owner is vested with the key principles of FIPPs (Culnan and Bies 2003; Greenaway et al. 2015). Organizations demonstrating behaviors that exceed compliance obligations to protect information entrusted to them, view themselves as information stewards rather than information owners and

¹ <https://www.macstories.net/news/apple-reveals-major-update-to-its-privacy-webpage/>

demonstrate a ‘culture of caring’ with regard to privacy (Accenture and Ponemon 2015). These types of organizations have also been found to experience less privacy incidents (Accenture and Ponemon 2015).

5.3 PRIVACY AND CLOUD COMPUTING

Although cloud computing enables reduced start-up costs, reduced operating costs and increased agility, its architectural features also raise various privacy concerns which are shared across several key stakeholders (Takabi et al. 2010) such as the CSP, the CSC, the consumer/data subject and application developers. Organizations are increasingly concerned about the risks of storing their data and applications on systems that reside outside of their on-premise data centres (Chen et al. 2010). ENISA (2009) define these risks as:

- privacy risks for the CSC e.g. non-compliance to enterprise policies and legislation, loss of reputation and credibility and being forced or persuaded to be tracked, or give personal information against their will (e.g. by governments)
- privacy risks for implementers of cloud platforms e.g. exposure of sensitive information stored on the platforms (potentially for fraudulent purposes), legal liability, loss of reputation and credibility, lack of user trust and take-up
- privacy risks for providers of applications on top of cloud platforms e.g. legal noncompliance, loss of reputation, ‘function creep’ using the personal information stored on the cloud, i.e. it might be used for purposes other than the original cloud intention
- privacy risks for the data subject e.g. exposure of personal information

However, unlike the traditional on-premise model of computing, responsibility for these privacy risks in the cloud computing model is shared between the CSC and the CSP, and the balance between the two responsibilities changes between cloud service models. This relationship is known as the shared responsibility model, and it is the basis for how modern cloud security and privacy operates with each service model differing in the amount of control offered to the CSC (Tripwire 2018). Haeberlen (2010) describes how different cloud service models affect the ways that privacy responsibilities are shared between CSPs and CSCs:

- IaaS—the CSP is responsible for the implementation and management of privacy controls only within the physical infrastructure. The CSC is responsible for all other aspects of privacy.
- PaaS—the CSP is responsible for IaaS. However, CSCs and CSPs are jointly responsible for ensuring appropriate privacy controls are implemented within the applications deployed on the PaaS environment.
- SaaS—the CSC has limited control over privacy and security. CSCs will generally maintain responsibility for managing identity and access management controls to ensure minimum permissions are assigned to roles. The CSP is responsible for ensuring all other privacy controls are in place.

As a CSC moves from on-premise models to cloud service models, they lose control over their data, including control over the privacy of that data. Although the shared responsibilities model assumes a level of transparency and control for the CSC, CSPs have traditionally lacked transparency regarding their privacy policies, strategy, service, thresholds etc. making it difficult for CSCs to objectively perform evaluations and risk assessments for a CSP service (Cruzes and Jaatun 2015). The implementation of ethical principles such as those in FIPPs not only mitigate the key privacy risks associated with cloud computing (Pearson 2009) but also offer the CSP an opportunity to rebalance the control-justice equilibrium for the CSC.

Many CSPs including Amazon, Microsoft, and IBM do offer simple breakdowns of performance metrics and responsibilities etc. However, some CSPs (e.g. SAAS model CSPs such as Salesforce or Workday) do not clearly define these sufficiently (Prüfer 2018). In a recent survey of IT decision makers (Netapp 2016) 35% believed responsibility for data sits with the CSPs, while 3% did not know who would be responsible. GDPR is very clear that responsibility for personal data lies firmly with the data controller (GDPR, Article 24). Under GDPR, the CSC is responsible (regardless of cloud computing model) for ensuring their own compliance requirements are handled effectively by the CSP and ensuring these requirements are adequately reflected in legally binding contractual agreements (called Data Processing Agreements, or DPAs) with the CSP. However, if a CSP is not transparent for instance, about which core IT services they themselves outsource to sub-processors, the CSC is unable to properly evaluate risks. In some cases, it may be difficult for the CSC (in its role as data controller) to assess the adequacy of the CSP's data

handling practices to ensure that their data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data e.g. between federated clouds. This lack of transparency is linked to decreased levels of trust in the CSP, is a key barrier for the adoption of cloud services (Del Alamo et al. 2015) and is associated with lack of accountability (Pearson 2009; Haeberlen 2010).

Finally, CSCs often overlook the on-premise privacy measures that traditional applications rely on such as on-premise firewall configurations that block logins from specific locations (such as embargoed countries), intrusion prevention systems, behavior analytics platforms (detecting insider threats), log management and alerting solutions (Oracle 2017). Since these and other measures protect privacy in applications in the enterprise campus, they are often taken for granted in the context of any one particular application and the responsibility for their installation and upkeep falls squarely on the CSC (Oracle 2017).

