Citizens' Support for AI Security Surveillance Systems: A Social Exchange Perspective

Mahdi Abouei
McMaster University, aboueim@mcmaster.ca

Yufei Yuan
McMaster University, yuanyuf@mcmaster.ca

Citizens' Support for AI Security Surveillance Systems: A Social Exchange Perspective

Short Paper

Mahdi Abouei
McMaster University
Hamilton, ON, Canada
aboueim@mcmaster.ca

Yufei Yuan
McMaster University
Hamilton, ON, Canada
yuanyuf@mcmaster.ca

Abstract

Artificial intelligence (AI) has tremendously transformed the patterns of security surveillance employed by governments. Although the primary goal of security surveillance is to maintain social order and enhance citizens' protection, significant privacy concerns were raised for citizens given the unprecedented amount of personal data accessed by various types of AI-powered security surveillance (AISS) systems, such as facial recognition technologies. Nonetheless, policymakers and academia rarely paid attention to the citizens' views as the main stakeholders of these systems. Motivated by this, in this study, we develop a theoretical model drawing on the assertions of the Social Exchange Theory (SET) to explain the factors and mechanisms that influence citizens' support for AISS. In particular, we elaborate on the role of privacy-security tradeoff, trust, and power and their interplay in explaining citizens' supportive attitudes. Potential contributions from this research to theory and practice are also outlined.

Keywords: Artificial intelligence, security surveillance, privacy-security tradeoff, social exchange, citizens' support

Introduction

Government security surveillance measures have long been critical to maintaining social security and protecting citizens' lives. These measures, specifically, became of great consequence after the terrorist attacks of September 11th in New York City and the London subway bombing of 2005 (Trüdinger & Steckermeier, 2017). In response to these threats, governments have continuously employed restricting legislations (e.g., anti-terror laws passed in France in 2014) and advanced surveillance technologies. Specifically, the use of Artificial Intelligence (AI) has transformed basic patterns of surveillance with extraordinary capabilities such as predictive policing, crowd control, and public sentiment monitoring (Van Zoonen, 2016). A recent report by AI Global Surveillance Index indicated that, as of 2019, at least 75 countries had been actively using AI technologies for surveillance purposes (Feldstein, 2019). However, the extensive use of AI-powered Security Surveillance (AISS) comes at a tradeoff. Though living establishments are becoming safer and more secure, AISSs are subjecting citizens to an increasing amount of permanent surveillance, increasing the risk of infringements of privacy and a restriction of civil rights (Srivastava et al., 2017). AISS intrudes into personal space by allowing governments to gather unprecedented private and public information about citizens. An authority that has spurred considerable fears of shaping Orwellian surveillance societies (Zuboff et al., 2019). In this respect, finding the right balance between privacy and security has long been at the core of the debates on surveillance (Verhelst et al., 2020). Nevertheless, academia and policymakers have rarely included citizens' perspectives, even though citizens' support is vital for successfully deploying social control systems (Kininmonth et al., 2018).

An AISS is an integrated system that incorporates AI capabilities such as information acquisition, logical reasoning, and self-correction to watch, monitor, record, and process the behavior and activities of humans,

objects, and events to enhance public security (Bundy, 2017). AISS relies primarily on the principles of datafication where surveillance systems are fed vast amounts of data from different sources such as surveillance cameras, smartphones, and social media platforms and vested with AI algorithms to passively and actively identify, monitor, and track online and physical spaces to predict and respond to potential and actual threats with high accuracy and almost in real-time (Fontes et al., 2022). AI's power to enrich and facilitate surveillance endeavors due to its interconnectedness, increased capacity to process data, and ability to automate tasks has opened new forms of security surveillance and enhanced the traditional means tremendously. For example, AI has transformed surveillance cameras into active observers with the capability to detect and alert about security threats such as weapons and suspicious objects, using advanced deep learning models without human intervention (Ahmed & Echi, 2021). Combining AI-powered facial recognition with biometric data such as fingerprints and iris scans can also be used for authentication and identification (Javvaji, 2023). Additionally, integrated with predictive analytics, AISS can be used to monitor communication networks to identify potential terrorist attacks, track criminals and other illegal behavior using Facial Recognition Technologies (FRT), and collect forensic evidence through video recordings (Allam & Dhunny, 2019). Several private companies, with Chinese and Americans at the front, are progressively globalizing the AISS market (Feldstein, 2019). Avista smart sensors, for example, an AI video surveillance system established in Minnesota, US, is a successful example of the implementation of AISS that helped reduce the crime rate in Minnesota by almost 75% (Srivastava et al., 2017).

