Design of Surveillance Technologies and Privacy Concerns

Rizwan Ahmad
USYD Business School
rahm4172@uni.sydney.edu.au

Uri Gal
USYD Business School
uri.gal@sydney.edu.au

Na Liu
USYD Business School
liu.na@sydney.edu.au

Abstract

Researchers from numerous management, social sciences and psychological disciplines have attempted to investigate the phenomenon of surveillance and the way it influences privacy concerns among individuals. But no study has attempted to interpret the relationship between individuals' perception of surveillance technologies and the way they react and develop their privacy concerns. We conduct a review of 207 prominent IT journals within the Scopus databases to examine and interpret individuals' perception of different designs of surveillance technologies (non-obtrusive vs. obtrusive) and how such technologies influence privacy concern at individual, corporate and societal level. Our review suggests that both non-obtrusive (automatic) and obtrusive (self-input) surveillance are used at individual, corporate and societal level differentially. In the light of our findings, we identify research gaps, propose recommendations, and further opportunities for future research that will enrich academic discourse in IS and create value for corporate firms, government and policy makers.

Keywords: *Surveillance, Privacy, Monitoring, Hacking, Data breaches.*

1. Introduction

Advancement of technology leads to diversified ways of data collection. Many of them lead to privacy concerns, but at different levels. Recently, new types of information technologies (mobile devices, sensors, social networking sites, digital apps etc.) have enhanced surveillance technologies, which collect and distribute individuals' personal data for various purposes. A number of studies have been conducted that report varying levels of privacy concerns among individuals. Some report low level of privacy concerns (Abramova et al., 2022; Sipior, 2021; De Moya & Pallud, 2020; Park et al., 2012); while others report high level of privacy concerns (Schyff, 2020; Stiff, 2019; Lightfoot & Wisneiwski, 2014; van Deursen et al., 2013). For example, technologies such as malware, adware (klitou, 2014), and remote neural monitoring (Binhi, 2009) can be used for illegal tracking and collecting individual personal data. Other technologies such as COVID-19 tracking app., smartphone sensors, GPS tracking, phone-calls/text message logs, social networking sites, and biometrics can be used for societal or individual beneficial purposes. The aim of the study is to find out how the context of surveillance and design of technologies influence privacy concerns.

The collection and distribution of individuals' personal data can encroach on their privacy (Lee et al., 2018; Newell & Marabelli, 2015) and influence their willingness to share their personal data. The collection of individuals' personal sensitive data and the possibility of their dissemination to third parties by vendors and service providers pose a grave risk to data privacy (Junglas et al., 2008). Furthermore, some government and corporations use technologies for mining and analyzing such data in order to interpret, understand and predict human behavior (Shaw et al., 2016), purchasing patterns (Huang et al., 2018), city dynamics (Gao et al., 2017), sensitive health conditions (Urbaczewski & Lee, 2020), geo-social networks (Scellato, 2011), and internet hacking (Elhai et al., 2017). Such surveillance technologies have vastly influenced individuals' concerns for privacy (Junglas et al., 2008; Kim et al., 2011).

Although a number of studies in the IS literature have examined the concept of surveillance in relation to specific technologies and if it influences privacy concerns among individuals (Abramova et al,, 2022; De Moya & Pallud, 2020; Andrejevic, 2019; Clarke, 2019; Anteby & Chen, 2018; Nam, 2018; Crosler & Posey, 2017; Andrejevic & Burdon, 2014; Almer, 2011), no study has examined the relationship between individuals' perception of different designs of surveillance technologies and how they react to such surveillance. Moreover, we still do not know how strong the relationship is between individuals' perception of different designs of surveillance technologies and their concerns for privacy.

In this work, we embark on reviewing and mapping the current body of knowledge on surveillance and its impact on individuals' concerns for privacy. In doing so, we differentiate various designs of surveillance based on the context, purpose and the type of technologies used to collect data. Based on examining the current body of knowledge, we identify areas of research in relation to surveillance technologies and their influence on individuals' concern for privacy. This is followed by proposing contributions to IS research with respect to individuals' perception of different designs of surveillance technologies and their concerns for privacy.

The rest of the paper is organized as follows: First, we discuss the theoretical background on surveillance technologies and individuals' concerns for privacy. Next, we discuss the research methodology and findings based on our review of the literature. Then, we propose research questions and discuss opportunities for future research on the relationship between individuals' perception of surveillance technologies and privacy concerns.

2. Theoretical Background

Surveillance

Surveillance is "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction"(Lyon, 2007, pp.14). Clarke (2019, pp.61) argues that surveillance is "the systematic investigation or

URI: https://hdl.handle.net/10125/103138
978-0-9981331-6-4

monitoring of the actions or communications of one or more persons". To further understand surveillance, we need to examine surveillance theories in order to examine the growth of surveillance technologies:

Panopticon and Panopticism. Foucault describes 'panopticism' as "a type of power that is applied to individuals in the form of continuous individual supervision, control, punishment, compensation, and correction, that is, the modeling and transforming of individuals in terms of certain norms" (Foucault, 2002, pp. 70); whereas 'panoptic' is defined as "seeing everything, everyone, all the time" (Foucault, 2006, pp. 52). Surveillance theorists regard the 'panopticon' as a metaphor for surveillance; a 'strategy of space' that causes "new mode of obtaining power of mind over mind in a quantity hitherto without example" (Bentham, 2010, pp. 15). With the advent of electronic forms of surveillance, systems of power shift from centralized institutions to informal and ad- hoc groups or networks within the society (Manokha, 2018) that lead to the development of post-panoptical surveillance and "digital panopticon".

Post- panoptical surveillance. It began in the late 1970s with the growth of capitalism and free market as a "global political system" as well as the rise of modern computer systems and networked technologies. Deleuze characterized it as a different form of surveillance that is exercised by profit-seeking corporate-firms rather than nation states due to modifications or transformations in the "socio-technical landscape" (Deleuze, 2006). Deleuze further argued that the emphasis of post-panoptical surveillance is no longer on "discipline" but on "controlling society" through monitoring and assessing markets and workforces to enhance financial goals using networked technology (Deleuze, 2006). The most important characteristic of post-panoptical surveillance is "modulation" referring to goods, services and skill sets that constantly change or modulate as corporate interests and markets change. Here, the emphasis is on "productive citizens" who are regarded as "consumers" that lead corporations to create consumer profiles with an objective of altering their purchasing patterns (Timan et al., 2017). Some of the examples of post-panoptical surveillance technologies are constant changing nature of "malware" and "creeper" developed in 1970s. Finally, the advent of Internet and mobile phones including smartphones led to the development of "contemporary surveillance".

