Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2022 Proceedings | Cybersecurity, Privacy and Ethics in AI

Dec 12th, 12:00 AM

Chief Privacy Officer Role and Organizational Transformation in the Digital Economy

Mazen Shawosh
King Fahd University of Petroleum & Minerals, mshawosh@kfupm.edu.sa

May Bantan
Nova Southeastern University, mb2627@mynsu.nova.edu

France Belanger
Virginia Polytechnic Institute and State University, belanger@vt.edu

Follow this and additional works at: https://aisel.aisnet.org/icis2022

Recommended Citation

Shawosh, Mazen; Bantan, May; and Belanger, France, "Chief Privacy Officer Role and Organizational Transformation in the Digital Economy" (2022). *ICIS 2022 Proceedings*. 15.
https://aisel.aisnet.org/icis2022/security/security/15

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Chief Privacy Officer Role and Organizational Transformation in the Digital Economy

Short Paper

Mazen Shawosh
Interdisciplinary Research Center for Finance & Digital Economy
KBS Business School, King Fahd University of Petroleum & Minerals
Dhahran, Saudi Arabia
mshawosh@kfupm.edu.sa

May Bantan
Nova Southeastern University
Saudi Electronic University
Medina, Saudi Arabia
bantanms@gmail.com

France Bélanger
Pamplin College of Business, Virginia Tech
Blacksburg, Virginia
belanger@vt.edu

Abstract

With increased digitalization and the evolving digital economy, consumers, regulating agencies, and business partners alike demand more transparency for organizational privacy practices, generating increased pressure on organizations to establish privacy programs and initiatives. The Chief Privacy Officer (CPO) role is central to the development of these privacy initiatives and is becoming more strategic. However, the role of the CPO appears to vary significantly across organizations. This study aims to investigate how an organization's privacy initiatives implementation influences the CPO role and understand how an organization needs to transform to support the emerging CPO roles in the digital economy. We present our initial findings and elaborate on a transformation model that shows the stages an organization follow to support the CPO role strategically.

Keywords: Chief privacy officer, Organizational information privacy, Organizational transformation, Digital economy

Introduction

With increased digitalization and the evolving digital economy, consumers, regulating agencies, and business partners alike demand more transparency for organizational privacy practices, generating increased pressure on organizations to establish (with varying structures) privacy initiatives. Organizational level studies on information privacy practices of organizations represent a significant stream of research that gained momentum with the rise of e-business and e-government, leading to abundant research analyzing website privacy policies (Bélanger and Crossler 2011; Xu et al. 2011), frameworks for organizational privacy practices (Greenaway et al. 2015; Greenaway and Chan 2013), and more recently privacy management architectures or models (Hajli et al. 2021; Wall et al. 2016). However, there remains limited empirical research trying to understand organizational information privacy management.

There are many options for organizations to implement a privacy program or initiative. Some initiatives are internally focused, looking at internal stakeholders and processes to ensure data and information privacy and security, or externally focused, either to avoid regulatory oversight or to improve relationships with external stakeholders (Greenaway and Chan 2013). As organizations develop their privacy initiative, one

role that has become central to these is the Chief Privacy Officer (CPO) (sometimes the Chief Information Privacy Officer). While initially the role of the CPO was often related to the protection of consumer privacy, whether representing compliance with internal policies or external laws and regulations (Sipior and Ward 2002), the CPO position is now often recognized to include risk management and protection of an organization's stakeholder interests (Bowcut 2022).

In the age of big data, large data breaches, the Internet of Things, and the interconnected world, the importance of managing and protecting an organization's data and information privacy is fairly evident. The role of the CPO in doing this, however, appears to vary significantly across organizations (Bamberger and Mulligan 2011; Greenaway et al. 2015; Kayworth et al. 2005); some organizations have no CPO supporting privacy initiatives; others have externally focused CPOs (Kayworth et al. 2005), and yet others have internally and compliance-focused CPOs (Sipior and Ward 2002). Clearly, the role of the CPO is relatively new in many organizations. Understanding which structure can better help address today's challenges for information privacy, this research seeks to answer the question of *How are the maturity of an organization's privacy programs shaped by and influence the nature of the CPO role??*