Alongside issues of transparency, responsibility and accountability, Abed and Chavan (2019) highlight a number of universal privacy issues facing CSCs, when considering cloud computing adoption, namely; the institutional obligation for disclosure (to governments), breach and incident disclosure, data accessibility and retention, and physical storage location):

- Institutional obligation for disclosure to Governments: Studies have shown that CSCs considering cloud adoption are concerned that data outsourced to the CSP can be accessed by others, notably public authorities with legitimate or illegitimate objectives as well as legal and illegal private actors (August et al. 2014). For instance in 2018, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act, House of Representatives Bill 4943, 2018) enabled law enforcement agencies to access data processed by US-based companies, regardless of whether the servers were located in the US.
- Breach and incident disclosure: GDPR mandates that a privacy incident/breach be reported within 72 hours of its discovery. However, when the privacy incident/breach occurs in the CSP environment, it is very difficult for the CSC to have transparent discovery and disclosure arrangements in place. The breach disclosure requirements are defined under Article 28 of the GDPR and need to be incorporated into the DPA with the CSP. This contract also needs to clearly define the balance of liability in the event of a data breach.

- Data accessibility and retention: Guaranteeing availability of cloud data when migrating from one CSP to another has become a primary concern for CSCs (Xue et al. 2017). In the CSP environment, personal data accessibility, retention and deletion become fundamental requirements to prevent CSCs being ‘locked in’ to a given CSP.
- Physical Storage Location: CSPs may store data in multiple geographically dispersed jurisdictional locations. Often this presents a challenge to identify which legislation takes precedence where laws conflict, particularly where there is conflict between the laws applying to the physical location of a CSP data centre and the physical location of the CSC (Abed and Chavan 2019).

5.4 THE PRIVACY ORIENTATION FRAMEWORK

In the early years of privacy, organizations understood their responsibilities toward privacy to be legal and financial responsibilities. In the 70’s discretionary frameworks such as FIPPs emerged—combining privacy standards with due process, consumer rights, and equality protections (Westin 2003). From the turn of the century Westin (2003) suggests that privacy became a first-level social and political issue in response to 9/11, the Internet, the cell phone, the human genome project, data mining, automation of government public records amongst others. In the last decade organizations began to respond to these fundamental changes to concern for privacy, with initiatives that exceeded their legal, financial and ethical responsibilities—ranging from privacy-by-design standards, developing open privacy standards, to collaborating with privacy advocacy groups. Given their association with justice and improved privacy protection, our framework was concerned with those privacy behaviors exceeding legislation. Much of the literature investigating privacy beyond legislation (Pollach 2011; Allen and Peloza 2015) explored privacy as a Corporate Social Responsibility (CSR). McWilliams and Siegel (2001) define CSR as those actions that appear to further some social good, beyond the interests of the organization and ‘beyond that which is required by law’.

Carroll’s model of CSR is the most commonly known model for CSR (Visser 2006). Carroll (1979) identified four pillars of CSR (financial responsibilities, legal responsibilities, ethical responsibilities, and philanthropic responsibilities). Privacy is a financial responsibility as organizations can be fined significant sums of money for non-compliance. Privacy

is also a legal responsibility as privacy legislation (e.g. the California Consumer Privacy Act (CCPA) or the GDPR) mandates strict governance over the processing of personal data. Carroll (1998) suggested that privacy not only is a legal and financial responsibility but is also an ethical responsibility, as legislation lags behind ethics, and morality comes into play. Privacy also meets Mason's (1995) test of what constitutes an ethical problem i.e. whenever one party in pursuit of its goals engages in behavior that materially affects the ability of another party to pursue its goals. In 2018, the then EU Data Protection Supervisor (Giovanni Buttarelli) argued that in order to address this ethical component of privacy, organizations should not overly rely on bare compliance with the letter of law, and should adopt a 'duty of care' for consumer data (Buttarelli 2018). CSR activities are most appropriate where existing legislation requires compliance with the spirit as well as the letter of the law and where the organization can fool stakeholders through superior knowledge (Mintzberg 1983).

Finally, privacy can be described as a philanthropic responsibility, where an organization's privacy behaviors demonstrate a 'duty of care' (Buttarelli 2018) towards data owners and society that exceeds compliance. Philanthropy presents itself in many forms e.g. cash contributions or employee commitments (Smith 1994) and is often explained by social exchange theory (Emerson 1962) where corporations use philanthropy to expand the scope of their business initiatives, influence governments, and position themselves as influential leaders (Jung et al. 2016). Both Husted (2003) and Stannard-Stockton (2011) suggest three classifications of philanthropy; (1) "check-book philanthropy" i.e. making cash contributions to a cause; (2) in-house projects and philanthropic investments; (3) strategic philanthropic collaboration between organizations and non-corporate partners. True philanthropy matches the resources of the giver with the needs of the recipient through a socially beneficial relation that is mobilized and governed by a force of morally armed entreaty (Schervish 1998).

