Qualitative Research Review Letter
https://qrrl.net/index.php/Journal/about
Online ISSN: 3007-0082
Print ISSN: 3007-0074
Vol. 3 No. 3 (2025)

EXPLORING USERS' PERCEPTIONS AND EXPERIENCES OF PRIVACY AND SURVEILLANCE IN PUBLIC INFORMATION ACCESS ENVIRONMENTS: A QUALITATIVE STUDY

[1]Zakir Khan, [2]Dr. Rahim Jan, [3]Izhar Muhammad, [4]Shehla Robab, [5]Irum Hassan, [6]Muhammad Shahab

[1]MPhil Scholar, Department of Library & Information Science Khushal Khan Khattak University Karak, KPK, Pakistan. zakirkhanmlis@gmail.com
[2]Assistant Professor, Department of Library & Information Science, Khushal Khan Khattak University, Karak, Pakistan rahimjanrajjar@gmail.com
[3]Lecturer, Department of Library & Information Science, Khushal Khan Khattak University, Karak, Pakistan izharmlis@yahoo.com
[4]MPhil Scholar, Department of Library & Information Science Khushal Khan Khattak University Karak, KPK, Pakistan shehlarobab649@gmail.com
[5]MPhil Scholar, Department of Library & Information Science Khushal Khan Khattak University Karak, KPK, Pakistan irumhassan860@gmail.com
[6]Ph.D Scholar, Department of Library & Information Science, Khushal Khan Khattak University, Karak, Pakistan muhammad.shahab@kkkuk.edu.pk

Abstract

This qualitative method inspects users' insights and skills regarding confidentiality and surveillance in public information access environment, such by means of libraries, internet cafés, and public Wi-Fi zones—frameworks usually observed as open, representative spaces for the permitted conversation of ideas and information. The rising integration of biometric documentation systems, surfing antiquity followers, facial acknowledgment cameras, and online data gathering approaches has shaped a distinguished struggle between the compensations of suitability and the protection of personal confidentiality. Using inclusive, semi-structured interviews and thematic examination, the study exposes varied stages of user consciousness, fluctuating from negligible acknowledgement of important monitoring methods to a skilled understanding of multifaceted surveillance methods. Members conveyed unsure feelings, commonly complementary advanced protection, working effectiveness, and instant connectivity beside the risks of summarizing, data misappropriation, and the progressive failure of sureness in public access zones. Many defendants experiential a preventive effect on their information-seeking performance when aware of surveillance. The results highpoint that while surveillance may improve operative competence, it strength corrode the essential intellect of liberty within public information environments. The study advocates for translucent strategy outlines, context-specific confidentiality defenses, and extensive digital literateness creativities to train residents with the essential expertise to navigate these surveilled settings sensibly and assuredly.

KEYWORDS: Privacy, Surveillance, Public Information Access, Qualitative Research, Digital Rights, User Perceptions

INTRODUCTION

Background of the Study

One remarkable revolution that has occurred in the 21st era is the way people look for, use, and involve with information. The propagation of digital skill and the constriction of security measures across diverse methods and organizations are the important reasons of this change (Lyon, 2018; Zuboff, 2019). Libraries, CRCs, academic organizations, and government information centers are examples of public information access settings that have distorted into complicated, linked digital environments, increasing beyond their traditional physical limitations. The appearances between public space and individual confidentiality have indistinct and are passionately discussed in these situations (Solove, 2021).

In today's data-driven culture, digital substructures often act as mediators, collecting, storing, and examining user performance in real-time. Imperceptible and unrestrained systems of monitoring, such as tracking users' IP addresses, biometric identifiers, and exploration pasts, are predominant when people use public information methods (Andrejevic, 2020; Richards & Hartzog, 2022). There is a thoughtful exertion to collect behavior data, strengthen organizational oversight, and development a diversity of recognized, economic, or governmental objectives through these monitoring actions; they are not only passive or incidental. Difficulties with consent, specific activity, and the public's right to know about one's private information are transported to light by the increasing reception of such actions (Bauman et al., 2014).

There is continuing discussion over the perception of privacy, which was previously seen as an individual's right inside generous democratic organizations (Regan, 2022). The existence of monitoring skills creates an inconsistency in public information spaces, which are intended to be free, open, and self-governing places of access. Study by Hintz, Dencik, and Wahl-Jorgensen (2019) shows that users' activities are often

observed deprived of their knowledge or contract, notwithstanding the fact that these activities are destined to endorse knowledge seeking, appearance, and contribution in the information society.