A vast literature in the management field explores how organizational structures, including reporting structures, control mechanisms, degree of centralization and integration, and collaboration structures, can serve as enablers or constraints in performing organizational work. Given the pervasiveness of data and information in organizations, and the need to manage these across various data owners (and stewards), we argue that these same structures within an organization can serve as enablers or constraints in allowing CPOs to perform their responsibilities towards both compliance and transparency. Therefore, the second question to be explored in this study is *What types of digital transformations occur when organizations develop and grow their CPO positions?*

To answer our research questions, we use a grounded theory approach and conduct a series of in-depth interviews with current CPOs in various organizations. Our analyses to date reveal the following. First, although some CPOs' work is visible to the C-suite and the Board, they are still not included as members of the top management and lack direct reporting to the CEO. CPO organizational structure in the form of direct reporting and membership in the TMT is important for CPO to push the privacy agenda in the organization. Second, the CPO role can include internal and external activities and responsibilities. Internal roles include compliance, training, and education of employees. External roles relate to enhancing relationships and trust with customers and partners. Third, organizations need to transform to facilitate the CPO role growth and strategically implement data and information practices. We propose a Privacy Implementation Maturity Model that depicts the stages of transformation towards increasingly strategic privacy initiatives and CPO role in organizations.

Methods

The current study examines the nature of the CPO role, how privacy initiatives implementation in organizations influence such a role, and how organizations need to transform to enable the CPO in the digital economy. Hence, we adopt a grounded theory approach (Corbin and Strauss 2015). We aim to develop a theory about privacy at the organizational level. Specifically, the inductive theory is about how the CPO – as an agent of information privacy – transforms organizations and is impacted by organizational privacy initiatives and structural choices. We apply the grounded theory approach for the following reasons: First, qualitative research allows for a better understanding and in-depth exploration of contemporary social phenomena in a natural setting. The qualitative research method will help us understand the CPO role and its transformational impact on organizational privacy. Second, the grounded theory approach offers a set of rigorous procedures for data analysis and generating theory from data (Corbin and Strauss 2015; Urquhart et al. 2010). Finally, the approach enables the study of emerging areas (Corbin and Strauss 2015; Wiesche et al. 2017). The global information privacy legal environment is witnessing several massive changes that present new challenges and opportunities for businesses. For example, the U.S. state of Massachusetts has recently been pushing for legislation to protect personal information called The Massachusetts Information Privacy and Security Act (Rundle 2022). Saudi Arabia introduced the Personal Data Protection Law that requires organizations, public and private, to make significant changes in how data are collected, stored, and processed. The new law's enforcement was postponed for enhancements as there were complaints about the negative impacts such a law might introduce (Parasie et al. 2022).

Data Collection & Analysis

The study aims to interview CPOs from different industries and countries. Having a broader range of participants enriches the results as information privacy policies, and laws differ from one country to another (e.g., Gramm-Leach Bliley Act in the U.S., General Data Protection Regulation in the European Union), and privacy enforcement and importance differ among industries (e.g., healthcare vs. metal industries). We developed an interview guide with open-ended questions organized into three general sections. The first is related to the CPO background, current activities and responsibilities, and role in the organization. The second contains questions related to information privacy in the organization (e.g., CEO and Board support, strategic priority), CPO relationship with technology executives (e.g., CIO, CTO, CISO), employee perceptions of information privacy and the CPO role, and information privacy importance to the organization's industry. The last section is related to the challenges and opportunities of information privacy in the digital economy and the evolution of the CPO role. Regarding the overall data collection and analysis approach, we follow the general guidelines for conducting grounded theory studies, which include constant comparison, iterative conceptualization, theoretical sampling, scaling up, and theoretical integration (Urquhart et al. 2010; Wiesche et al. 2017). These guidelines help improve the conceptualization needed to develop a good theory, scope the theory, and integrate it with the extant literature in the discipline (Urquhart et al. 2010). We note that the research was influenced by various theoretical lenses and literature, including upper echelon, strategic management, and the digital economy, which helped the researchers develop their sensitivity towards the CPO topic and scope the research (Urquhart and Fernandez 2006).