However, while AISS has significant potential to improve public safety, widespread ethical criticism is directed toward this technology due to its capacity to compromise citizens' privacy significantly. In particular, deploying AISS allows governments to establish a network of continuous monitoring of citizens in public and private spheres that allows for collecting numerous identifiable data, such as behavioral data based on live video recordings and social media activities on citizens, with the potential to enforce mass surveillance and social control (Javvaji, 2023). AISS's privacy risks originate from its inherent data-driven nature, whose accuracy depends, in essence, on the quantity and quality of data collected to extract both personalized (i.e., direct surveillance of individual targets) and generalized knowledge (e.g., on spaces, services, and societies) (Fontes et al., 2022). AISSs often run on sophisticated models that require access to large amounts of data to decipher the complexities within social phenomena and efficiently respond to security threats while mitigating potential biases such as racializing vulnerable groups. However, the less transparent and, in some cases, inconsentable nature of AISS blurs the boundaries delineated to protect citizens' privacy, which can lead to the erosion of civil liberties and democratic values (Selinger & Hartzog, 2020). Moreover, unlike the centralized approaches used in traditional public security, AISS's operation heavily relies on transnational cooperation among security experts and various interconnected private and public surveillance networks (Feldstein, 2019). For example, Clearview AI's (an American private company) facial recognition system, which more than 600 law enforcement agencies worldwide use as an investigative resource, has induced significant concerns about citizens' privacy after a data breach that revealed numerous commercial enterprises on the company's customers list (Hill, 2020, Jan 18). In fact, the interdependency of governments and private sector on feeding AISS with data available to private entities would increase the probability of the abuse or misuse of personal data accessed by third parties, thus violating citizens' privacy and tampering their rights to freedom.

Past literature in different disciplines, such as information systems and political sciences, indicates that the common wisdom about deploying AISS is the traditional privacy-security tradeoff where citizens' judgments about surveillance systems are primarily formed due to this cognitive equilibrium. For example, Ezzeddine et al. (2023) explored citizens' views on AI use by police forces and identified five perspectives based on citizens' privacy and security perceptions. Kostka et al. (2021) also investigated the acceptance of FRT in China, Germany, the UK, and the US and found that socio-demographic factors such as age, gender, and social context can explain the variabilities in citizens' acceptance of FRT caused by citizens' perceptions of security benefits and privacy risks. Nonetheless, a growing body of research is referring to the inefficiency of this framework, calling for deeper quantitative empirical investigation by offering theoretically sound explanations of the role of potential factors in explaining citizens' judgment and attitudes toward AISS (Saheb, 2022; Saura et al., 2022). Prior research argues that governments and citizens are entities within a social structure interacting through various social exchange processes (Alford, 2002). It is also noted that exchange outcomes can significantly vary based on the level of trust among exchange parties and the power dynamics governing the exchange relationships (Cropanzano et al., 2017). In our context, studies have shown that the strengthened covert and overt aspects of AISS can trigger a sense of distrust among citizens,

which in turn can deteriorate the legitimacy of governments and, thus, citizens' support for AISS (Duberry, 2022). A recent study of nine European Union countries also showed that citizens tend to trade their privacy with security only if AISSs are deployed in a way that demonstrates the trustworthiness of the governments (Degli Esposti et al., 2021). Indeed, trust is a significant factor in the relational aspect of many surveillance systems, and it has a vital role in establishing and sustaining the connections that form the foundation of government institutions' legitimacy and promoting outcomes that are advantageous to society. Power dynamics are another factor affecting social exchange outcomes and are central to any surveillance-related topic. It is argued that the use of AISS can result in an asymmetry of power among citizens and governments, which can risk principles of liberal democracy, such as privacy (Smith & Miller, 2022). Zuboff et al. (2019) has warned about the danger of a powerful, ubiquitous, networked institutional regime leading us toward a new world of surveillance capitalism. A world where all human experiences are recorded, modified, and commodified, and citizens are no longer presumed innocent but rather ranked based on their risk profiles (Selinger & Hartzog, 2020). Zuboff also argues that the "Big Other is the sovereign power of the near future that annihilates the freedom achieved by the rule of law" (Zuboff, 2015: 81-2). Accordingly, it is crucial to incorporate the trust and power relationships between governments and citizens along with the privacy-security tradeoff arguments when formulating citizens' views on AISS deployment.