As we could find no reference in the literature to philanthropic privacy, based on definitions of CSR from McWilliams and Siegel (2001) we describe it as: *'Any privacy behavior(s) exceeding legislative requirements, that furthers privacy as a societal good, beyond the interests of the organization'*. Philanthropic privacy behaviors would therefore include behaviors such as advising on government policy, developing open privacy standards or tools, exceeding privacy laws for employees, even lobbying for strengthened privacy on behalf of the consumer or society. Whilst traditional

lobbying often aims at shaping rules for privacy in the best interest of the organization, some organizations may try to shape the rules in a way that favors society's needs for privacy. The inclusion of the philanthropic dimension is important, as organizations taking privacy actions beyond their corporate obligations have been found to experience less privacy incidents (Accenture and Ponemon 2015). It therefore seems reasonable to suggest that the philanthropic privacy dimension may help identify privacy behaviors that could help strengthen privacy protection effectiveness.

Although privacy behaviors 'beyond that which is required by law' may demonstrate the differentiating behaviors of justice that this chapter is keen to explore, it is important to highlight that this concept of 'beyond that which is required by law' differs from one jurisdiction to another. For instance, the GDPR mandates that organizations provide transparency, choice, purpose and notice to the data subject. Many other jurisdictions, particular large sectors of the US, do not mandate the provision of these privacy behaviors through regulation but through industry self-regulation and discretionary codes such as FIPPs. Thus, choice for example, would be considered a legal requirement within GDPR, and in certain US contexts an ethical requirement. This is an important consideration for any future application of our framework, as an evaluation of the local privacy landscape for a given organization would first be required, in order to determine their legal minimums.

5.4.1 *Framework Dimensions*

Greenaway et al. (2015), combine control and justice theory to form a privacy orientation which they call Company Information Privacy Orientation (CIPO). Their research forms the starting point for the construction of the privacy orientation framework we develop in this chapter. Greenaway et al. (2015) suggest that an organization's privacy orientation is founded on three dimensions namely: information management (i.e. how an organization uses information for profit), legal and ethical dimensions. These three dimensions are underpinned by several theoretical components: stakeholder theory, stockholder theory, social contract theory, information processing theory and cognitive categorization theory (Greenaway et al. 2015). Through triangulation of their three CIPO dimensions with the four pillars of CSR from Carroll's (1979) CSR pyramid of responsibilities (economic, legal, ethical, and philanthropic), we extend the CIPO framework with the addition of the philanthropic

dimension. Triangulation enables a systematic search for convergence among sources of information to form new or revised themes/categories representing the state of knowledge for a given subject (Denzin 1978; Yardley 2008). See Table 5.1 for the Privacy Orientation Framework

Table 5.1 Privacy orientation framework dimensions including philanthropy

<i>Dimensions</i>	<i>Definition</i>	<i>Theory base</i>	<i>Attribute range</i>	<i>Behavior definition</i>
Philanthropic responsibilities	The firms contributions to society	Social exchange theory (Emerson 1962). CSR theories (Carroll 1998). Triple bottom line theory of CSR (Savitz 2013).	Checkbook philanthropy	Paying for charitable events or activities that promote privacy, outside of the organisation.
			Inhouse Projects	Participation in groups/activities aimed at supporting privacy for employees or extended supply chain.
			Strategic Collaboration	Participating in groups/activities aimed at supporting privacy for consumers, society, humanity.
Ethical responsibilities	The firms' obligations to its consumers	Ethical theories: Smith and Hasnas (1999). Social contract theory (Beauchamp and Bowie 1993; Donaldson and Dunfee 1999).	Stockholder theory	Consumers are obligated to protect themselves in transaction with the firm
			Stakeholder theory	Firm and consumer share responsibility for consumer wellbeing
			Social contract theory	Firm obligated to promote consumer wellbeing.

(continued)

Table 5.1 (continued)

<i>Dimensions</i>	<i>Definition</i>	<i>Theory base</i>	<i>Attribute range</i>	<i>Behavior definition</i>
Information management/ financial responsibilities	The firm’s purpose for gathering and using information—how it intends to make profit	Information processing theory (Tushman and Nadler 1978) as used by Brohman et al. (2003)	Transaction focused	Consumer focused transaction data collected for short term efficiency
			Data focused	Consumer data collected from various sources to improve profitability
			Inference focused	Consumer profiles created from historic/ preference data: cross-sell & up-sell
Legal and risk responsibilities	The firm’s view of the impact that privacy laws have on its ability to carry out business	Cognitive categorisation theory (Rosch 1978) as used by Jackson and Dutton (1988)	Advice focussed	Consumer profiles created from historic, preference, aspirational data to create profitable sustainable relationships
			No threat no opportunity	Firms lack awareness or concern for privacy laws
			Threat	Privacy laws viewed as constraint to maximize shareholder value
			Threat and Opportunity	Privacy laws viewed as required to ensure ongoing transactions with consumers
			Opportunity	Privacy laws embraced as strategic differentiation

Adapted and extended from Greenaway et al. (2015)

dimensions, adapted from the Greenaway et al. (2015) CIPO framework, extended to include details for the Philanthropic dimension.