Coding

We follow open, axial, and selective coding techniques in analyzing the data (Corbin and Strauss 2015; Urquhart et al. 2010; Wiesche et al. 2017). Open coding is about labeling the data from interviews with codes that capture the meaning of the data. In the open coding phase, all three co-authors separately coded one interview to generate an initial coding scheme. We discussed the resulting scheme and narrowed it down from the set of categories based on the major themes. We then separately coded a second interview to both validate and add to our initial coding scheme. We completed several rounds of these open and axial coding phases iteratively, looking for relationships among the codes to identify categories and sub-categories of codes (Corbin and Strauss 2015). The resulting high-level coding categories and sub-categories are defined in Table 1. Finally, we performed selective coding, which involves forming associations among data codes and categories. Selective coding is about refining and relating categories around the core concepts. The analysis was iterative (i.e., dynamic interplay between data collection and analysis) (Urquhart et al. 2010), generating a set of relations among categories to provide better abstraction. The interview guide was updated after the first two rounds of interviews to accommodate essential questions. We added questions related to the different laws and regulations to which the CPO organization is subjected and their effect on the privacy practices and the CPO establishment history in the organization.

Category	Description	Sub-category
CPO demographic	Characteristics directly related to the CPO (e.g., history as a CPO, organizational title).	Respondent title; Respondent organization; Respondent length at current organization; Respondent total length as CPO or related; CPO reporting structure (CEO, CISO); Number of people reporting to CPO organization; Respondent path to CPO; Certifications or other official privacy training.
CPO role	Responsibilities and activities related to the CPO as a function in the organization (e.g., role type, challenges).	CPO role description; CPO role type; Reasons for CPO position in Org (legal pressure, other); CPO role challenges; CPO role advantages; Relationship to external stakeholder; Relationship to employees.
CPO metrics	Success and organizational outcomes related to the CPO role.	Performance metrics; Other outcomes; Metric measurement challenges.
Privacy in the organization	Strategic importance of information privacy in the CPO organization (CPO voice at the executive level, CEO and Board privacy understanding).	Definition of privacy; Importance of privacy; Strategic role of privacy; Relationship with CIO, CTO, and/or CISO; Sharing of responsibilities.
Privacy external to organization	Importance of information privacy in organization's industry and the impact of privacy-related laws and regulations on the organization's privacy practices.	Importance to industry/sector; Impacts of privacy laws and regulations
Privacy in the digital economy	New challenges and opportunities imposed by the digital technologies and innovations on information privacy and CPO role.	New challenges for privacy; New opportunities for privacy.

Evolution of CPO role	How the CPO role is changing over time and the predicted future of the role.	CPO changes over time; Future of CPO role.

Table 1. Coding Categories and Sub-categories

Study Current Status

Our study aims to stop conducting interviews to gather data when we reach the point of theoretical saturation (Urquhart and Fernandez 2013), which we estimate to be around 20-30 interviews. Several studies in the field followed the same range of interviews [e.g., Califf et al. (2020), Furneaux and Wade (2011), Jenkin et al. (2019)]. As of submission, we have conducted six interviews with CPOs from different industries and backgrounds, with an average of 50 minutes per interview (Table 2). The interviews were conducted and recorded via Zoom. Transcriptions were generated using automated transcription services. The quality of the transcriptions was then checked by an independent person. Moreover, during each interview, process notes were taken to achieve data quality and consistency and to provide triangulation during data analyses.

	Title	Industry/Sector	Tenure (years)	Organization Size
A	CPO & VP Privacy Services	IT Services & Consulting	1.5	Medium
B	CPO	Education	0.75	Large
C	HIPAA Compliance Officer	Government Administration (public)	2	Large
D	Data Protection Officer	Education	0.75	Large
E	Legal Counsel, Information and Privacy	Education	7	Large
F	VP & CPO	IT	4	Large

Table 2. Summary of CPO Participants

Initial Findings

Organizational Structure and CPO Role

Top management team (TMT) literature suggests that organizational factors such as structure, size, and strategies are antecedents that impact how functional executives perform their roles and generate organizational outcomes (Ma et al. 2021; Menz 2012). Organizational structural factors include centralization vs. decentralization of a specific role, membership in the top management team, direct reporting to the CEO, and others (Banker et al. 2011; Bendig et al. 2022; Menz 2012). Organizational structure can enable or hinder CPOs from performing their activities and responsibilities and determining their unit authority and power, which can have direct and indirect consequences on the organization's success in implementing privacy initiatives and managing privacy-related risks and violations.