The current study addresses the following research question: *How does deploying AISS influence citizens' support for AISS?* We base our arguments on the premises of the social exchange theory (Blau, 1968; Molm, 1990) and the literature on AISS and propose a theoretical model that explains the factors influencing citizens' support for deploying AISS. Specifically, we theorize that citizens' support for AISS occurs in exchange for the security offered by AISS. However, the extent of this exchange is influenced by an interplay of citizens' rationality, trust in government, and power imbalance caused by the deployment of AISS. To address the proposed research question, we will follow a survey-based design methodology and collect data via a stratified random sampling technique on citizens living in countries with active AISS establishments to test the proposed theoretical model. The results of this study will contribute both to theory and practice. This study offers an integrative theoretical model explaining the socio-technical aspects of using AI for security surveillance. It also helps policymakers inform their strategies related to the deployment of AISS.

Theoretical Background

Social Exchange Theory (SET) is a broad conceptual paradigm that can be applied to various social life phenomena (Cropanzano et al., 2017). These models primarily treat social exchange as sequential transactions of tangible and intangible resources between two or more parties, where interdependence is considered a defining characteristic of social exchange (Mitchell et al., 2012). According to SET, parties exchange valued resources primarily through the rules of rationality, reciprocity, and negotiation. The rule of rationality indicates that the primary motive of social relations is self-interest, and thus, the reward and cost structures of the relationships account for the patterns of interactions (Homans, 1958). In other words, while exchanging valued resources, parties behave in a way that the outcome of the exchange maximizes their gains and minimizes losses. The rule of reciprocity, however, refers to the obligation caused by the reception of benefits whereby one party tends to repay the deeds of another party (Blau, 1968). This rule argues that social exchanges, unlike economic exchanges which tend to be quid pro quo, are more flexible and open-ended (Cropanzano et al., 2017). In this view, social exchange is often seen as a long-term, reciprocal relationship where trust between the exchange parties is central to the sustainability of the social relationship (Zafirovski, 2005). Molm et al. (2000: 1402) define trust in social exchange as "expectations that an exchange partner will behave benignly, based on the attribution of positive dispositions and intentions to the partner in a situation of uncertainly and risk." The nature of trust, however, may differ given the quality of exchange relationships. While at the early stages of a relationship, trust is calculus-based, it transforms to be based on shared desires and intentions with the gradual expansion of exchange transactions because the regular discharge of obligations proves one's trustworthiness and quality for receiving further credit (Mitchell et al., 2012). Moreover, an individual's investments by fostering a friendly relationship with others commit them to the relationship, making it disadvantageous to abandon the partnership in favor of another, leading to additional trust and not evading their obligations (Blau, 1968).

Finally, the negotiation rule presumes that social exchanges can be subject to explicit terms and arrangements where transactions occur to achieve a more beneficial outcome (Mitchell et al., 2012). Negotiated exchanges are based on expectations of benefits obtained because of the stated agreement and,

thus, are less reliant on assessments of risks and trustworthiness of the other parties. Instead, the definitive factor in negotiated exchanges is the power imbalance among the exchange actors, which can determine the parties' ability to take advantage of the exchange outcome (Emerson, 1962). Power imbalances occur due to actors' control over valued resources. In negotiated exchanges, actors with high power tend to direct the outcome of the exchange toward their interest, knowing the other actors' dependency upon their resources (Molm et al., 1999). However, the instability caused by power imbalances often leads the low-power actors to resist agreement and push negotiation outcomes toward their proportionate power advantage. Like negotiated exchanges, power is also essential in reciprocal exchange relationships yet with different consequences. While power inequality in negotiated exchanges drives behaviors through the increased costs incurred by the high-power on the lower-power actor, in reciprocal exchanges, power inequality benefits high-power actors by withholding rewards given their lower reciprocity and more opportunity to partake in other exchanges (Molm et al., 1999). In return, low-power actors take balancing actions such as abandoning the relationship, locating alternative resources, status-giving, or engaging in collective actions.