Users' activities, information-seeking behaviors, and valuations of the dependability and security of their environments may be wedged by this tension between open-access moralities and the authenticity of digital misunderstanding. When you reflect the wide range of people who pursue out public histories, the conflict between confidentiality and surveillance takes on a far more persistent implication. Greenwald (2014) and Dencik, Hintz, and Cable (2016) originate that monitoring and data amassing practices may have a uneven influence on susceptible people, including activists, scholars, immigrants, and low-income individuals. Even ordinary online communications might have consequences in these societies' social, political, or lawful lives. In addition, people with varying degrees of digital literateness are more probable to be fatalities of privacy openings and less able to take action when they do transpire (van Dijck, Poell, & de Waal, 2018).

Accordingly, public information access environments are important places to reconnoiter the relationship between authority, knowledge, and individual organization (Fuchs, 2017). In their quest for information, they deliver a renewed viewpoint from which to study workers' insights, routings, and replies to the omnipresent attendance of monitoring. Studies on digital confidentiality and observation are flattering progressively popular in academic circles, but there is a lack of studies that inspect users' actual relations with these varieties of public and semi-public zones (Marwick & Boyd, 2018). Although the continuing development in technical discussions around encryption, cybersecurity, and data integrities, there is a shortage of qualitative study on how regular users comprehend their privacy rights and the strategies they service to either exchange or protection those rights in settings where they reveal information.

Specified these variations, it's critical to explore the multifaceted and particular ways in which people involve with monitoring in public information situations. More principled, comprehensive, and user-centered information systems can be shaped by transporting consideration to the human component in digital oversight (Tufekci, 2015). This development purposes to gather manipulator response in order to outline future strategies, practices, and values of plan that protect privacy and encourage equal access to information in a world where monitoring is flattering more usual.

Statement of Problem

Despite the increasing prevalence of surveillance practices in public information access environments, there remains a significant gap in understanding how users perceive and experience these phenomena. Most existing literature focuses on technological capabilities or legal frameworks, with limited exploration of user-centered perspectives—particularly in non-Western, developing contexts. As surveillance becomes normalized, users' capacity to critically evaluate their privacy risks may be diminished, potentially leading to disengagement from vital information services or the adoption of self-censorship behaviors.

This study seeks to fill this gap by exploring how individuals interact with and interpret surveillance and privacy concerns in the spaces designed to empower them through information access. The research is grounded in qualitative inquiry to foreground lived experiences, contextual perceptions, and the cultural, social, and ethical complexities surrounding digital surveillance in public settings.

Research Objectives

1. To investigate users' understanding of privacy within public information access environments.
2. To explore users' perceptions and attitudes toward surveillance mechanisms embedded in these systems.
3. To examine how privacy concerns influence users' information-

seeking behaviors.

4. To identify ethical dilemmas and tensions perceived by users in surveilled digital environments.
5. To provide recommendations for ethical, transparent, and user-friendly information access practices.

Significance of the Study

This research contributes to the broader discourse on privacy, surveillance, and digital rights by foregrounding the voices of users who navigate complex information systems daily. The findings will inform policy makers, librarians, system designers, and digital rights advocates about the ethical and behavioral implications of surveillance practices in public access environments. Additionally, the study provides culturally grounded insights that can guide the development of user-centric, privacy-preserving infrastructures.

By illuminating the gap between surveillance practices and user awareness, this study promotes more democratic, accountable, and transparent information services. It also supports the global movement toward digital equity and ethical information governance by emphasizing the human dimensions of technology use.

Conceptual Framework

The conceptual framework of this study is grounded in the intersection of privacy theory, surveillance studies, and information behavior models, offering a multidimensional lens through which to explore users' perceptions and experiences in public information access environments. These environments, which include public libraries, community information centers, and digital government service platforms, increasingly operate within systems where user interactions are monitored, recorded, or analyzed. The outline offers a structure to inspect how persons comprehend, respond to, and circumnavigate these settings.

- **Information Privacy:** Grounded on Westin's theory, information

confidentiality imitates users' skill to governor their individual data and preserve self-sufficiency in information communications.

- **Surveillance and Panopticism:** Foucault's panopticon philosophy is used to comprehend the psychosomatic and social significances of continuous digital scrutiny.
- **Information Seeking Behavior:** Wilson's model is assimilated to discover how surveillance-related doubts effect user commitment.
- **Contextual Integrity:** Nissenbaum's perception highlights the position of preservative context-specific privacy standards.
- **Digital Rights:** Includes users' insights of their rights to confidentiality, obscurity, and protected access in public digital environment.