Five of the CPOs indicated that they indirectly report to their organizations' CEOs. Moreover, none of the CPOs consider themselves members of their TMTs. However, three CPOs specified that they have direct visibility to the C-suite and the Board. Reporting structure and TMT membership are indications of the role importance within the organization (Preston and Karahanna 2009). They are measures of the structural power in the form of formal organizational position (Preston and Karahanna 2009). Hence, the relationship between the functional executives and the CEO and other executives is a central theme in the TMT studies [e.g., CIO (Bendig et al. 2022); CMO (Nath and Mahajan 2008); COO (Marcel 2009)]. We posit that when CPOs have greater organizational structural power, they can push the privacy agenda and have more influence on the CEO and other executives. When the CPO reports to the CEO, he or she will have hierarchical proximity to the CEO, which would lead to successful privacy-related initiatives. With a direct reporting structure, the CPO will establish a trusting relationship, facilitate the CPO role and allowing the CPO to have direct communications with the CEO about the organization and its strategies. Moreover, membership in the TMT can provide the CPO with several advantages. First, the CPO can have more opportunities to educate executives and the Board about the importance of privacy, its initiatives, and what potential consequences might occur with privacy violations and lack of compliance. Second, the CPO would interact and exchange knowledge with other executives to better understand privacy and its strategic values to the organization. Third, the CPO brings a unique set of knowledge and experiences that would augment the TMT knowledge and positively influence the decision-making process.

Two major factors impact the CPO organizational structure: strategic privacy priority and privacy maturity. First, strategic priority means that organizations not only comply with laws and regulations, but also seamlessly embed privacy practices and processes across the organization. Also, the CEO and Board are involved by having a reporting channel with the CPO about privacy and compliance issues. The CPO of a privately held company provided insights into how an organization views privacy as a strategic priority:

> *"The strategy is not only the collection and protection of the employee data, but it's the ability to offer the services to our clients*." The CPO adds: "*So from the strategy perspective, it's implementing [privacy] organizational-wide and incorporating it tactically into any of the engagements or efforts that we have internally and externally*." – Alfred, Org A

Another CPO mentions that his role is strategic, and privacy is considered an organizational strategic priority. This is reflected in the CEO's and the board's understanding and involvement in privacy. The CPO says:

> "*It is. Through our risk management process, various privacy risks are given a very high rating. And so information security, which is related. And so, it's certainly on the radar of our senior executive as a very significant priority*." The CPO adds: "*And so, the president, I think has a good understanding of the importance of privacy. I think the board of governors, adequate, I'm not sure that it's as important on their radar screen, there are committees of the board of governors, which are dedicated to it issues and security issues who really do get it, and really do understand the importance of privacy. So as a general response, I would say that I think there's good understanding and good support*." – Erik, Org E

On the other hand, the CEO and Board of organizations with less privacy strategic priority show less support and involvement in privacy. The CPO of a public organization explains:

> "*...once in the two years I was there, I did a presentation for agency heads and for the [Organization] executive... at the end of the day, it just seemed to me like, right, he's here, we're punching the regulatory ticket where I got someone to take care of this... let's move on to the next. Who's next on the agenda for today! You know, I gave my 12-slide presentation, didn't get any questions, like, how do we stand? Are we in good shape?"* – Charles, Org C

The second major factor relates to the maturity of privacy both at the organizational and industry levels. Low privacy maturity involves seeing privacy as a 'necessary evil' with limited impact. Moreover, the legal requirements might not be mature enough to strategically force organizations to support privacy-related initiatives. With such low privacy maturity, the CPO struggles with establishing legitimacy in the organization and generating real impact. One CPO reflects the idea by saying:

> *"Part of the difficulty is legitimizing yourself as an individual. And part of the difficulty is legitimizing the position of privacy."* – Alfred, Org A

Nevertheless, as privacy programs implementation and laws and regulations mature, the role of the CPO evolves and gets more strategic to the organization.