In this study, we draw on SET to examine how the interplay of the exchange rules and influential factors involved in the social exchange between governments and citizens affect citizens' support for AISS deployment. Our motivation for using SET in our context is two-fold. First, SET allows us to extend the theoretical formulations concerning the deployment of surveillance systems beyond the privacy-security tradeoff and view this phenomenon from a socio-technological perspective. Second, SET has been used and validated in various contexts, such as individuals' workplace and law compliance attitudes and behaviors (e.g., Cropanzano et al. (2017)), and thus is suitable in our context to study citizens' support for AISS.

Research Model and Hypotheses

Figure 1 shows the research model that we propose to address this study's research question.

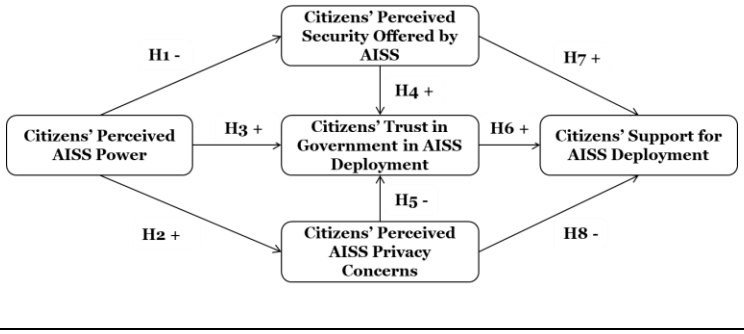

Figure 1. Research Model

AISS Power and Privacy-Security Tradeoff

Power in social exchange refers to a party's influence on other exchange actors given possession of valuable resources (Blau, 1968). In such relationships, parties take advantage of the outcome of exchange based on the power-dependence relation (Emerson, 1962). This is in accord with the power-dependence theory, which considers resource dependence in explaining social exchange behaviors. According to SET, power structure can influence exchange outcomes regarding the rewards and punishments distributed among exchange parties (Molm, 1990). Specifically, the power imbalance leads to the asymmetrical distribution of the exchange where benefits are shifted toward the power-advantaged actor, motivating the disadvantaged actor to engage in non-reciprocal behaviors. Furthermore, SET argues that power imbalance in exchange relations might cause the low-power actors to perceive the interaction negatively (Molm et al., 1999).

In our context, governments' ability to control and manipulate citizens' activities using AISS and citizens' dependence on government interventions to ensure their security shape the governments' power base. On the other hand, citizens' power stems from governments' dependency on citizens for achieving political legitimacy, which gives citizens the right to demand and the ability to negotiate with governments to secure their interests. This mutual dependence, however, varies in strength and direction, and thus, the power imbalance can emerge as a consequence (Fontes et al., 2022). If citizens think that AISS would afford

governments the power to exert unsolicited control through the intrusion of their privacy (e.g., by continuously monitoring citizens and profiling them based on their behavioral patterns), the power imbalance will shift to the government's advantage and thus lower the expected reward citizens achieve (i.e., perceived security). Besides, it is expected that the negative perceptions associated with the power imbalance for citizens (i.e., low-power actors) lead them to experience intensified privacy concerns, which, in return, may trigger a backlash (Feldstein, 2021). The findings of previous studies in public-government relations contexts also support the above arguments. Nunkoo (2016), for example, found that residents who feel more powerful view tourism as more beneficial and less costly. Therefore, based on the theoretical discussion above and the empirical evidence provided, we argue that citizens' privacy-security tradeoff is influenced by the extent of power imbalance caused by the deployment of AISS and hypothesize that:

H1. Citizens' perception of AISS power is negatively related to their perceived security.
H2. Citizens' perception of AISS power is positively related to their privacy concerns.