Contemporary Surveillance. Surveillance theorists label this as the final stage of surveillance that focuses on contemporary conceptualizations or constantly evolving technologies of surveillance that started during late 1980s (Timan et al., 2017). In this stage of surveillance, the roles are diffused between "watcher" and "being watched" along with power-relations in social structures. Here, the emphasis is on "discipline" and "control" to both "underclass" and "productive citizens" (Timan et al., 2017) through "automated surveillance" and "taming" (Andrejevic, 2019). Hence, the thriftiness of "panopticon, which traded on the uncertainty provided by its one-sided gaze, is replaced by the tendency towards comprehensive monitoring associated with the proliferation of distributed, embedded, always-on sensing networks" (Andrejevic, 2019, pp. 1). There are three fundamental contemporary surveillance concepts: "alternative opticons, sousveillance, and participatory surveillance" (Timan et al., 2017). "Alternative opticons" refer to a vast net of Internet infrastructures of servers, databases, and screens along with various consumer technologies blended through ICT. "Sousveillance" refers to the citizens or individuals who watch the governing bodies such as governments, institutions, and consumer firms, using bottom- up approach instead of the classic top-down approach. In other words, these individuals surveil the surveillors (Mann, 2004). Building on the idea of decentralized counter-surveillance, Albrechtslund (2008) invented the concept of "participatory surveillance" that refers to the citizens or individuals who not only engage in surveillance as "watchers" or "sousveillors" but also voluntarily take an active part in the role of being "watched". Recently, De Moya and Pallud (2020) conducted a study with respect to wearable "quantified-self" (QS) technologies representing self-surveillance. They named this type of self- surveillance as "heautopticon" that, on one hand, offers individuals a sense of "freedom, reassurance and knowledge" but, on the other, it also offers a sense of "identification, subjection and feeling of guilt" (De Moya & Pallud, 2020). Furthermore, Zuboff (2015) signal the development of "surveillance capitalism" defined as the distribution of power between organizations and public spheres instead of power being centralized as in the case of "panopticon". This is relevant to corporate-based surveillance as discussed above by Deleuze (2006). Similarly, Latour (2012, pp. 91- 93) coins the term "oligopticon" and argues that "similar panoptic principles are still in place, yet dispersed via smaller sub-systems and situations—a network of multiple smaller panopticons that all have a different disciplining power on individuals" such as "the few watching the many" characterized by "caring" and "coercive control" at workplace (Sewell & Barker, 2006). Hence, we see that surveillance, in the contemporary world, is a by-product of digitization of all the activities of individuals, commonly known as "datification" (Newell & Marabelli, 2015).

Further, 9/11 gave rise to new forms of surveillance surrounding "control" and "global insecurity", such as BanoPticon (Bigo, 2006) that refers to "detaining" and keeping bad guys out through various check points. Moreover, it is also evident from Snowden's leak in June 2013 that intelligence agencies are conducting mass-surveillance program in the US and UK in the name of controlling crime and national security (Macaskill & Dance, 2013). Finally, Lyon (2015) argues that "big data is at the heart of the surveillance state..." (p.68). it can allow law enforcement agencies and consumer firms to investigate and understand human moods, behavior patterns, relationships, networks, and opinions. This has also resulted in "predictive policing" that relies heavily on "historical patterns of crime data" in order to curb crime (Andrejevic et al., 2015).

Hence, we see that digitization is the key to contemporary surveillance. But, panopticon may be still be considered as a metaphor to analyze contemporary surveillance as it "highlights the role played by new technologies in strengthening surveillance in contemporary society" (Leclercq-Vandelannoitte, 2010, pp. 59). Therefore, perception of "surveillance" is defined as how individuals react to the threat of various designs of surveillance technologies constantly evolving in the society. This raises a concern for privacy among individuals (Shiau et al., 2021). Next, we will discuss literature on Privacy.

Privacy

In this study, we define privacy as protecting one's personal information from unnecessary disclosure (Gerber et al., 2018). Further, we characterize "privacy" along its four basic dimensions: privacy of a person, personal behavioral privacy, personal

communication privacy, and personal data privacy (Clarke, 2019). Since most of the communications and personal information are comprised of digitized data in the contemporary world, we combine "personal communication privacy" and "personal data privacy" into a single concept of "information privacy" (Belanger & Crossler, 2011) defined as individuals' managing, governing or considerably regulating ones' personal information (Clarke, 1999, as cited in Belanger & Crossler, 2011, pp. 1018).

With the increased use of email, social networking, micro-blogging and e-commerce, the traffic on Internet has risen sharply. This has escalated debate on privacy about what information should be kept confidential and what information should be stored. Similarly, the advent of location tracking devices such as cellular phones and wearables led us to "locational data privacy" (Klitou, 2014). Further, Smith et al. (2011) argue that individuals' privacy concerns have transformed into value-laden commodity; whereas, Schoeman (1984) argues that individuals' privacy concerns are determined by their social and moral values and have legal implications. Literature suggests that conceptions of "information privacy" also depend upon personal experiences, attitudes, personality, occupation, and social and cultural background. Therefore, the relevance of information privacy should be investigated based on "privacy as a control", "privacy as a value" (Smith et al., 2011), and "privacy as ethics" (Schoeman, 1984).

Privacy as a control. Privacy can be defined as individuals having an access and control to self-disclosure of their personal information. Individuals are not likely to disclose their personal information if they feel that the perceived risk for a privacy breach is higher as a result of them having less personal control over their information disclosure and dissemination by government or consumer firms (e.g., in the form of faulty privacy policies). This translates into low "general trust" in them (Dinev et al., 2013). The literature describes a significant positive relationship between "general trust" and "perception of control". Here, a low level of "general trust" implies trust that individuals have in government or consumer firms. This suggests that individuals want to exercise their self-control about how, what and to whom they want to disclose their personal information (Keith et al., 2015). However, when individuals perceive a low level of "general trust", they disclose their personal information based on "information sensitivity"; the degree to which they perceive their information as sensitive and the level of control they have over information disclosure. Individuals interpret and evaluate the degree of "information sensitivity" based on how severe they will suffer their privacy loss resulting from their "self-disclosure" behavior; however, enhancing more "general trust" in government or consumer firms compensates for the degree of their "privacy loss" (Mothersbaugh et al., 2012).

Finally, "privacy as a control" may also be viewed as how and, to what level, individuals experience the interplay between influence and power among individuals, groups and institutions within society. This helps them decide on the degree to which they disclose their personal information (Dinev et al., 2013). Thus, we see how perceived concerns for privacy interact with individuals' access to their personal information, general trust, and control by industries or government and shapes individuals' self-disclosure behavior (Crossler & Belanger, 2019).

Privacy as a value. Privacy may be defined as having its "economic market value" (Xu et al., 2009). Hence, privacy may be viewed as "self-surveillance" in which individuals willingly participate and disclose their personal information in an anticipation of getting some future benefits in the form of monetary values, convenience, personalization, and customization (Adjerid et al., 2018). This gives rise to "privacy paradox" defined as a difference between individuals' actual practice of self-disclosure and their stated preferences of information disclosure in which they evaluate "cost vs. benefit" of disclosing their personal information (Xu et al., 2009). Numerous studies have attempted to examine the notion of "privacy paradox" in elaborating individuals' behavior and attitudes of disclosing their personal information (Adjerid et al., 2018; Sutanto et al., 2013; Crossler & Clay, 2017).

Privacy as ethics . Privacy may be defined as based on individuals' "public values" (democratic principles that constrain state power such as "individuals' association" & "freedom of speech"), "collective components" (collective goods within particular political & social systems), and "shared perceptions" ("diversity of thought" & "freedom to choose" based on social and cultural values). These values are the tools that enable state to devise privacy policies and regulations in order to alleviate the risks of breach (Regan, 2000). Thus, privacy as ethics is based on individuals' moral and social values that is deeply rooted in their political, social and cultural system within the society (Schoeman, 1984). As individuals' social and political values change with the passage of time, so do their concerns for privacy as these need "value judgments" from time to time (Keith et al., 2015).