CPO Role Evolution

While many organizations have implemented a CPO position in compliance with legal requirements, the nature of the CPO role has not been static across different industries. Each of the six CPOs highlight the impact of the privacy implementation maturity level on the CPO role; starting from handling operational tasks (e.g., data protection, policy compliance) all the way towards building trust and a strategic image. Information privacy researchers suggest that recruiting a CPO is either considered as an operational goal by organizations when privacy is viewed as an opportunity with an internal focus to educate internal employees and enhance information management practices; or it is considered a strategic goal when organizations have an external focus to boost customers' trust and relationships (Greenaway and Chan 2013). Interestingly, our interviewees revealed that CPOs hold tasks and responsibilities that include both internal and external goals combined. Internally, CPOs are responsible for overall compliance towards privacy policies, as well as assessing, auditing, and reporting privacy practices to C-level executives to ensure that privacy was built into their operations, thus fostering the organization's effective information management. Compliance is not only legal, but can also focused on a variety of demands from public disclosures to stakeholder contractual agreements, for example. Other CPO internal tasks would also involve staff training and education activities across the organization. On the external focus, CPOs ensure

compliance towards privacy notices and legal requirements to enhance trust with external parties (e.g., customers, partners) and maintain a strategic ethical reputation. For instance, one CPO explained the internal and external nature of the role by saying:

> *"I have two roles. One, I'm the chief privacy officer of the organization. And within the organization itself, I'm responsible for all of the regulatory and ethical requirements associated with the collection and protection of personal data from a policy procedure and operational standpoint. So that's one, the other half of my role is I'm also the vice president of privacy services. And in that role, I lead the privacy practice for this [Org type]. And I consult with other companies to do assessments, design, build, operationalization and audit of their privacy programs. So, I have two roles, one is internal and one is external facing"* – Alfred, Org A

Our results show that the type of the industry or sector (e.g., health vs. higher education, public vs. private) may impact the nature of the CPO role. In addition, the results indicate that sizes of the organization and privacy team may affect CPO roles and responsibilities. In small to medium organizations, CPOs tend to wear multiple hats (e.g., legal, technical, managerial, financial). In larger organizations, CPOs tend to collaborate and share some responsibilities with top managers and employees from other functional areas.

Our results also outline that senior decision makers and top managers affect the legitimacy of the CPO position. CPOs who are acknowledged by the top management and are perceived as valuable by external stakeholders (e., clients, government, partners), receive better support to achieve their internal and external goals. We posit that the managerial support towards the legitimacy of the CPO position might be influenced by organizations' privacy orientations, namely differentiators, balancers, minimizers, and ignorers (Greenaway et al. 2015). First, privacy differentiators are organizations that distinguish themselves apart from their competitors by providing considerably better privacy protection as part of their business strategy. Second, privacy balancers are organizations that abide by industry or professional privacy regulations. Third, privacy minimizers participate in as many privacy-related actions as necessary to avoid any legal actions. Finally, privacy ignorers are organizations whose customers have little to no control over the information obtained. Our results imply that managers in privacy differentiators organizations are more likely to offer significant support to their CPOs than managers in privacy balancers where CPOs perform as decision-makers. Further, managers in privacy minimizer organizations are expected to provide little support to CPOs compared to managers in privacy ignorer organizations, who may resist the existence of CPOs. In this case, the CPO operates as a privacy advisor or consultant.

Organizational Transformation

Our results indicate that not all organizations are at the same level in terms of implementing privacy. Furthermore, our data show that organizations will need to transform to facilitate the growth of the CPO role and the implementation of more privacy practices. We propose that such transformation will occur in stages, summarized in our Privacy Implementation Maturity Model (PIMM) in Figure 1.