AISS Power and Citizens' Trust in Government in AISS Deployment

Despite the criticality of trust in social exchange, analysis of a social exchange without considering a vital source of variation in trust, namely, power, may be misleading. As Cook et al. (2005) discussed, these two constructs should be considered together in any theory dealing with the world of social relations and institutions. Two opposing theoretical accounts were offered to explain the interplay of power and trust in social exchanges. First, the rationality account argues that given the availability of alternatives, power-advantaged actors are motivated to behave opportunistically, and thus, the power imbalance would result in low-power actors trusting high-power actors less (Mitchell et al., 2012). In contrast, the motivated cognition account argues that low-power people are motivated to alleviate cognitive dissonance inherent to unpleasant feelings of dependence rather than following the rules of rationality (Weber et al., 2004). Therefore, they are likely to view the high-power actors as more trustworthy regardless of supporting evidence to protect themselves from the potential harms of power disadvantage. However, high-power actors are less willing to be involved in motivated cognition and, therefore, have less intense perceptions of trustworthiness, resulting in comparatively lower trust. Schilke et al. (2015) tested the above hypotheses and reported confirming evidence that an actor's power negatively affects their trust in others. They suggest that low-power actors often trust more compared to high-power actors to maintain their status. Smith and Overbeck (2014) also indicate that, due to the same reason, many people admire power holders and hold a positive view of them. Following the same logic, we argue that citizens may trust in governments in AISS deployment more when they perceive an imbalance of power toward governments offered by AISS since they tend to avoid facing the reality that governments would actually misuse AISS power and behave against the interest of citizens. Hence, following this theoretical expression and argument, we hypothesize that:

H3. Citizens' perception of power imbalance caused by AISS positively relates to their trust in governments in AISS deployment.

Privacy-Security Tradeoff and Trust in Government in AISS Deployment

Institutional theories treat trust as a product of institutional performance, capable of being enhanced or eroded according to the behavior of the institutions. In fact, trust can be seen as a logical response to the performance of government institutions rather than a blind belief (Goold, 2009). SET argues that, in a social exchange relationship, the trustworthiness of another partner is determined by an exchange partner's assessment of positive and negative outcomes. Mainly, in the initial stages of exchange (e.g., deployment of a new surveillance system), trust is formed based on the expected cost-benefit calculations (Mitchell et al., 2012). Therefore, when governments decide to deploy new AISS, citizens' trust in governments will be affected by the expected outcomes, including the level of security provided and threats to their privacy.

Governments often justify the deployment of AISS due to its power to afford additional layers of protection to citizens. When citizens benefit from deploying AISS, such as automated detection of suspicious objects using FRT or capturing criminals using unmanned drones, their trust in security authorities on the benign use of AISS will increase. However, citizens' legitimate reasons to be concerned about the government's abuse of citizens' personal data, such as social behavior manipulation using real-time sentiment analysis techniques, would undermine the state authorities' trustworthiness in using AISS. In this respect, Saura et al. (2022) argued that the increasing trend toward higher levels of state surveillance using AI-power

technologies can weaken established governance norms and, thus, harm citizens' trust due to privacy, identity, and personal liberty threats. Duberry (2022) also argued that despite the enhanced security achieved by using AI in state surveillance, AISS's potential to intrude on citizens' right to privacy can challenge the trust relations between citizens and governments. These theoretical suppositions and empirical findings suggest that the positive and negative outcomes of deploying AISS may influence citizens' trust in governments. Specifically, higher levels of perceived security are expected to increase citizens' trust in their government, while greater concerns about privacy are likely to reduce it. Thus, we hypothesize that:

H4. Citizens' perceived security offered by AISS is positively related to their trust in governments.
H5. Citizens' perceived privacy concern caused by AISS is negatively related to their trust in governments.

Citizens' Trust in Government in AISS deployment and Support for AISS

Political scientists aiming at understanding citizens' trust relationship with governments view trust as an aspect of legitimacy and citizens' beliefs that the political system or some of it will produce preferred outcomes even in the absence of constant scrutiny (Sønderskov & Dinesen, 2016). According to SET, trust is a binding glue in exchange relationships since it allows exchange parties to carry on resource transactions with the acceptance of some level of vulnerability given their positive interactions (Zafirovski, 2005). In fact, trusting parties in a social exchange are motivated to act upon their trust beliefs beyond basic judgments on actual expectations of benefits. In our context, when governments deploy AISS, citizens would refer to their deep beliefs and concerns shaped over their experience of living under the political system. Under circumstances that citizens' prior interactions with governments (e.g., traditional state surveillance) were harmless, they would likely be more willing to support AISS as another initiative led by governments given the expectancy that governments will behave similarly in the new interaction. In this respect, previous studies has examined the role of trust in government in forming citizens' attitudes toward government surveillance. Degli Esposti et al. (2021), for example, based on a survey of nine EU countries, found that citizens are more willing to accept digital surveillance technologies when they find security agencies trustworthy. Similarly, the findings of Ioannou and Tussyadiah (2021)'s study on government surveillance during the COVID-19 pandemic point to the key role of trust in government in the citizens' acceptance of surveillance technologies. Sapp et al. (2022) also argue that citizens' trust in governments can act as indicators of a government's competency and legitimacy required for the administration of AISS, contributing to citizens' support for AISS deployment. Overall, the results of these studies tend to support the idea that citizens' trust in governments positively influences their support for security surveillance policies and measures, including the use of AISS. Therefore, we hypothesize that:

H6. Citizens' trust in governments in AISS deployment is positively related to their support for AISS.

Privacy-Security Tradeoff and Citizens' Support for AISS

According to SET, the rule of rationality motivates individuals to partake in exchanges that maximize their benefits while reducing the costs associated with the exchange (Homans, 1958). Therefore, it is expected that individuals tend to increase their involvement in exchange relationships to the extent of benefits they obtain and disengage from the exchange when the costs of engagement increase. In our context, supporting AISS is the valuable resource that citizens provide to governments in exchange for the additional layers of protection they receive by the establishment of AISS. Therefore, it is likely that citizens' support for AISS deployment is influenced by the extent of protection it offers. Prior studies argued that convenience and security are the foremost notions on the minds of citizens when facing digital surveillance systems (Kostka et al., 2021). Ezzeddine et al. (2023) also found that, despite citizens' divergent views on AISS, they support AISS primarily for the safety and protection afforded by AI capabilities. In fact, the underlying rationale for supporting AI surveillance measures is AI's power to collect and process in real-time an extensive amount of personal and environmental data that allows public security authorities to intervene in an intelligent, targeted manner against emerging threats and possibly disrupt them before their occurrence (Fontes et al., 2022). Therefore, it is likely that citizens' perceptions of the security offered by obtain motivate them to maintain the exchange relationship by supporting AISS deployment. Hence, we hypothesize that:

H7. Citizens' perceived security offered by AISS is positively associated with their support for AISS.

However, this seemingly beneficial transaction occurs at the cost of citizens' privacy. According to SET, individuals' motivation to maximize the net gain from transactions leads them to avoid exchange

relationships that incur high costs (Blau, 1968). Privacy concerns have long been known as a significant harming factor accounting for negative attitudes and resistance toward surveillance systems (e.g., Dinev et al. (2008)). AISS characteristics of integration and automation, for example, increase the risk of mass surveillance and, thus, the likelihood of privacy violations and misuse of private information (Park & Jones-Jang, 2022). For example, AISS can unwantedly monitor and gather personal information that could be used for purposes other than security surveillance such as when surveillance is conducted in collaboration with private sector parties. In this respect, van den Broek et al. (2017) work on a series of security research projects, namely, PRISMS, PACT, and SurPRISE, revealed that European citizens' high level of privacy concerns negatively affected acceptance levels of surveillance systems. Therefore, citizens' intentions to support AISS in exchange for security are expected to diminish along with their concerns about privacy violations caused by AISS. Accordingly, we hypothesize that:

H8. Citizens' privacy concerns caused by AISS are negatively associated with their support for AISS.

Proposed Method

The proposed research model will be empirically validated through an cross-sectional online survey of citizens from different countries that have invested in AISS (e.g., the US, China, and Germany). We follow the stratified random sampling technique to reflect the geographical distribution of the residential area (Zikmund, 1997). Specifically, the sample size for each country will be determined by their proportional population. Participants are citizens above 18 years old who live in their country of citizenship. We recruit participants via an online platform where they respond to a structured survey questionnaire, including the measurement items related to the constructs within the research model and control variables. We adopt from and develop measurement scales based on the extant literature and adapt them to the AISS context to ensure content validity. In particular, we will adapt the measurement items from Steinfeld (2017) to capture citizens' support for AISS. Citizens' perceived security obtained by AISS deployment will be measured by adapting the 5-item reflective scale developed by Gurinskaya (2020) for the security benefits of state security surveillance. Citizens' trust in government in AISS deployment will also be operationalized by adapting the 4-item reflective scale from Thompson et al. (2020) used for trust in political institutions. Finally, following the procedure suggested by MacKenzie et al. (2011), we will develop new measurement scales for citizens' perceived privacy AISS concerns and AISS power to operationalize the specific privacy concerns raised and power gained by the employment of AI in security surveillance endeavours. All the measurement items will be measured on a 7-point Likert scale, and a pilot survey of 50 participants will be conducted to test the reliability and validity of measurement instruments and apply potential refinements.