A CSP may demonstrate a combination of both control-based behaviors and justice-based behaviors in varying levels. We therefore position control and justice as two continua, where four privacy orientations emerge, namely; ‘low-justice, low-control’ orientations (we call CSPs in this orientation ‘Compliers’); ‘low-justice, high-control’ (we call CSPs in this orientation ‘Integrators’); ‘high-justice, high-control’ (we call CSPs in this orientation ‘Citizens’); and ‘high-justice, low-control’ (we call CSPs in this orientation ‘Warriors’). We summarize our privacy orientation framework below in Fig. 5.1.

5.4.1.1 *Compliers*

Complier CSPs focus on privacy risk mitigation. CSPs in this orientation demonstrate privacy behaviors that measure low on justice and low on control. This orientation sets compliance as the goal, with privacy governance assigned to functional management. Their privacy policies and

Fig. 5.1 Privacy orientations framework

practices are often centred on compliance with laws and industry standards. These organizations report little more than privacy metrics mandated by privacy. They may undertake lobbying towards privacy but only where beneficial to the organization. They have no real philanthropic perspective with regard to privacy. Compliers tend to provide rudimentary transactional services (for instance Cloudways and Digital Ocean). They will typically offer security and privacy features at an additional cost, or like Amazon AWS, allow the CSC to reconfigure private buckets to be non-private. Risk-Managers rarely exceed legislative minimums.

In 2019, Capital One (using AWS as their CSP) suffered a breach impacting 100 m customers' financial data including social security numbers (Business Insider 2019). The AWS server used by Capital One was vulnerable to a well-known attack (called server-side request forgery [SSRF]). AWS denied liability (as their contracts indemnified them) however—without being legally required to do so, AWS's largest competitors (Google and Microsoft) had already addressed the threat of SSRF attacks two years previously.²

5.4.1.2 *Integrators*

Integrator CSPs offer robust compliance to privacy legislation whilst integrating society's increasing expectations to address privacy as a social responsibility. CSPs in this privacy orientation demonstrate privacy behaviors that measure low on justice and high on control. Relinquishing control (by offering increased justice behaviors) to their CSCs is not important to these organizations, as they require widespread access to data and systems in order to minimize costs and maximize profit. CSPs in this orientation may actively reflect on ways they can use social issues such as privacy to gain competitive advantage. For instance, privacy rights for employees, their families, and local communities may be supported. The CSPs objective in this orientation is to mitigate the erosion of economic value in the medium term and to achieve longer-term gains by integrating responsible privacy practices into their daily operations (Zadek 2004). These CSPs not only want to monetize their cloud service, but they also want to maximize data value. Although CSPs in this orientation may appear to demonstrate philanthropic privacy—for example by producing white papers, open

² <https://www.wyden.senate.gov/imo/media/doc/102419%20Wyden%20Warren%20Letter%20to%20FTC%20RE%20Amazon%20Capital%20One%20Hack.pdf>

standards, open tools etc. this philanthropy towards privacy is not always a ‘felt’ value.

For instance, Google Cloud’s published privacy commitments (Google 2020) state that “*we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud*”. Yet in 2019, Google were fined €50m by the French data protection authority for lack of transparency in their privacy policies (CNIL 2019).

5.4.1.3 Citizens

Citizen CSPs assume a citizenship role, leading privacy issues and transforming their business models to achieve this objective. Citizen CSPs demonstrate privacy behaviors that measure high on justice and high on control. They openly acknowledge their new roles and responsibilities towards society, and recognize how responsibilities towards private, public, and social sectors have become interdependent (Latapi-Agudelo et al. 2019). The Citizen orientation addresses privacy strategically, where privacy programs are focused on building and maintaining sustainable relationships, and often exceed legislative obligations. These organizations incorporate privacy as a value held strongly by the organization, associating their privacy behaviors with other strong values such as trust and integrity (Mirvis and Googins 2006). CSPs in the Citizen privacy orientation broaden their agenda by expanding their privacy concerns and deepen the involvement of top management in the leadership addressing privacy issues. Organizations form long-term alliance and partnerships with stakeholders in order to drive change in privacy issues. Caldwell et al. (2010) refer to this leadership as a ‘stewardship role’ which generates commitment from other stakeholders and organizations in order to drive change in several key privacy issues. CSPs in this orientation consider privacy to be a compliance obligation however they also consider privacy to be strategic, where privacy is used to build and maintain sustainable relationships, and often exceeds legal minimums—reflecting philanthropic privacy.