Therefore, the implementation of technologies and their applications must be regulated based on existing "ethical values, frameworks and principles" that encompasses "fairness, accountability and transparency" as a policy and law (Raab, 2020).

3. Methodology

Scope of research & Journals-searching

We examined the existing research on individuals' perception of surveillance technologies and concerns for privacy by conducting a review of 87 important IS journals with the help of large (L) "LIBASKETS" within the "Scopus" database. The "L" "LITBASKETS" of IS journals included the basket of 8 journals as well. "LITBASKETS" (www.litbaskets.io) is a search engine that allows researchers to search literature baskets with different number of journals (e.g. XS, S, M, L) within the Scopus databases. We employed a full-text search in these journals during the last twelve years (2011-2022) using separately the keywords "surveillance and privacy", "monitoring and privacy" and "hacking and privacy" in order to investigate how individuals' perception of different designs of surveillance technologies along with their concerns for privacy have evolved during the period. We selected the time-period between 2011 and 2022 after counting the number of yearly publications on surveillance and privacy. We found that the research on surveillance and privacy picked up its momentum and became more matured since 2011. We included those articles in the review that covered a wide range of different designs of surveillance technologies along with how these technologies influence individuals' concerns for privacy across different stages of analysis and epistemological approaches.

Selecting & Examining Articles

Having conducted the search using the above three keywords separately, LITBASKETS provided a total of "207" articles (Table 1) after removing duplications in all the three search results. Next, we read the entire abstract and keywords of all the articles in order to specify those articles that covered individuals' perception of different designs of surveillance technologies along with the concerns for privacy either to theorize or to investigate empirically

using data. If the abstracts or keywords used in the articles indicated that the articles did not employ the concept of privacy resulting from surveillance technologies or scarcely employed the concept relevant to surveillance and privacy, or employed the concept in a generic way, we eliminated those articles from the analysis. This reduced the list of articles to a total of "82" articles (Table 1). Finally, we read each of the 82 articles carefully and thoroughly, and examined them on the basis of the following two issues: (i) whether the use of the concept of surveillance (i.e control, discipline, hacking or data breaches, top-down, bottom-up, peer-to-peer, self-surveillance), resulting from the perception of different designs of surveillance technologies, was significant in each of the articles, and (ii) if, and how, perception of different designs of surveillance technologies influence individuals' concern of privacy (i.e. commodified value, control of access to information, & social, moral and legal implications). In the process, we eliminated those articles that employed the perception of surveillance technologies and concerns for privacy as a peripheral idea or employed it as a technical, design, or implementation issue or entirely to a different focus of our research. The final list of the paper contained 64 articles (Table 1, Appendix 1).

Table 1. Sample Sizes of Journals and Articles

	Step 1	Step 2	Step 3
Total No. of Articles	207	82	64
Total No. of Journals	41	33	24

4. Analysis and Findings

Guided by the literature reviewed, we categorized the 64 studies based on their approach to "context" of surveillance, "purpose" of surveillance, "data-collection method" of surveillance technologies and "types" of surveillance technologies used. Next, we identified patterns and themes, using grounded theory approach (Heath & Cowley, 2004; Straus & Corbin, 1998), and generated categories based on their approach to surveillance surrounding "individuals", "society", and "corporate level" and how these influence their privacy concerns. The findings suggested some duplications among individual, corporate and societal level. We analyze the findings using Table Matrix 2. The Table Matrix 2 is based on "non-obtrusive" surveillance and "obtrusive surveillance" and display the findings in terms of the purpose of surveillance depending upon the context and type of technologies used for surveillance. We define "non-obtrusive" surveillance in which technologies collect data without individuals' knowledge or their efforts such as drones, smartphones sensors etc.; whereas, we define "obtrusive surveillance" in which individuals participate and share their data willingly such as 'biometrics', "scanning the QR codes of COVID19 apps" etc. We follow the above theoretical background to analyze findings and propose recommendations for future research.

Our findings suggest that non-obtrusive surveillance and obtrusive surveillance are used at the individual, corporate, and societal level and influence privacy concerns differentially. (Wolfowicz , 2021; Muratbekova-Touron, & Leon, 2021; DeMoya & Pallud, 2020; Stark et al., 2020; Stiff, 2019; Crossler & Posey, 2017; Elhai & Hall, 2016). Based on the Table Matrix 2, although obtrusive surveillance is used for beneficial purpose at an individual level, such as contact tracing through disease-control e-health monitoring technology (Ehrari et al., 2020) or COVID-19 application (Wnuk etal., 2021; Urbaczewski & Lee, 2020), social

Table Matrix 2. Purpose of Surveillance

	Non-Obtrusive Surveillance	Obtrusive Surveillance
Individual	• Health Sensitive Data • Location Tracking • Personally Identifiable Info. • Phone/Text Message/Email Logs • Behavioral/Purchasing Patterns • Personal Sensitive Data (Credit Cards) • Usage Patterns/Electricity Use • Health/Fitness Tracking Data • Cyber-security/Data Breaches	• COVID19-tracking • Social Networking peer-to-peer • Disease Control • E-commerce • Impression Management • Social Networking Self-disclosure
Corporate	• Employee Productivity • Targeted Marketing/Advertising • Controlling Employees • Cyber-security/Data Breaches • Facial & Emotion Recognition	• Online Video Conferencing
Societal	• National Security • Intelligence • Crime Control • Societal Health Patterns (Public Health) • Illegal Migrant Data Breaches from humanitarian IT Systems	• COVID19 Tracking • Disease Control • Biometrics

networking monitoring through social media (Mullen, & Fox, 2016), e- commerce through identity eco-systems (Crossler & Posey, 2017), online impression management (Marder et al., 2016) or peer-to-peer monitoring (Tokunaga, 2011) or online sharing of personal data using social media/online blogs (Park et al., 2012) etc., there is still a risk of data being disclosed if not handled carefully or used for commercial purposes (Bhatt et al., 2022; Martin, 2016; Park et al., 2012; Wills, & Zeljkovic, 2011). Similarly, non-obtrusive surveillance, at an individual level, may be used either for beneficial purpose such as using GPS or smartphones sensors for location tracking (Park & Jang, 2014), self-monitoring one's health using smart wearable devices (DeMoya & Pallud, 2020) or for the purpose of marketing or advertising such as collecting unauthorized data for interpreting one's behavioral or purchasing patterns using data analytics (Mai, 2016; Zuboff, 2015), collecting personally identifiable information (Bansal & Nah, 2022; kauffman et al., 2011) etc. Further, non-obtrusive surveillance may also be used for cyber-attacks through web-tracking (Samarasinghe & Mannan, 2019), adware, malware, phishing, DoS etc. (Kim et al., 2011) and cyber bullying by collecting others' personal information from Facebook profiles and posts (Stiff, 2019).