Next, we will run the main study by recruiting a larger sample of 250 participants. In this step, we examine the constructs' reliability as well as convergent and discriminant validity to validate the measurement using the full sample data. The structural model will be tested using SmartPLS 4.0 following the Partial Least Squares Structural Equation Modeling technique (Hair Jr et al., 2017). First, the explanatory and predictive power of the model will be evaluated using in-sample and out-of-sample predictiveness criteria and model fit indices. Then, the significance of the model paths will be tested using t-statistics and bootstrapping. In the analysis, we will also control for age, gender, AISS type, and deployment context to account for the differences that may confound the results (Kostka et al., 2023).

Conclusion

The study has potential contributions to theory and practice. This study leverages social exchange theory and the literature on AI, political science, and information systems to propose a theoretical model that explores the factors and mechanisms affecting citizens' support for deploying AISS by governments. Using this integrative view, this study can advance our understanding of the interplay of the social and individual factors relevant to security surveillance research. It also would be an addition to the information systems literature by empirically testing a theoretical model that explains the socio-technical mechanisms that influence human actors' perceptions and behavioral reactions to a new breed of information technologies (i.e., AISS) within the social exchange structure. The results of this study can also have implications for policymakers. Many countries worldwide are investing in AISS to increase their social security strength. However, governments should be aware of the potential impact of massive surveillance on citizens' trust and public-state power dynamics, which can influence the entire framework of democracy. The findings of

this study can help policymakers make informed strategies in the AISS deployment process that may meet its intended goals and reduce the costs associated with these systems, including privacy concerns.

References

Ahmed, A. A., & Echi, M. (2021). Hawk-eye: An ai-powered threat detector for intelligent surveillance cameras. *IEEE Access*, *9*, 63283-63293.

Alford, J. (2002). Defining the client in the public sector: A social-exchange perspective. *Public administration review*, *62*(3), 337-346.

Allam, Z., & Dhunny, Z. A. (2019). On big data, artificial intelligence and smart cities. *Cities*, *89*, 80-91.

Blau, P. M. (1968). Social exchange. *International encyclopedia of the social sciences*, *7*, 452-457.

Bundy, A. (2017). Preparing for the future of Artificial Intelligence. In: Springer.

Cook, K. S., Hardin, R., & Levi, M. (2005). *Cooperation without trust?* Russell Sage Foundation.

Cropanzano, R., Anthony, E. L., Daniels, S. R., & Hall, A. V. (2017). Social exchange theory: A critical review with theoretical remedies. *Academy of Management Annals*, *11*(1), 479-516.

Degli Esposti, S., Ball, K., & Dibb, S. (2021). What's in it for us? Benevolence, national security, and digital surveillance. *Public administration review*, *81*(5), 862-873.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233.

Duberry, J. (2022). AI in public and private forms of surveillance: Challenging trust in the citizen-government relations. In *Artificial Intelligence and Democracy* (pp. 93-125). Edward Elgar Publishing.

Emerson, R. M. (1962). Power-dependence relations. *American sociological review*, 31-41.

Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Safety, privacy, or both: evaluating citizens' perspectives around artificial intelligence use by police forces. *Policing and Society*, 1-16.

Feldstein, S. (2019). *The global expansion of AI surveillance* (Vol. 17). Carnegie Endowment for International Peace.

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, *71*, 102137.

Goold, B. (2009). Technologies of surveillance and the erosion of institutional trust. *Technologies of InSecurity. The Surveillance of Everyday Life*, 207-218.

Gurinskaya, A. (2020). Predicting citizens' support for surveillance cameras. Does police legitimacy matter? *International journal of comparative and applied criminal justice*, *44*(1-2), 63-83.

Hair Jr, J. F., Babin, B. J., & Krey, N. (2017). Covariance-based structural equation modeling in the Journal of Advertising: Review and recommendations. *Journal of Advertising*, *46*(1), 163-177.