Microsoft for instance established an online trust centre to respond to queries on privacy for all its products, particularly on Office 365. They also provide tools to simplify responding to Subject Access Requests mandated by GDPR (Microsoft 2018a). Microsoft has also extended the rights available to Europeans under the GDPR, to all its consumers, noting that “*GDPR establishes important principles that are relevant globally*”

(Microsoft 2018b). IBM, as another example, were among the first companies to sign the EU Data Protection Code of Conduct for Cloud Service Providers (IBM 2017).

5.4.1.4 Warriors

Warrior CSPs highlight privacy as a societal issue and may even revolt against laws in order to support it. CSPs who are positioned in this orientation demonstrate privacy behaviors that measure high on justice, however unlike those of the Citizen, their behaviors may also measure low on control. In terms of philanthropic privacy, Warrior CSPs may lobby government for increased privacy for individuals, knowing it will increase organizational costs, reduce shareholder returns and/or marginalize certain stakeholders. They may stake claims to privacy, to such a degree that they will breach laws if they feel that those laws compromise social or democratic freedoms.

Apple for example, in 2015 and 2016, refused to comply with, and challenged, at least 12 orders issued by the FBI compelling Apple to enable decryption of phones involved in criminal investigations and prosecutions. It could be argued that Apple monetize ‘privacy’ as part of their brand, however in the US they did not garner widespread support for their decision and at that time 51% of American smartphone users were against Apple’s decision, while only 38% supported Apples stance (Pew 2016). Warriors may demonstrate less control than those in the Citizen orientation, however in its place they introduce strong privacy governance and accountability structures. In Apple for instance, any collection of customer data requires sign-off from a committee of three “privacy czars” and a top executive (Reuters 2016).

Cisco, as another example, recognized that their systems could be used in a manner contrary to their values and state “*Cisco technologies are used by government agencies to promote public safety, but the same technology can be used for surveillance that would violate individuals’ privacy*”. (Cisco 2018c). Cisco issued a position statement opposing government backdoors and opposing attempts to prohibit public disclosure about new surveillance capabilities demanded by governments (Cisco 2018b). Cisco therefore retain a high level of control to ensure that their product cannot be misused but also balance this control with a commitment to “*build our products on the open, global standards we believe are critical to overcoming*

censorship, protecting privacy, and keeping the world connected” (Cisco 2018c). Cisco also undertakes several philanthropic privacy activities such as the Cisco Privacy Maturity Benchmark Study and sponsoring the National Cybersecurity Alliance’s Data Privacy Day (Cisco 2018c).

5.5 CONCLUSION

Researchers, practitioners, and policymakers need a better understanding of how and why organizations differ in their treatment of consumer privacy. Belanger and Xu (2015) advocate that privacy researchers conduct qualitative interpretive research about relationships between privacy antecedents and outcomes. Using this framework, such research could be achieved by categorizing and weighing levels of control and justice demonstrated by a CSP’s privacy behaviors and positioning them as one of the four orientations in the framework. The framework also presents opportunities for such future research to empirically examine the effectiveness of one orientation over another, or the potential impact of an organization’s orientation on other variables such as privacy protection effectiveness, cybersecurity behaviors, or privacy strategies. The framework can also be applied in different contexts—comparing privacy orientations for CSPs in different countries, of different sizes, or with different market dependencies on data.

Being able to position a CSP’s privacy orientation allows the CSP to establish baselines within their industry and to determine if certain orientations provide more robust security and privacy protection, where privacy incidents may be reduced. At the same time, the framework challenges CSPs to articulate their ethical, financial, legal, and philanthropic strategies. Moreover, identifying their privacy orientation will assist CSPs to better align their actual privacy programs with the CSCs top concerns (Chan 2003). If CSPs can use their privacy orientation to enhance and make more effective their privacy provisions, then the wider stakeholder community, particularly the CSC, and ultimately the data subject, may benefit. We hope the framework provides a helpful foundation for future theoretical and empirical work.

Acknowledgements This chapter and the work described therein was funded by the Irish Research Council’s Employment Based Post-graduate Scholarship programme.