At the corporate level, obtrusive surveillance may be used for improved and efficient communication over-the distance using video-conferencing tool (Stark et al., 2020); whereas, non-obtrusive surveillance may be used to control employees and recognize their productivity by using organizational employee monitoring system (Holt et al., 2017), AI and emotion recognition tool (Sipior, 2021) or facial recognition tool (Stark et al., 2020) so that they can perform effectively and efficiently. Further, non-obtrusive surveillance may also be used to market target consumers by collecting and interpreting behavioral patterns and locations using big data and data analytics (Clarke, 2019; Martin,

2016), to cyber- attack or to breach data by using multiple contemporary digital technologies (Lee & Lee, 2012).

At the societal level, obtrusive surveillance may be used for contact tracing using COVID-19 tracking app. (Fox, Clohessy et al., 2021) or to collect patients' health sensitive passive data using healthcare app. (Maher et al., 2019) or for identification purposes using biometrics (Nam. 2018). Similarly, non-obtrusive surveillance, at the societal level, may be used to control crime by collecting data using open- source intelligence platforms (Bayerl & Akhgar, 2015) or by intelligence agencies collecting data using IoTs, tablets, mobile phones, social media etc. (Shores et al., 2022; Cayford & Pieters, 2018), to monitor national security by collecting data provided by 3rd party communication-service-providers (Thompson et al., 2020) or by analyzing behavioral patterns or activities on social media for prediction (Wolfowicz et al., 2021), to monitor health patterns using consumers' wearable devices (Saifuzzaman et al., 2022), to breach humanitarian data about illegal immigrants using their online IT systems (Vannini, 2019) etc.

Hence, we see that both obtrusive and non-obtrusive surveillance are used for beneficial purposes but, at times, also used for unauthorized data collection or even cyber-attacks or data-breaches. Next, the findings suggest that "privacy" should be viewed based on "value", "control", and "ethics" as well, as discussed above in the theoretical background so that we can locate opportunities and propose recommendations for further research in IS literature.

Privacy as a Value

30 of 64 studies (Appendix 1) showed how people approach their privacy concerns based on some value (health, convenience, national security, e-commerce, employee productivity, biometrics etc.) attached to self-disclosing or sharing their personal data across individual, society, and corporate level against both "non-obtrusive" and "obtrusive" surveillance. Further, 15 of the studies (Fox, Clohessy et al., 2021; De Moya & Pallud, 2020; Tokunaga, 2011 etc.) focused on individual level of privacy concerns as value (individual health, self-empowerment, relationship management on social networking sites etc.) associated with disclosure or sharing of their data, 5 of the studies (Stark et al., 2020; Afriat et al., 2020; Morris et al. 2014 etc.) focused on corporate level of private concerns as value (employee productivity, marketing, improved business decision making etc.) associated with collecting or sharing the data, and 15 of the studies (Saifuzzaman et al., 2022; Wolfowicz et al., 2021; Cayford & Pieters, 2018 etc.); focused on societal level of privacy concerns as value (public health, national security, curbing crime etc.) associated with disclosing or sharing the data, against both "non-obtrusive" and "obtrusive" surveillance (Appendix 1).

For example, Abramova et al. (2022) investigated obtrusive surveillance in Germany and Switzerland at an individual level (N=589) and found that individual privacy calculus behavior is a major factor in explaining huge intention-behavior gap where social risks mediate between acceptance of COVID-19 app. & privacy risks leading to technology acceptance. Similarly, Holt et al. (2017) investigated non-obtrusive surveillance at a corporate level at two steps (N=312 & N=341) and found that active monitoring of employees reduced their perceptions on organizational ethics as well as lowered the level of their job acceptance and job satisfaction; however higher pay was proportional to job acceptance and had marginal effect on job satisfaction. Further, Wolfowicz et al. (2021) investigated non-obtrusive surveillance at the societal level by comparing 48 Palestinian terrorists with non-violent radicals using their interactions on Facebook and found that social learning theory's behavioral metrics was useful to differentiate violent (i.e. terrorists) vs. non-violent radicals of social media. They further concluded that this could help in controlling terrorist activities.

Privacy as a Control

17 of 64 studies (Appendix 1) showed how people approach their privacy concerns based on control of access to their information associated with disclosing or sharing their personal data (individual health, targeted marketing, humanitarian IT Systems breaches etc.) across individual, society, and corporate level against both "non-obtrusive" and "obtrusive" surveillance. Furthermore, 4 of the studies (Bhatt et al., 2022; Mullen & Fox, 2016; Crossler & Posey, 2017 etc.) focused on individual level of privacy concerns based on control of access to personal information for their self- disclosure (individual health, social networking among adolescents, controlling ones' personal sensitive information etc.), 11 of the studies (Lightfoot & Wisneiwski, 2014; Lee & Lee 2012; Wills, & Zeljkovic, 2011 etc.) focused on corporate level of private concerns based on control of access to information (employee productivity, business Internet hacking, targeted marketing/advertising etc.) associated with control of access to personal information or sharing the data with the third parties, and 5 of the studies (Bansal & Nath, 2022, Vannini et al., 2019; Thompson et al., 2020 etc.) focused on societal level of privacy concerns based on control of access to information (national security, humanitarian data breaches, crime control, etc.) associated with disclosing or sharing the data with law-enforcement or any other party, against both "non-obtrusive" and "obtrusive" surveillance (Appendix 1) as discussed above.

For example, Mitchell (2019) investigated both obtrusive and non-obtrusive surveillance at an individual level. She conducted platform and content analysis of the two disease tracking apps.,"Sickweather" & "Healthmap", .and found that both the apps. constructed disease threats or alerts by collecting data from open source and by collecting users' personal sensitive health information with users scanning the QR code. This provided an opportunity for service providers to sell their data to third parties if the users don't have appropriate level of access of control to their personal information. Similarly, Anteby and Chan (2018) investigated non-obtrusive surveillance at the corporate level by conducting unstructured interviews (N=89) and found that surveillance was used as a mean to control employees where employees felt both visible and unnoticed by management. This produced a "paradoxical" effect leading them to engage in practices that could help them get unnoticed. This led to more surveillance by management; thereby creating a cycle of "coercive" surveillance. Further, Thompson et al. (2020) investigated non-obtrusive surveillance at the societal level by conducting an online survey of 100 Australian and 142 Sri Lankan residents and found that low power distance culture (Australia) had a significant influence on the relationship between privacy concerns and surveillance acceptance as opposed to that of the higher power distance culture (Sri Lanka). This explained the influence of culture on individuals' concerns for privacy as a Control.

Privacy as Ethics

17 of 64 studies (Appendix 1) showed how people approach their privacy concerns based on social or/and legal policies associated with disclosing or sharing their personal data (individual

or corporate data breaches, marketing, advertising, public health, social networking etc.) across individual, society, and corporate level against both "non- obtrusive" and "obtrusive" surveillance. Furthermore, 9 of the studies (Alassad et al., 2021; Samarasinghe & Mannan, 2019; Stiff, 2019 etc.) focused on individual level of privacy concerns based on social or/and legal implications associated with personal information for their self-disclosure (cyber attacks, data breaches, cyber-bullying or spying etc.), 7 of the studies (Jones, 2017; Zuboff, 2015; Manohan, 2016 etc.) focused on corporate level of private concerns (marketing, targeted advertising, employee productivity etc.) associated with collecting or sharing the data with the third parties based on certain regulations and legal implications, and 6 of the studies (Meher et al., 2019; Jones, 2017; van Deursen et al., 2011 etc.) focused on societal level of privacy concerns based on social or/and legal values (public health, crime control, health data breach etc.) associated with disclosing or sharing the data with law-enforcement or any other party, against both "non-obtrusive" and "obtrusive" surveillance as discussed above (Appendix 1).