Hill, K. (2020, Jan 18). The Secretive Company That Might End Privacy as We Know, The New York Times. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Homans, G. C. (1958). Social behavior as exchange. *American journal of sociology*, *63*(6), 597-606.

Ioannou, A., & Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society*, *67*, 101774.

Javvaji, S. (2023). SURVEILLANCE TECHNOLOGY: BALANCING SECURITY AND PRIVACY IN THE DIGITAL AGE. *EPRA International Journal of Multidisciplinary Research (IJMR)*, *9*(7), 178-185.

Kininmonth, J., Thompson, N., McGill, T., & Bunn, A. (2018). Privacy concerns and acceptance of government surveillance in Australia.

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, *30*(6), 671-690.

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, *40*(1), 101761.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS quarterly*, 293-334.

Mitchell, M. S., Cropanzano, R. S., & Quisenberry, D. M. (2012). Social exchange theory, exchange resources, and interpersonal relationships: A modest resolution of theoretical difficulties. In *Handbook of social resource theory* (pp. 99-118). Springer.

Molm, L. D. (1990). Structure, action, and outcomes: The dynamics of power in social exchange. *American sociological review*, 427-447.

Molm, L. D., Peterson, G., & Takahashi, N. (1999). Power in negotiated and reciprocal exchange. *American sociological review*, 876-890.

Molm, L. D., Takahashi, N., & Peterson, G. (2000). Risk and trust in social exchange: An experimental test of a classical proposition. *American journal of sociology*, *105*(5), 1396-1427.

Nunkoo, R. (2016). Toward a more comprehensive use of social exchange theory to study residents' attitudes to tourism. *Procedia Economics and Finance*, *39*(588), 30303-30303.

Park, Y. J., & Jones-Jang, S. M. (2022). Surveillance, security, and AI as technological acceptance. *Ai & Society*, 1-12.

Saheb, T. (2022). Ethically contentious aspects of artificial intelligence surveillance: a social science perspective. *AI and Ethics*, 1-11.

Sapp, S. G., Dorius, S. F., Bertelson, K. A., & Harper, S. B. (2022). Public support for government use of network surveillance: An empirical assessment of public understanding of ethics in science administration. *Public Understanding of Science*, *31*(4), 489-506.

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 101679.

Schilke, O., Reimann, M., & Cook, K. S. (2015). Power decreases trust in social exchange. *Proceedings of the National Academy of Sciences*, *112*(42), 12950-12955.

Selinger, E., & Hartzog, W. (2020). The inconsentability of facial surveillance. *Loy. L. Rev.*, *66*, 33.

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, 1-9.

Sønderskov, K. M., & Dinesen, P. T. (2016). Trusting the state, trusting each other? The effect of institutional trust on social trust. *Political Behavior*, *38*, 179-202.

Srivastava, S., Bisht, A., & Narayan, N. (2017). Safety and security in smart cities using artificial intelligence—A review. 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence,

Steinfeld, N. (2017). Track me, track me not: Support and consent to state and private sector surveillance. *Telematics and Informatics*, *34*(8), 1663-1672.

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.

Trüdinger, E.-M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly*, *34*(3), 421-433.

van den Broek, T., Ooms, M., Friedewald, M., van Lieshout, M., & Rung, S. (2017). Privacy and security: Citizens' desires for an equal footing. In *Surveillance, privacy and security* (pp. 15-35). Routledge.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.

Verhelst, H. M., Stannat, A., & Mecacci, G. (2020). Machine learning against terrorism: how big data collection and analysis influences the privacy-security dilemma. *Science and engineering ethics*, *26*, 2975-2984.

Weber, J. M., Malhotra, D., & Murnighan, J. K. (2004). Normal acts of irrational trust: Motivated attributions and the trust development process. *Research in organizational behavior*, *26*, 75-101.

Zafirovski, M. (2005). Social exchange theory under scrutiny: A positive critique of its economic-behaviorist formulations. *Electronic journal of sociology*, *2*(2), 1-40.

Zikmund, W. (1997). Business Research Method (Fifth). In: Orlando: Harcourt Brace College Publishers.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89.

Zuboff, S., Möllers, N., Wood, D. M., & Lyon, D. (2019). Surveillance capitalism: An interview with shoshana zuboff. *Surveillance & Society*, *17*(1/2), 257-266.