REFERENCES

- Abed, Y., & Chavan, M. (2019). The Challenges of Institutional Distance: Data Privacy Issues in Cloud Computing. *Science, Technology and Society*, 24(1), 161–181. <https://doi.org/10.1177/0971721818806088>.
- Accenture and Ponemon. (2015). How Global Organizations Approach the Challenge of Protecting Personal Data. Retrieved June 2020, from http://www.ponemon.org/local/upload/file/ATC_DPP%20report_FINAL.pdf
- Acquisti, G. (2008). Identity Management, Privacy, and Price Discrimination. *IEEE Security and Privacy*, 6(1), 46–50. <https://doi.org/10.1109/MSP.2008.35>.
- Allan, L., & Tyler, T. (1988). *The Social Psychology of Procedural Justice*. Plenum Press New York.
- Allen, A., & Pelozo, J. (2015). Someone to Watch Over Me: The Integration of Privacy and Corporate Social Responsibility. *Business Horizons*, 58, 635–642. <https://doi.org/10.1016/j.bushor.2015.06.007>.
- Ashworth, L., & Free, C. (2006). Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers Online Privacy Concerns. *Journal of Business Ethics*, 67, 107–123.
- August, T., Niculescu, M., & Shin, H. (2014). Cloud Implications on Software Network Structure and Security Risks. *Information Systems Research*, 25(3), 489–510.
- Beauchamp, T., & Bowie, N. (1993). *Ethical Theory and Business*. Chambersburg, PA: Prentice Hall.
- Belanger, F., & Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35, 1017–1041.
- Belanger, F., Hiller, J., & Smith, W. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems*, 11, 245–270.
- Belanger, F., & Xu, H. (2015). The Role of Information Systems Research in Shaping the Future of Privacy. *Information System Journal*, 25, 573–578.
- Brohman, M., Watson, R., Piccoli, G., & Parasurama, A. (2003). Data Completeness: a Key to Effective Net-Based Customer Service Systems. *Communications of the ACM*, 46, 47–51.
- Business Insider. (2019). To Prevent Disasters like the Capital One Hack from Happening Again, Experts Say Amazon Web Services Could Do More to Protect Customers from Themselves. Retrieved from May 2020, from <https://www.businessinsider.com/capital-one-hack-amazon-aws-breach-security-analysts-2019-8?r=US&IR=T>
- Buttarelli, G. (2018). Interview with the European Data Protection Supervisor Giovanni Buttarelli: ‘The GDPR is a Radical Update to the Rulebook for the

- Digital Age'. Retrieved September 30, 2018, from <https://irishtechnews.ie/interview-with-the-european-data-protection-supervisor-giovanni-buttarelli-the-gdpr-is-a-radical-update-of-the-rule-book-for-the-digital-age/>
- Caldwell, C., Hayes, L., & Long, D. (2010). Leadership, Trustworthiness, and Ethical Stewardship. *Journal of Business Ethics*, 96(4), 497–512.
- Carroll, A. (1979). A Three Dimensional Conceptual Model of Corporate Performance. *Academy of Management Review*, 4, 497–505.
- Carroll, A. (1998). The Four Faces of Corporate Citizenship. *Business and Society Review*, 100, 1–7.
- Caudill, E., & Murphy, P. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing*, 19(1), 7–19.
- Chan, Y. (2003). Competing Through Information Privacy. In J. N. Luftman (Ed.), *Competing in the Information Age: Align in the Sand* (2nd ed., pp. 350–361). New York: Oxford University Press.
- Chen, H., Chiang, R., & Storey, V. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, 36, 1165–1188.
- Chen, Y., Paxson, V., & Katz, R. (2010). *What's New About Cloud Computing Security?* Tech. Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley. Retrieved June 2020, from www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html.
- Cisco. (2018a). Global Cloud Index White Paper. Retrieved June 2020, from <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html>
- Cisco. (2018b). Cisco Position Statement on Human Rights and Privacy. Retrieved June 2020, from <https://www.cisco.com/c/dam/assets/csr/pdf/Human-Rights-Position-Statements-2018.pdf>
- Cisco. (2018c). Cisco Corporate Social Responsibility Report. Retrieved May 2020, from <https://www.cisco.com/c/dam/assets/csr/pdf/CSR-Report-2018.pdf>
- CNIL. (2019). Commission Nationale D'Information Liberation. (The French Data Protection Supervisory Authority). Retrieved from <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>
- Consumers International. (2019). The State of Data Protection Rules Around the World: A Briefing for Consumer Organizations. Retrieved May 2020, from <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf>
- Cruzes, D., & Jaatun, M. (2015). *Cloud Provider Transparency—A View from Cloud Customers*. 5th International Conference on Cloud Computing and Services Science.
- CSA. (2009). Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. Retrieved May 2020, from <https://cloudsecurity-alliance.org/csaguide.pdf>