For example, Elhai and Hall (2016) investigated non-obtrusive surveillance at an individual level by distributing a survey of adults (N=304) and found that individuals' anxiety around Internet hacking is dependent upon intervention, human behavior & education. Similarly, Martin et al. (2016) investigated non-obtrusive surveillance at a societal level by collecting qualitative responses (N=102) in two different phases and found that both technical and non-technical measures must be adopted and privacy policies must be strengthened with opt-in control for individuals if they wish to disclose their information. Furthermore, van Deursen et al. (2011) investigated non-obtrusive surveillance at a societal level by combining historical data of security incidents along with experts' elicitations in the form of surveys. They found that health data-breaches are the result of socio-technical factors focusing on human-behavior.

5. Discussions, Recommendations & Contributions

Our review has explored some central issues and how these issues influence privacy concerns of individuals, corporations and society respectively. These issues include monitoring, collecting or sharing location sensitive data, health sensitive data, personal identifiable information, behavioral or purchasing patterns, sensitive financial data, health or fitness tracking data, usage and billing patterns of various appliances, phone or email logs, social networking self-disclosure, peer-to-peer social media surveillance, and cyber-security risks at an individual level. At the corporate level, the issues include monitoring, collecting or sharing information for employee's productivity and control, parallel surveillance among employees, targeted marketing or advertising, employees' facial and emotion recognition, cyber- security breaches, and over-the-distance audio and video conferencing tool. At the societal level, these issues include monitoring, collecting or sharing data for national security and crime-control, public health patterns, biometrics, and disease control. The review further suggests that these issues influence privacy concerns differentially based on the value, control of access to information, and social and legal implications. The research has also revealed that the extent of privacy concerns is dependent on the purpose of surveillance and the type of surveillance technologies used for surveillance.

Next, our theoretical frameworks include "communication privacy management" (CPM) theory (Petronio, 2015) and "deterrence" theory (Williams & Hawkins, 1986) that we used to identify research-gaps in our review. Communication privacy management (CPM) theory has been found very effective in understanding privacy in day-to-day lives. CPM theory acknowledges that individuals have the right to own and control their information where "ownership" is symbolized by "privacy boundaries" that refers to where individuals contain and safeguard their information (Petronio, 2015). CPM uses identifiers- "information owner" and "authorized co-owners" representing control of access to their information along with "trust" that they can impose in granting right to who can access their information and, to whom, their information is off-limit (Petronio & Gaff, 2010). This helps them decide to open their "privacy boundaries" to whom they can reveal or conceal their information (Hammond, 2015). If they decide to reveal their information, they use "privacy rules criterion" that may predict constantly changing "privacy regulations" or "law" depending upon their current social and cultural factor (Petronio, 2013). This helps them manage their privacy concerns effectively. Furthermore, deterrence theory (Williams & Hawkins, 1986) is the most widely accepted theory in IS behavioral security research. It is used to forecast human behavior that either disrupts or supports IS-related security outcomes. For example, D'Arcy and Herath (2011) demonstrated the existence of "deterrence theory" with regards to employees' compliance of organizational security regulations. They further argued that employees or individuals constantly evaluated the pros and cons of performing an action based on "severity, certainty, or celerity" of its consequences that helped them decide whether the costs of performing an action outweighs its benefits. If so, they deter from performing an action otherwise they go ahead and perform the action.

Based on "communication privacy management (CPM)" theory and "deterrence" theory, we have identified four research gaps in our review. The first about if and how we can measure the relationship between privacy-concerns as a result of non-obtrusive surveillance and privacy concerns as a result of obtrusive surveillance at the individual, corporate and societal level. Non-obtrusive surveillance collects data automatically; whereas, obtrusive surveillance is based on self-input, as discussed above in Table matrix 2. The review points to a second research gap about why, and to what extent, individuals' perception of surveillance surrounding different designs of surveillance technologies relate to their concerns for privacy across individual, corporate and societal level as the review suggests that privacy-concerns differ based on the purpose of surveillance and the type of technologies used across individual, corporate and societal level. The review points to a third research gap about if there exists a relationship among "privacy as a value", "privacy as a control", and "privacy as ethics" and, to what extent, they interact and influence each other. Finally, the review points to fourth research gap about how, and to what extent, "cultural factor" at an individual level, and "trust" and "socio-technical factor" at the corporate level moderates the relationship between perception of different designs of surveillance technologies and concerns for privacy.

The above research gaps suggest that there is a difference between the perception of different designs of surveillance technologies used for data collection and the way individuals address their privacy concerns surrounding such technologies. The review suggests that such perceptual difference also depend upon cultural factor, socio-technical factor and data sensitivity (Thompson et al, 2020; Leclercq-Vandelannoitte,& Aroles , 2020, Elhai & Hall, 2016, van Deursen et al., 2011). The researchers should investigate such differences carefully in order to have holistic understanding about people's behavioral patterns and what might lead them to cyber-security or data breaches. Further, the

researchers should investigate the trade- offs among "privacy as a value", "privacy as a control" and "privacy as ethics" and how such trade-offs help mitigate concerns for privacy. Finally, the researchers should also perform a longitudinal study to investigate the degree to which the concerns for privacy as a "value", "control", and "ethics" have changed over a particular span of time at individual, corporate and societal level. This will help consumer firms and government formulate and implement better and effective privacy policies. This will mitigate privacy concerns at the individual, corporate and societal level and help the firms to design more efficient consumer products.

In order to address the above research gaps, we propose a mixed-method approach by combining "factorial survey approach" (Wallander, 2009) based on varying "situations" or "vignettes" with complementary unstructured interviews. Factorial survey is a very effective tool to investigate and explore the relationships among variables that will help come holistic understanding of the phenomenon under study. Finally, unstructured interviews will help complement in terms of "convergence" or "divergence" (Venkatesh et al., 2016) of the findings.

Theoretically, the study will help IS researchers to delve deep into people's perception of different designs of surveillance technologies and help propose a better theoretical model based on the relationship between people's perception of surveillance, their privacy concerns, and information disclosure behavior. Further, our study will also have practical implications for two different types of stakeholders- (i) consumer marketers, and (ii) policymakers and government regulatory authorities. These two sets of stakeholders may find interests in my research outputs. The findings will help develop algorithms for a system using "artificial intelligence" (Jackson, 2019) that will connect with human minds in order to understand their attitudes, and behavioral patterns. This will help government and elite consumer firms to respectively formulate policies and marketing strategies. Additionally, this will also help consumer firms to develop better products based on human needs and desires.