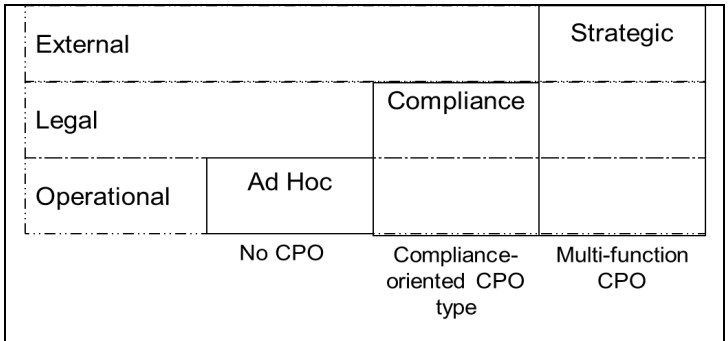

Figure 1. Privacy Implementation Maturity Model

The initial stage represents ad hoc implementation of privacy. It may involve some data owners or stewards within the organization developing some access policies or some other privacy awareness initiatives. Generally, there is no specific CPO role. The second stage is the compliance stage, where the organization implements a more structured unit to ensure that it follows the rules and regulations related to data and

information protection. This level of implementation is often a result of legal requirements or self-regulation to avoid further regulations. The CPO role in this type of organization often focuses on data protection (e.g., Data protection officer) or legal compliance (e.g., HIPAA compliance officer), and the CPO team tends to be small. Several of our interviewees were from this type of organization.

The third stage is strategic. This is where privacy is not only seen as a compliance issue but also as a mean to gain a competitive advantage, such as improved reputation either with customers or business partners. Therefore, the CPO role goes beyond the internal organization to be externally focused as well. At this stage, the organization may have both a data compliance officer and a CPO and has individuals evaluating the organization's products or services for their potential effect on data and information privacy, in addition to individuals focused on ensuring compliance with privacy laws.

How does an organization transform to support the increasingly strategic role of the CPO and privacy initiatives? First, as discussed in the first sub-section above, the organization needs to implement a reporting structure that facilitates the CPO having a voice at the executive level. Second, as discussed in the second sub-section organizations need to decide to go beyond compliance to realize that privacy can be used as a strategic tool. These first two elements are structural requirements for moving towards a strategic CPO role. However, the CPO at this level will only be successful if everyone in the organization also supports the strategic role of privacy. This means privacy awareness and proactive privacy behaviors at the individual, group, and organizational levels. The top-down approach may not be successful without serious implementation of privacy education, training, and awareness programs (Bélanger and Crossler 2011) that are targeted at changing the culture or mindset in the organization. Several of our interviews indicated that this was crucial but challenging. Evolving the privacy culture is required to move from ad hoc to compliance, as well as compliance to strategic.

> *"it requires some amount of shifting of the mindsets because privacy by design means that before you go to market, you have to ask these questions"* – Danny, Org D
>
> *"creating a culture of compliance that everyone can buy into"* – Charles, Org C

Conclusion

Transformation in the digital economy has been creating a challenge to protect consumers' personal information due to the drastic advancement of digital technologies. With that, data privacy has increasingly become a strategic priority that organizations need to manage and maintain (Greenaway et al. 2015; Greenaway and Chan 2013). Consequently, the need for a data privacy officer at a strategic level has increased as well.

The Chief Privacy Officer (CPO) title emerged in organizations in the health and financial sectors in the U.S. in the late 1990s (Bamberger and Mulligan 2011) and was solidified in 2000 when IBM named Harriet Pearson as CPO. "The chief privacy officer is a trend whose time has come," said Gartner analyst Bill Malik when IBM appointed Harriet P. Pearson as its CPO. The title became trendy in the 2000s in various industries (Awazu and Desouza 2004; Kayworth et al. 2005; Shalhoub 2009). The CPO role is evolving as a new strategic management position to enhance organizations' data privacy practices (Oh and Kim 2018).

Nevertheless, even with the increase in the number of privacy professionals (International Association of Privacy Professionals 2022) and the significance of implementing effective programs to protect customers' information privacy in organizations, research is still needed to understand the Chief Privacy Officer (CPO) role in shaping organizations privacy practices (Bantan and Shawosh 2021). Our search aims to contribute to organizational information privacy literature by investigating how the implementation of an organization's privacy initiatives influences the CPO role, and understanding how an organization needs to transform to support the emerging CPO role in the digital economy.