- Culnan, M., & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organizational Science*, 10, 104–115. <https://doi.org/10.1287/orsc.10.1.104>.
- Culnan, M., & Bies, R. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59, 323–342. <https://doi.org/10.1111/1540-4560.00067>.
- Culnan, M., & Williams, C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches. *MIS Quarterly*, 33, 673–687.
- Davis, K., Frederick, W., & Blomstrom, R. (1980). *Business and Society* (2nd ed.). New York, NY: McGraw-Hill.
- Del Alamo, J., Trapero, R., Martín, Y., & Yelmo, J. (2015). Assessing Privacy Capabilities of Cloud Service Providers. *IEEE Latin America Transactions*, 13(11), 3634–3641.
- Denzin, N. (1978). *Sociological Methods Sourcebook* (2nd ed.). NY: McGraw Hill.
- DHS. (2008). *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*. Memorandum Number: 2008-01. US Department of Homeland Security Privacy Office Publications. Retrieved April 2020, from https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
- DHS. (2017). *Handbook for Safeguarding Sensitive Personal Information*. Privacy Policy Directive 047-01-007, Revision 3. US Department of Homeland Security Privacy Office Publications. Retrieved April 2020, from <https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf>
- Dinev, T. (2014). Why Would We Care about Privacy? *European Journal of Information Systems*, 23, 97–102.
- Donaldson, T., & Dunfee, T. (1999). *Ties That Bind: A Social Contracts Approach to Business Ethics*. Boston, MA: Harvard Business School Press.
- Emerson, R. (1962). Power-Dependence Relations. *American Sociological Review*, 27(1), 31–41.
- ENISA. (2009). Cloud Computing: Benefits, Risks and Recommendations for Information Security, by Catteddu, D. and Hogben, G. Retrieved April 2020, from www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
- Forbes. (2017). Global Cloud Spending Predicted to Reach \$390b by 2020. Retrieved May 2020, from <https://www.forbes.com/sites/louiscolumbus/2017/02/11/global-cloud-spending-predicted-to-reach-390b-by-2020/#125897191085>
- Fortune. (2019). Capital One's Data Breach Could Cost the Company Up to \$500 Million. Retrieved May 2020, from <https://fortune.com/2019/07/31/capital-one-data-breach-2019-paige-thompson-settlement/>

- Fried, C. (1984). *Philosophical Dimensions of Privacy* (E. D. Schoeman, Ed., pp. 203–222). New York: Cambridge University Press.
- Google. (2020). Privacy on GoogleCloud. Retrieved May 2020, from <https://cloud.google.com/security/privacy>
- Greenaway, K., Chan, Y., & Crossler, R. (2015). Company Information Privacy Orientation. A Conceptual Framework. *Information Systems Journal*, 25, 579–606.
- Haeberlen, A. (2010). A Case for the Accountable Cloud. *SIGOPS Operating Systems Review*, 44(2), 52–57.
- Husted, B. (2003). Governance Choices for Corporate Social Responsibility: To Contribute, Collaborate or Internalize? *Long Range Planning*, 36(5), 481–498.
- IBM. (2017). IBM Among the First Companies to Sign EU Data Protection Code of Conduct for Cloud Service Providers. BlogPost by Christine Capella, CPO IBM. Retrieved May 2020, from <https://www.ibm.com/blogs/policy/eu-cloud-code-of-conduct/>.
- Jackson, S., & Dutton, J. (1988). Discerning Threats and Opportunities. *Administrative Science Quarterly*, 33(1), 370–387.
- Johnson, D. (2009). *Computer Ethics* (3rd ed.). Upper Saddle River, NJ: Pearson Education Inc. Retrieved May 2020, from <https://www.ibm.com/blogs/policy/eu-cloud-code-of-conduct/>
- Jung, T., Phillips, S., & Harrow, J. (2016). *The Routledge Companion to Philanthropy*. London, UK: Routledge Press.
- Laczniak, G., & Murphy, P. (1993). *Ethical Marketing Decisions: The Higher Road*. Boston: Allyn & Bacon.
- Latapi-Agudelo, M., Johannsdottir, L., & Davidsdottir, B. (2019). A Literature Review of the History and Evolution of Corporate Social Responsibility. *International Journal of Corporate Social Responsibility*, 4(1), 1–23.
- Martin, K. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. *Journal of Business Ethics*, 11(4), 519–539.
- Martin, K. (2016). Understanding privacy online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, 137(3), 551–569.
- Mason, R. (1995). Apply Ethics to Information Technology Issues. *Communications of the ACM*, 38, 55–57.
- McWilliams, A., & Siegel, D. (2001). Corporate Social Responsibility: A Theory of the Firm Perspective. *Academy of Management Review*, 26, 117–127.
- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. US National Institute of Science and Technology. Retrieved November 2019, from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Microsoft. (2018a). Microsoft Trust Centre GDPR Compliance. Retrieved from <https://www.microsoft.com/en-us/TrustCenter/CloudServices/office365/GDPR>
- Microsoft. (2018b). Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data. <https://blogs.microsoft.com/on->