6. Conclusion

Our review has suggested that there is a significant level of interest on surveillance and privacy in IS research but most of the literature is based on design and implementation of the technology pertaining to surveillance, monitoring or protection of data. Although there have been studies conducted about how individuals react to surveillance and address their privacy concerns, there are still quite a few research gaps left about how individuals address their privacy concerns in response to both non-obtrusive and obtrusive surveillance and how such privacy concerns differ at the individual, corporate and societal level. The review also revealed that cultural factor, socio-technical factor and data sensitivity influence people's perception of different design of surveillance technologies and their privacy concerns. Hence, researchers should delve into such influences in IS research and investigate about how such influences may impact the trade-off, if any, among privacy as a value, privacy as a control and privacy as ethics. This will present a complete picture of how people's privacy concerns can be mitigated in response to both non-obtrusive and obtrusive surveillance.

As we know that the field of surveillance and privacy is a multi-disciplinary field (Georgiadou & Fischer-Hübner, 2010). Hence, we propose IS research should appear from the intersections of information technology, sociology, psychology, people, culture, law, information, and organizations. Therefore, non-IS researchers examining the field of surveillance and privacy should be brought into IS- field and investigate the phenomenon from the perspectives of such multi-disciplinary intersections. Moreover, researchers should also investigate the phenomenon of "artificial intelligence" (Jackson, 2019) that can help communicate and understand human minds in relation to using various designs of surveillance technologies. This will help us interpret and understand varying perceptions of people's privacy concerns and how it relates to their cultural and socio-technical factor.

7. References

Abraham, J., Meng, A., Holzer, K. J., Brawer, L., Casarella, A., Avidan, M., & Politi, M. C. (2021). Exploring patient perspectives on telemedicine monitoring within the operating room. *International Journal of Medical Informatics*, *156*, 104595 (1-11).

Abramova, O., Wagner, A., Olt, C. M., & Buxmann, P. (2022). One for all, all for one: Social considerations in user acceptance of contact tracing apps using longitudinal evidence from Germany and Switzerland. *International Journal of Information Management*, *64*, 102473 (1-16)

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making. *MIS Quarterly*, *42*(2), 465–488.

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2021). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society*, *37*(2), 115–127.

Alassad, M., Spann, B., & Agarwal, N. (2021). Combining advanced computational social science and graph theoretic techniques to reveal adversarial information operations. *Information Processing & Management*, *58*(1), 102385 (1-21).

Albrechtslund, A. (2008, March 3). Online social networking as participatory surveillance. *First Monday*, *13*(3).

Allmer, T. (2011). Critical Surveillance Studies in the Information Society. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *9*(2), 566–592.

Andrejevic, M. (2019). Automating Surveillance. *Surveillance & Society*, *17*(1/2), 7–13.

Andrejevic, M., & Burdon, M. (2014). Defining the Sensor Society. *Television & New Media*, *16*(1), 19–36.

Andrejevic, M., Hearn, A., & Kennedy, H. (2015). Cultural studies of data mining: Introduction. *European Journal of Cultural Studies*, *18*(4-5), 379–394.

Anteby, M., & Chan, C. K. (2018). A Self-Fulfilling Cycle of Coercive Surveillance: Workers' Invisibility Practices and Managerial Justification. *Organization Science*, *29*(2), 247–263.

Aspland, D. (2011). The Other Side of "Big Brother." *Journal of Cases on Information Technology*, *13*(2), 34–48.

Bansal, G., & Nah, F. F.-H. (2022). Internet Privacy Concerns Revisited: Oversight from Surveillance and Right To Be Forgotten as New Dimensions. *Information & Management*, *59*(3), 103618 (1–17).

Bayerl, P. S., & Akhgar, B. (2015). Surveillance and falsification implications for open-source intelligence investigations. *Communications of the ACM*, *58*(8), 62–69.

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

Bhatt, P., Vemprala, N., Valecha, R., Hariharan, G., & Rao, H. R. (2022). User Privacy, Surveillance and Public Health during COVID-19 – An Examination of Twitterverse. *Information Systems Frontiers*, *n/a*(n/a), 1–16.

Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorizing surveillance:the panopticon and beyond*. William Pub.

Binhi, V. N. (2009). *Electromagnetic mind control : fact or fiction? a scientific view*. Nova Science Publishers.

Boltanski, L., & ThévenotL. (2006). *On justification : economies of worth*. Princeton University Press.