In this ongoing qualitative study, we have conducted six interviews to understand the impact organizations' privacy implementation maturity and the CPO role's evolution have on each other. First, based on our initial results, we proposed the Privacy Implementation Maturity Model (PIMM) as a theoretical framework, which includes three stages of the organizational transformation (i.e., external, legal, and operational) in support of the emerging CPO role and data privacy practices. Second, we initially found that the greater the priority of both strategic privacy and privacy maturity, the greater the chance that the CPO will direct reporting to the CPO or, at least, more visibility to the C-suite and board of directors. When CPOs are closer

to the decision-making circle, they will have a bigger impact on organizational privacy and its practices. Lastly, the CPO role has evolved over time. With that, their job has also evolved to include both internal and external responsibilities. Nevertheless, these responsibilities are subject to different organizational and environmental factors such as privacy implementation maturity level, organizational size, and industry type.

We aim to extend our work by conducting additional interviews to understand such CPO role across different industries better, taking into consideration the impact of digital technologies on creating challenges and/or opportunities for the future CPO role. We anticipate that our research can help practitioners by providing clear CPO role definitions from a strategic, legal, and operational perspective, allowing organizations to attract qualified candidates. Moreover, we expect that our work can provide a foundation for thinking about the future strategic role of privacy in organizations. While it may be argued that it may currently not be necessary for all organizations to have a strategic privacy orientation, we believe that there is going to be more and more pressure to do so, but in the short term, many organizations may not even be aware that they could or should consider strategic privacy.

References

Awazu, Y., and Desouza, K. C. 2004. "The Knowledge Chiefs: CKOs, CLOs and CPOs," *European Management Journal* (22:3), pp. 339–344. (https://doi.org/10.1016/j.emj.2004.04.009).

Bamberger, K. A., and Mulligan, D. K. 2011. "New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry," *Law & Policy* (33:4), pp. 477–508. (https://doi.org/10.1111/j.1467-9930.2011.00351.x).

Banker, R. D., Hu, N., Pavlou, P. A., and Luftman, J. 2011. "CIO Reporting Structure, Strategic Positioning, and Firm Performance," *MIS Quarterly* (35:2), pp. 487–504.

Bantan, M., and Shawosh, M. 2021. "Chief Privacy Officers: A Literature Review," in *AMCIS 2021 Proceedings*, August 9.

Bélanger, F., and Crossler, R. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017–1041.

Bendig, D., Wagner, R., Jung, C., and Nüesch, S. 2022. "When and Why Technology Leadership Enters the C-Suite: An Antecedents Perspective on CIO Presence," *The Journal of Strategic Information Systems* (31:1), p. 101705. (https://doi.org/10.1016/j.jsis.2022.101705).

Bowcut, S. 2022. *How to Become a Chief Privacy Officer: A Complete Career Guide*, (2022:April 20).

Califf, C. B., Sarker, Saonee, and Sarker, Suprateek. 2020. "The Bright and Dark Sides of Technostress: A Mixed-Methods Study Involving Healthcare It," *MIS Quarterly* (44:2), pp. 809–856. (https://doi.org/10.25300/MISQ/2020/14818).

Corbin, J., and Strauss, A. 2015. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, (Fourth edition.), Los Angeles, Calif.: SAGE Publications, Inc.

Furneaux, B., and Wade, M. R. 2011. "An Exploration of Organizational Level Information Systems Discontinuance Intentions," *MIS Quarterly* (35:3), pp. 573–598. (https://doi.org/10.2307/23042797).

Greenaway, K. E., and Chan, Y. E. 2013. "Designing a Customer Information Privacy Program Aligned with Organizational Priorities," *MIS Quarterly Executive* (12:3), Association for Information Systems, pp. 137–150.

Greenaway, K. E., Chan, Y. E., and Crossler, R. E. 2015. "Company Information Privacy Orientation: A Conceptual Framework," *Information Systems Journal* (25:6), pp. 579–606. (https://doi.org/10.1111/isj.12080).

Hajli, N., Shirazi, F., Tajvidi, M., and Huda, N. 2021. "Towards an Understanding of Privacy Management Architecture in Big Data: An Experimental Research," *British Journal of Management* (32:2), pp. 548–565. (https://doi.org/10.1111/1467-8551.12427).

International Association of Privacy Professionals. 2022. *LIVE IAPP Summit 2022 General Session with Tim Cook, Zahra Mosawi, Didier Reynders and Trevor Hughes*, International Association of Privacy Professionals. (https://www.youtube.com/watch?v=Dq0fcmmzfog).