- the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/
- Mintzberg, H. (1983). *Power In and Around Organizations*. Englewood Cliffs, NJ: Prentice-Hall.
- Mirvis, P., & Googins, B. (2006). Stages of Corporate Citizenship. *California Management Review*, 48(2), 104–126.
- Moor, J. (1997). Towards a Theory of Privacy in the Information Age. *Computers and Society*, 27, 27–32.
- Mulligan, D., Koopman, C., & Doty, N. (2016). Privacy is an Essentially Contested Concept: A Multi-dimensional Analytic for Mapping Privacy. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences*, 374(2083), 20160118.
- Netapp. (2016). Retrieved November 2019, from <https://www.netapp.co.uk/company/news/press-releases/news-rel-20160712-103195.aspx>
- Oracle. (2017). White Paper: “Making Sense of the Shared Responsibility Model”. Retrieved November 2019, from <http://www.oracle.com/us/solutions/cloud/platform-as-a-service/shared-responsibility-model-wp-3497462.pdf>
- Pearson, S. (2009). *Taking Account of Privacy When Designing Cloud Computing Services*. Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44–52.
- Pew. (2016). *More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone*. Pew Research Center for the People and the Press.
- Pollach, I. (2011). Online Privacy as a Corporate Social Responsibility: An Empirical Study. *Business Ethics: A European Review*, 20, 88–103.
- Prüfer, J. (2018). Trusting Privacy in the Cloud. *Information Economics and Policy*, 45, 52.
- Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. *IEEE Internet Computing*, 16(1), 69–73.
- Reuters. (2016). Apple Privacy Czars Grapple With Internal Conflict Over User Data. Retrieved October 2019, from <https://www.reuters.com/article/us-apple-encryption-privacy-insight-idUSKCN0WN0BO>
- Rosch, E. (1978). Principles of Categorization. In E. Rosch & B. Lloyd (Eds.), *Cognition and Categorization*. Lawrence Elbaum Associates. ISBN 0835734048, 9780835734042.
- Rosenbaum, S. (2010). Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access. *Health Services Research*, 45, 1442–1455.
- Savitz, A. (2013). *The Triple Bottom Line: How Today's Best-Run Companies Are Achieving Economic, Social and Environmental Success—and How You Can Too*. San Francisco, CA: Jossey-Bass Press.
- Schervish, P. (1998). Philanthropy. In R. Wuthnow (Ed.), *Encyclopaedia of Politics and Religions* (pp. 600–603). Washington, DC: Congressional Quarterly.

- Smith, C. (1994). The New Corporate Philanthropy. *Harvard Business Review*, 72(3), 105–116.
- Smith, H., Dinev, T., & Xu, H. (2011). Theory and Review of Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35, 989–1015.
- Smith, H., & Hasnas, J. (1999). Ethics and Information Systems: the Corporate Domain. *MIS Quarterly*, 23, 109–127.
- Stannard-Stockton, S. (2011). The Three Core Approaches to Effective Philanthropy. *Stanford Social Innovation Review*. Retrieved from https://ssir.org/articles/entry/the_three_core_approaches_to_effective_philanthropy#
- Takabi, H., Joshil, J., & Ahn, G. (2010). *Security and Privacy Challenges in Cloud Computing Environments*. IEEE Computer and Reliability Societies.
- Techcrunch. (2019). Data Management Giant Rubrik Leaked a Massive Database of Client Data. Retrieved May 2020, from <https://techcrunch.com/2019/01/29/rubrik-data-leak/>
- Tripwire. (2018). Cloud Security Shared Responsibility Model Explained. Retrieved September 2019, from <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/cloud-securitys-shared-responsibility-model-explained/>
- Tushman, M., & Nadler, D. (1978). Information Processing as an Integrating Concept in Organizational Design. *Academy of Management Review*, 3, 613–624.
- Visser, W. (2006). Revisiting Carroll's CSR Pyramid: An African Perspective. In E. Pedersen & M. Huniche (Eds.), *Corporate Citizenship in Developing Countries* (pp. 29–56). Copenhagen Business School Press.
- Westin, A. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), 431–453.
- Wright, S., & Xie, G. (2019). Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations. *Journal of Business Ethics*, 156(1), 123–140. <https://doi.org/10.1007/s10551-017-3553>.
- Xu, H., Tan, B., & Agarwal, R. (2012). Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research*, 23, 1342–1363.
- Xue, L., Ni, J., & Shen, J. (2017). Provable Data Transfer from Provable Data Possession and Deletion in Cloud Storage. *Journal of Computer Standards and Interfaces*, 54(1), 46–54.
- Yardley, L. (2008). Demonstrating the Validity of Qualitative Research. *The Journal of Positive Psychology*, 12, 295–296.
- Zadek, S. (2004). The Path to Corporate Responsibility. *Harvard Business Review*, 82(12), 125–132.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.