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online Surveillance

and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606.
Cayford, M., & Pieters, W. (2018). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, *34*(2), 88–103.
Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, *34*(1), 59–80.
Crossler, R. E., & Bélanger, F. (2019). Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. *Information Systems Research*, *30*(3), 995–1006.
Crossler, R., & Posey, C. (2017). Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem. *Journal of the Association for Information Systems*, *18*(7), 487–515.
D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658.
De Moya, J.-F., & Pallud, J. (2020). From panopticon to heautopticon: A new form of surveillance introduced by quantified-self practices. *Information Systems Journals, 30*(6), 940-976.
Deleuze, G. (2013). *Nietzsche and philosophy*. Bloomsbury.
Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316.
Ehrari, H., Ulrich, F., & Andersen, H. B. (2020). Concerns and Trade- Offs in Information Technology Acceptance: The Balance between the Requirement for Privacy and the Desire for Safety. *Communications of the Association for Information Systems*, *47*, 227–247.
Elhai, J. D., Chai, S., Amialchuk, A., & Hall, B. J. (2017). Cross- cultural and gender associations with anxiety about electronic data hacking. *Computers in Human Behavior*, *70*, 161–167.
Elhai, J. D., & Hall, B. J. (2016). Anxiety about internet hacking: Results from a community sample. *Computers in Human Behavior*, *54*, 180–185.
Foucault, M. (2002). *POWER : the essential works of michel foucault 1954-1984.* (J. D. Faubion, Ed.). Penguin Books.
Foucault, M. (2006). *Psychiatric power : Lectures at the Collège de France, 1973-74.* (J. Lagrange, Ed.). Palgrave Macmillan.
Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the Competing Influences of Privacy Concerns and Positive Beliefs on Citizen Acceptance of Contact Tracing Mobile Applications. *Computers in Human Behavior*, *121*, 106806 (1-15).
Fox, G., van der Werff, L., Rosati, P., Takako Endo, P., & Lynn, T. (2021). Examining the determinants of acceptance and use of mobile contact Tracing applications in Brazil: An extended privacy calculus perspective. *Journal of the Association for Information Science and Technology*, *73*(7), 944–967.
Friedwald, M., Finn, R. L., & Wright, D. (2013). Seven Types of Privacy. In S. Gutworth, R. Leenes, P. D. Hert, & Y. Poullet (Eds.), *European Data Protection: Coming of Age* (pp. 3–32). Springer, Dordrecht.
Gao, S., Janowicz, K., & Couclelis, H. (2017). Extracting urban functional regions from points of interest and human activities on location-based social networks. *Transactions in GIS*, *21*(3), 446–467.
Georgiadou, Y., & Fischer-Hübner, S. (2010). Surveillance and Privacy. In J. Berleur, M. D. Hercheui, & L. M. Hilty (Eds.), *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience. HCC CIP 2010 2010. IFIP Advances in Information and Communication Technology* (Vol. 328). Springer, Berlin, Heidelberg.
Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226– 261.
Gozman, D., & Currie, W. (2014). The Role of Investment Management Systems in Regulatory Compliance: A Post- Financial Crisis Study of Displacement Mechanisms. *Journal of Information Technology*, *29*(1), 44–58.
Haggerty, K. D. R., & Ericson, V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622.
Hammonds, J. R. (2015). A Model of Privacy Control: Examining the Criteria That Predict Emerging Adults' Likelihood to Reveal Private Information to Their Parents. *Western Journal of Communication*, *79*(5), 591–613.
Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis : a regression-based approach*. The Guilford Press.
Heath, H., & Cowley, S. (2004). Developing a grounded theory approach: a comparison of Glaser and Strauss. *International Journal of Nursing Studies*, *41*(2), 141–150.
Holt, M., Lang, B., & Sutton, S. G. (2017). Potential Employees' Ethical Perceptions of Active Monitoring: The Dark Side of Data Analytics. *Journal of Information Systems*, *31*(2), 107– 124.
Huang, H., Gartner, G., Krisp, J. M., Raubal, M., & Van de Weghe, N. (2018). Location based services: ongoing evolution and research agenda. *Journal of Location Based Services*, *12*(2), 63–93.
Jackson, P. C. (2019). *Introduction To Artificial Intelligence.* (3rd ed.). New York, USA: Dover Publications, Inc.
Jones, S. (2017). Doing social network ethics: a critical, interdisciplinary approach. *Information Technology & People*, *30*(4), 910–926.
Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387–402.
Kauffman, R. J., Lee, Y. J., Prosch, M., & Steinbart, P. J. (2011). A Survey of Consumer Information Privacy from the Accounting Information Systems Perspective. *Journal of Information Systems*, *25*(2), 47–79.
Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637–667.
Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675– 705.
Klitou, D. (2014). *Privacy-Invading Technologies and Privacy by Design Safeguarding Privacy, Liberty and Security in the 21st Century*. The Hague T.M.C. Asser Press.
Latour, B. (2012). Paris, invisible city: The plasma. *City, Culture and Society*, *3*(2), 91–93.
Leclercq-Vandelannoitte, A. (2010). A critical look at the structurist approach in SI: A comparison with the Foucaldian approach. *Systèmes d'Information & Management*, *15*(1), 35–68.
Leclercq-Vandelannoitte, A., & Aroles, J. (2020). Does the end justify the means?Information systems and control society in the age of pandemics. *European Journal of Information Systems*, *29*(6), 746–761.
Lee, C. S. (2019). Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review*, *43*(6), 952–970.
Lee, J., Cho, D., & Lim, G. (2018). Design and Validation of the Bright Internet. *Journal of the Association for Information Systems*, *19*(2), 63–85.
Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information Systems Frontiers*, *14*(2), 375–393.
Lightfoot, G., & Wisniewski, T. P. (2014). Information asymmetry and power in a surveillance society. *Information and Organization*, *24*(4), 214–235.
Lukes, S. (1974). *Power : a Radical View*. London, UK: Palgrave Macmillan.
Lyon, D. (2007). *Surveillance studies: an overview*. Cambridge Polity Press.
Lyon, D. (2015). *Surveillance after Snowden*. Cambridge Polity Press.
MacAskill, E., Dance, G., Cage, F., Chen, G., & Popovich, N. (2014, March 23). *NSA files decoded: Edward Snowden's surveillance revelations explained*. The Guardian; The Guardian. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1
Maher, N. A., Senders, J. T., Hulsbergen, A. F. C., Lamba, N., Parker, M., Onnela, J.-P., Bredenoord, A. L., Smith, T. R., & Broekman, M. L. D. (2019). Passive data collection and use in healthcare: A systematic review of ethical issues. *International Journal of Medical Informatics*, *129*, 242–247.
Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199.
Mann, S. (2004). Sousveillance: Inverse Surveillance in Multimedia Imaging. *Multimedia 2004: Proceedings of the 12th Annual ACM International Conference on Multimedia*, 620–627.
Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society*, *16*(2), 219–237.
Marder, B., Joinson, A., Shankar, A., & Houghton, D. (2016). The extended "chilling" effect of Facebook: The cold reality of ubiquitous social