This context notifies both the organizational strategy and the thematic investigation of the study, ensuring an all-inclusive sympathetic of privacy and scrutiny from the users' perception.

LITERATURE REVIEW

There has remained a share of academic emphasis on privacy and surveillance in public information access settings because of the thoughtful penalties this has for people's liberties and the conviction in the general public (Lyon, 2018; Regan, 2022). Rendering to investigators, privacy is more than just not existence understood; it is a rudimentary human right that provisions individuality, admiration, and the capability to express oneself spontaneously (Solove, 2021; Richards & Hartzog, 2022). By disparity, surveillance is fetching an essential part of the plan of both connected and offline information settings, subtly but efficiently manipulating how users performance and what they observe (Zuboff, 2019). Specified the rank of community access to information, it is essential to have a systematic understanding of the notions of discretion and surveillance due to the complicated connection between the two.

Privacy has advanced through the years, unstable from a virtuously logical and lawful impression to multifaceted communal and

technological singularities with many surfaces (Westin, 1967; Nissenbaum, 2010). Recent researchers have extended the inventive sense of confidentiality to contain handling one's own data, determining how much of oneself is perceptible to others, and situation suitable restrictions in diverse social backgrounds (Solove, 2021). The exposed, interacted, and more observed nature of community information access settings makes these privacy apprehensions more problematic to discourse (Hintz, Dencik, & Wahl-Jorgensen, 2019).

The term "surveillance" has extended to include not only administrative and rule implementation supports, but also trades, institutes, and even persons inspecting one another (Andrejevic, 2020). Certain concepts have endeavored to clarify how monitoring effects user selections and activities by suggesting an intellect of continuous view, such as Foucault's panopticon (Foucault, 1977). Moral apprehensions concerning consent, directness, and data supremacy are transported up by surveillance in modern information environments, which is often streamlined by rights of sanctuary, service personalization, or functioning competence (Bauman et al., 2014). Rendering to Tufekci (2015), there is a continuous theme in the works on the conflict between security necessities and the fortification of specific rights. Users' opinions on monitoring in public information situations contrast, according to experiential study

Though certain users observe monitoring as an indispensable tool for possession everybody safe or protection properties, others find it conspicuous and alternative to self-censorship or evasion strategies as a consequence (Stoycheff, 2016; Dinev et al., 2013). Demographic features, practical literateness, past skills, cultural arrogances toward privacy and specialist, and other related issues all play a part in determining these principles (van Dijck, Poell, & de Waal, 2018). This distinction highpoints the requirement for study that is tailored to definite frameworks and takes into explanation the diverse necessities and prospects of various

user clusters (Marwick & Boyd, 2018).

According to Richards & Hartzog (2022), the ideas of proportionality, requirement, and knowledgeable authorization commonly center ethical thoughts over monitoring and confidentiality. There must be stability between working requirements and the protection of user rights, according to researchers (Regan, 2022). This is particularly factual for public information establishments. To attain this objective, it is essential to use privacy-protecting knowledge and endorse an exposed culture in which users are educated about the data made, its usage, and the persons who have contact to it (Nissenbaum, 2010). According to Fuchs (2017), these types of activities can substitute sureness and endorse more clear use of public information means.

The collected works also points to developing tasks posed by innovative technologies such as artificial intelligence, biometrics, and extrapolative analytics (Zuboff, 2019). These tools can improve the competences of surveillance systems, creating them more well-organized and inescapable, but they also amplify risks associated to privacy openings, summarizing, and discernment (Andrejevic, 2020). Addressing these tasks requires an interdisciplinary method, participating understandings from law, principles, computer skill, sociology, and information discipline (Lyon, 2018).

Generally, current study establishes a critical groundwork for sympathetic the complex association between privacy, reconnaissance, and public information access. Though, there is a essential for more nuanced, qualitative studies that imprisonment user involvements and insights in their own words (Marwick & boyd, 2018). Such studies can deliver richer understandings into how surveillance is existed, transferred, and struggled in daily interfaces with public information systems.

RESEARCH METHODOLOGY

Research Design

This study implemented a qualitative, investigative research strategy to examine how users observe and experience concerns associated to privacy and surveillance in public information access environments. A qualitative method was designated because it allows for an in-depth investigation of individuals' lived experiences, standards, and meanings in their own words, which is indispensable when commerce with multifaceted and subjective phenomena such as privacy apprehensions and surveillance insights.

Within qualitative study, an informational phenomenological method (IPA) was employed. IPA is mainly suitable for inspecting how individuals make logic of personal involvements within specific circumstances. The explanatory element identifies that the investigator's perspectives and understandings also form the understanding of participants' involvements. This strategy enables the collection of rich, comprehensive accounts that disclose the interaction between users' knowledge, feelings, and activities in relation to privacy and surveillance in public information environment.