Jenkin, T. A., Chan, Y. E., and Sabherwal, R. 2019. "Mutual Understanding in Information Systems Development: Changes Within and Across Projects," *MIS Quarterly* (43:2), pp. 649–671. (https://doi.org/10.25300/MISQ/2019/13980).

Kayworth, T., Brocato, L., and Whitten, D. 2005. "What Is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles," *Communications of the Association for Information Systems* (16:1). (https://doi.org/10.17705/1CAIS.01606).

Ma, S., Kor, Y. Y., and Seidl, D. 2021. "Top Management Team Role Structure: A Vantage Point for Advancing Upper Echelons Research," *Strategic Management Journal*, pp. 1–28. (https://doi.org/10.1002/smj.3368).

Marcel, J. J. 2009. "Why Top Management Team Characteristics Matter When Employing a Chief Operating Officer: A Strategic Contingency Perspective," *Strategic Management Journal* (30:6), pp. 647–658. (https://doi.org/10.1002/smj.763).

Menz, M. 2012. "Functional Top Management Team Members: A Review, Synthesis, and Research Agenda," *Journal of Management* (38:1), pp. 45–80. (https://doi.org/10.1177/0149206311421830).

Nath, P., and Mahajan, V. 2008. "Chief Marketing Officers: A Study of Their Presence in Firms'Top Management Teams," *Journal of Marketing* (72:1), pp. 65–81. (https://doi.org/10.1509/jmkg.72.1.65).

Oh, H.-K., and Kim, T.-S. 2018. "Factors Affecting an Organization's Information Security Performance: The Characteristics of Information Security Officers," in *Big Data Analyses, Services, and Smart Data*, Springer, Singapore, September 19, pp. 77–84. (https://doi.org/10.1007/978-981-15-8731-3_6).

Parasie, N., Martin, M., and Bartenstein, B. 2022. "U.S. Firms Warn Saudi Arabia New Data Law Could Hit Investment," *Bloomberg*. (https://www.bloomberg.com/news/articles/2022-03-16/u-s-firms-warn-saudi-arabia-new-data-law-could-hit-investment).

Preston, D. S., and Karahanna, E. 2009. "Antecedents of IS Strategic Alignment: A Nomological Network," *Information Systems Research* (20:2), pp. 159–179. (https://doi.org/10.1287/isre.1070.0159).

Rundle, J. 2022. "Massachusetts Legislature Advances Data-Privacy Bill," *Wall Street Journal*. (https://www.wsj.com/articles/massachusetts-legislature-advances-data-privacy-bill-11644575402).

Shalhoub, Z. K. 2009. "Analysis of Industry-Specific Concentration of CPOs in Fortune 500 Companies," *Communications of the ACM* (52:4), pp. 136–141. (https://doi.org/10.1145/1498765.1498802).

Sipior, J. C., and Ward, B. T. 2002. "A Strategic Response to the Broad Spectrum of Internet Abuse," *Information Systems Management* (19:4), Taylor & Francis, pp. 71–79. (https://doi.org/10.1201/1078/43202.19.4.20020901/38837.9).

Urquhart, C., and Fernandez, W. 2006. "Grounded Theory Method: The Researcher as Blank Slate and Other Myths," *ICIS 2006 Proceedings*. (https://aisel.aisnet.org/icis2006/31).

Urquhart, C., and Fernandez, W. 2013. "Using Grounded Theory Method in Information Systems: The Researcher as Blank Slate and Other Myths," *Journal of Information Technology* (28:3), Great Britain: Palgrave Macmillan, pp. 224–236.

Urquhart, C., Lehmann, H., and Myers, M. D. 2010. "Putting the 'Theory' Back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems," *Information Systems Journal* (20:4), pp. 357–381. (https://doi.org/10.1111/j.1365-2575.2009.00328.x).

Wall, J. D., Lowry, P. B., and Barlow, J. B. 2016. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the Association for Information Systems* (17:1), pp. 39–76.

Wiesche, M., Jurisch, M. C., Yetton, P. W., and Krcmar, H. 2017. "Grounded Theory Methodology in Information Systems Research," *MIS Quarterly* (41:3), pp. 685-A9.

Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798–824.