networking. *Computers in Human Behavior*, *60*, 582–592.
Martin, K. (2016). Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop? *The Information Society*, *32*(1), 51–63.
Martin, N., Rice, J., & Martin, R. (2016). Expectations of privacy and trust: examining the views of IT professionals. *Behaviour & Information Technology*, *35*(6), 500–510.
Mitchell, S. S. D. (2019). "Warning! You're entering a sick zone": The construction of risks and privacy implications of risk and privacy implications of disease tracking apps. *Online Information Review*, *43*(6), 1046–1062.
Monahan, T. (2016). Built to lie: Investigating technologies of deception, surveillance, and control. *The Information Society*, *32*(4), 229–240.
Morris, B. W., Kleist, V. F., Dull, R. B., & Tanner, C. D. (2014). Secure Information Market: A Model to Support Information Sharing, Data Fusion, Privacy, and Decisions. *Journal of Information Systems*, *28*(1), 269–285.
Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context. *Journal of Service Research*, *15*(1), 76–98.
Mullen, C., & Fox Hamilton, N. (2016). Adolescents' response to parental Facebook friend requests: The comparative influence of privacy management, parent-child relational quality, attitude and peer influence. *Computers in Human Behavior*, *60*, 165– 172.
Muratbekova-Touron, M., & Leon, E. (2021). "Is there anybody out there?" Using a telepresence robot to engage in face time at the office. *Information Technology & People*, *n/a*(n/a), 1–18. https://doi.org/10.1108/itp-01-2021-0080
Nam, T. (2018). Untangling the relationship between surveillance concerns and acceptability. *International Journal of Information Management*, *38*(1), 262–269.
Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of "datification." *The Journal of Strategic Information Systems*, *24*(1), 3–14.
Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027.
Park, Y. J., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303.
Petronio, S. (2013). Brief Status Report on Communication Privacy Management Theory. *Journal of Family Communication*, *13*(1), 6–14.
Petronio, S., & Durham, W. T. (2015). Communication Privacy Management Theory. Significance for Interpersonal communication. In *Relationship-Centered Theories of Interpersonal Communication* (pp. 335–347). Sage Publications.
Petronio, S., & Gaff, C. (2010). Managing privacy ownership and disclosure. In C. Gaff & C. Bylund (Eds.), *Family Communication About Genetics: Theory and Practice* (pp. 120– 135). Oxford University Press.
Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017). Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior*, *75*, 811–825.
Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55.
Pu, W., Li, S., Bott, G. J., Esposito, M., & Thatcher, J. B. (2022). To Disclose or Not to Disclose: An Evaluation of the Effects of Information Control and Social Network Transparency. *Computers & Security*, *112*, 102509 (1–17).
Raab, C. D. (2020). Information privacy, impact assessment, and the place of ethics. *Computer Law & Security Review*, *27*, 105404 (1-16).
Rahimi, R., Khoundabi, B., & fathian, A. (2021). Investigating the Effective Factors of Using mHealth Apps for Monitoring COVID-19 Symptoms and Contact Tracing: A Survey among Iranian Citizens. *International Journal of Medical Informatics*, *155*, 104571(1-10).
Ranzini, G., & Hoek, E. (2017). To you who (I think) are listening: Imaginary audience and impression management on Facebook. *Computers in Human Behavior*, *75*, 228–235.
Reed, L. A., Tolman, R. M., Ward, L. M., & Safyer, P. (2016). Keeping tabs: Attachment anxiety and electronic intrusion in high school dating relationships. *Computers in Human Behavior*, *58*, 259–268.
Regan, P. M. (2000). *Legislating privacy : technology, social values, and public policy*. North Carolina, USA: The University Of North Carolina Press.
Saifuzzaman, M., Ananna, T. N., Chowdhury, M. J. M., Ferdous, M. S., & Chowdhury, F. (2022). A systematic literature review on wearable health data publishing under differential privacy. *International Journal of Information Security*, *n/a*(n/a), 1–26. https://doi.org/10.1007/s10207-021-00576-1
Samarasinghe, N., & Mannan, M. (2019). Towards a global perspective on web tracking. *Computers & Security*, *87*, 101569 (1-14).
Scellato, S., Noulas, A., Lambiotte, R., & Mascolo, C. (2011). Socio- spatial properties of online location--□based social networks. *Proceedings of 5th International AAAI Conference on Weblogs and Social Media*, *5*(1), 329–336.
Schoeman, F. (Ed.). (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, UK: Cambridge University Press.
Schyff, K. van der, Flowerday, S., & Furnell, S. (2020). Duplicitous Social Media and Data Surveillance: An evaluation of privacy risk. *Computers & Security*, *94*, 101822 (1-17).
Sewell, G., & Barker, J. R. (2006). Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance. *Academy of Management Review*, *31*(4), 934–961.
Shaw, S.-L., Tsou, M.-H., & Ye, X. (2016). Editorial: human dynamics in the mobile and big data era. *International Journal of Geographical Information Science*, *30*(9), 1687–1693.
Shiau, W.-L., Shi, P., & Yuan, Y. (2021). A Meta-Analysis of Emotion and Cognition in Information System. *International Journal of Enterprise Information Systems*, *17*(1), 125–143.
Shore, A., Prena, K., & Cummings, J. J. (2022). To share or not to share: Extending Protection Motivation Theory to understand data sharing with the police. *Computers in Human Behavior*, *130*(C), 107188 (1-11).
Sipior, J. (2021). Monitoring Remote Employees at FinPro. *Communications of the Association for Information Systems*, *49*, 304–320.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015.
Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.
Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance. *Journal of the Association for Information Science and Technology*, *71*(9), 1074–1088.
Stiff, C. (2019). The Dark Triad and Facebook surveillance: How Machiavellianism, psychopathy, but not narcissism predict using Facebook to spy on others. *Computers in Human Behavior*, *94*, 62–69.
Strauss, A. L., & Corbin, J. M. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (2nd ed.). Thousand Oak, CA: Sage.
Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly*, *37*(4), 1141–1164.
Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology*, *71*(9), 1129–1142.
Timan, T., Galic, M., & Koops, B. (2017). Surveillance Theory and its Implications for Law. In R. Brwonsword, E. Scotford, & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation & Technology* (pp. 1–24). Oxford, New York: Oxford University Press.
Tokunaga, R. S. (2011). Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. *Computers in Human Behavior*, *27*(2), 705–713.
Urbaczewski, A., & Lee, Y. J. (2020). Information Technology and the pandemic: a preliminary multinational analysis of the impact of mobile tracking technology on the COVID-19 contagion control. *European Journal of Information Systems*, *29*(4), 405–414.
van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *Computers & Security*, *37*, 31–45.
Venkatesh, V., Brown, S., & Sullivan, Y. (2016). Guidelines for Conducting Mixed-methods Research: An Extension and Illustration. *Journal of the*

Association for Information Systems, *17*(7), 435–494.
Wallander, L. (2009). 25 years of factorial surveys in sociology: A review. *Social Science Research*, *38*(3), 505–520.
Williams, K. R., & Hawkins, R. (1986). Perceptual Research on General Deterrence: A Critical Review. *Law & Society Review*, *20*(4), 545–572.
Wills, C. E., & Zeljkovic, M. (2011). A personalized approach to web privacy: awareness, attitudes and actions. *Information Management & Computer Security*, *19*(1), 53–73.
Wnuk, A., Oleksy, T., & Domaradzka, A. (2021). Prosociality and endorsement of liberty: Communal and individual predicto rs of attitudes towards surveillance technologies. *Computers in Human Behavior*, *125*, 106938(1-12).
Xu, H., Teo, H.-H., Bernard C. Y. Tan, & Agarwal, R. (2009). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems*, *26*(3), 135–174.
Zorina, A., Bélanger, F., Kumar, N., & Clegg, S. (2021). Watchers, Watched, and Watching in the Digital Age: Reconceptualization of Information Technology Monitoring as Complex Action Nets. *Organization Science*, *32*(6), 1571– 1596.
Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89.

8. Appendix I

(Step 3 Papers: Please note some duplications at individual, corporate & societal level)

Privacy	Individual	Corporate	Societal
Value (30)	De Moya & Pallud (2020); Abramova et al. (2022); Wnuk et al. (2021); Fox, Clohessy et al. (2021); Fox, Werff et al. (2021); Urbaczewski & Lee (2020); Marder et al. (2016); Reed et al. (2016); Jung et al. (2013); Park et al. (2012); Tokunaga (2011); Abraham et al. (2021); Rahimi et al. (2021); Ehrari et al. (2020); Ranzini, & Hoek (2017)	Stark et al. (2020); Afriat et al. (2020); Mai (2016); Sipior (2021); Morris et al. (2014)	Shore et al. (2022); Wnuk et al. (2021) Fox, Clohessy et al. (2021); Wolfowicz et al. (2021); Fox, Werff et al. (2021); Urbaczewski & Lee (2020); Lee (2019); Leclercq-Vandelannoitte & Aroles (2020); Cayford & Pieters (2018); Nam, T. (2018); Mai (2016); Bayerl & Akhgar (2015); Preibusch (2015); Saifuzzaman et al. (2022); Aspland (2011)
Control (17)	Bhatt et al. (2022); Mullen & Fox (2016); Pu et al. (2022); Crossler, & Posey (2017)	Bansal & Nah (2022); Muratbekova-Touron, & Leon (2021); Zorina et al. (2021); Clarke (2019); Anteby & Chan (2018); Potoglou et al. (2017); Martin (2016); Lightfoot & Wisneiwski (2014); Park & Jang (2014); Wills, & Zeljkovic (2011); Lee & Lee (2012)	Bansal, & Nah (2022); Thompson et al. (2020); Vannini et al. (2019); Potoglou et al. (2017); Lightfoot & Wisneiwski (2014);
Ethics (17)	Alassad et al. (2021); Mitchell (2019); Stiff (2019); Schyff et al. (2020); Samarasinghe & Mannan (2019); Martin et al. (2016); Elhai et al. (2017); Elhai & Hall (2016); Kim et al. (2011)	Jones (2017); Holt et al. (2017); Manohan (2016); Zuboff (2015); Kauffman et al. (2011); Gozman & Currie (2014); Kim et al. (2011)	Mitchell (2019); Jones (2017); Manohan (2016); Kauffman et al. (2011); Maher et al. (2019); van Deursen et al. (2011);