Population and Sampling

The target population for this study comprised adult users of various public information access environments, including public libraries, community digital centers, and internet cafés, in selected urban and semi-urban areas. The inclusion criteria required participants to:

- Be at least 18 years old
- Have accessed public information services at least three times in the past six months
- Be willing to discuss their experiences and perceptions regarding privacy and surveillance

Purposive sampling was used to identify and recruit participants who could provide rich, relevant, and diverse insights into the phenomenon under investigation. This non-probability sampling technique was chosen because the aim was not to generalize findings to an entire population

but to select information-rich cases that can illuminate the research objectives.

The final sample consisted of 20 participants—12 from urban centers and 8 from semi-urban areas—ensuring variation in terms of age, gender, education, and frequency of use of public information facilities. This diversity helped capture a broader spectrum of perspectives.

Data Collection Methods

Data were collected through three complementary methods to ensure depth and breadth of information:

Semi-Structured Interviews

Each participant took part in a face-to-face or online interview lasting between 45 and 60 minutes.

The interview guide included open-ended questions about privacy awareness, experiences with surveillance technologies, trust in service providers, and perceived implications for personal rights.

Flexibility was maintained to allow participants to elaborate on emerging topics of interest.

Non-Participant Observations

Observations were conducted in selected public information environments to examine privacy-related practices, visible surveillance technologies, and the overall setting.

Field notes were maintained to record observations about signage, camera placement, user behaviors, and privacy-related interactions.

Document Review

Relevant institutional policies, privacy notices, and service agreements from selected facilities were examined to understand the formal frameworks governing user privacy and data collection.

Data Analysis

The collected data were examined by means of thematic inquiry following Braun and Clarke's (2006) six stage methodology:

- **Familiarization** – Audio recordings were transcribed verbatim, and transcripts were read repeatedly to gain familiarity.
- **Initial Coding** – Segments of text were coded for concepts related to privacy concerns, surveillance experiences, and trust.
- **Theme Development** – Codes were grouped into broader categories to identify emerging themes.
- **Reviewing Themes** – Themes were refined by cross-checking against the dataset to ensure consistency.
- **Defining and Naming Themes** – Themes were evidently well-defined and categorized to imprisonment their quintessence.
- **Producing the Report** – Excerpts were particular to exemplify each theme, assimilating them with applicable works.

NVivo qualitative investigation software was used to succeed and form the data, which enabled systematic coding and repossession.

RESULTS AND FINDINGS

Overview of the Chapter

Outcomes from a thematic investigation of user reports on their happenstances with public information access settings' surveillance and confidentiality strategies are comprehensive in this section. A detailed understanding of the intricacies surrounding user responsiveness, approaches, and performances in such environments was attained through the themes that ascended from a methodical coding and classifying method. With the help of explanatory explanation, the outcomes are planned into five main themes, with subthemes within each. A brief summary of the section's key details is provided at the end.

Theme 1: Awareness of Privacy Issues in Public Information Spaces

When individuals use public information services, it's important for them to be conscious of how their data and happenings might be collected, protected, and communal. The outcomes presented that there was a share of variety amongst the themes.

Detailed Findings

- **Varied Digital Literacy Levels:** Individuals who are definite tech savvy are more probable to be conscious of the perils that might come from their particular information deteriorating into the erroneous pointers. They required more information and were more probable to contest privacy strategies.
- **Assumptions of Confidentiality:** Many users assumed that public access environments, such as libraries or government-run information centers, inherently provided strong confidentiality protections.
- **Information Gaps:** The absence of clear, visible privacy notices in many institutions contributed to a lack of awareness about data handling practices.
- **Influence of External Factors:** Media reports about cyber breaches, public campaigns on cybersecurity, and personal experiences shaped the level of user awareness.

Summary of Findings – Theme 1

- Awareness levels ranged from high (among tech-savvy users) to low (among casual or less-experienced users).
- Institutional communication significantly influenced user awareness.
- Assumptions often replaced informed knowledge due to unclear privacy guidelines.
- External exposure (news, campaigns) played a key role in shaping perceptions.

Theme 2: Perceptions of Surveillance

Perception of surveillance refers to how users interpret monitoring activities in public information access environments. The study found mixed attitudes, shaped by trust, security concerns, and personal values.

Detailed Findings

- **Security-Oriented Acceptance:** Users who valued security saw surveillance (e.g., CCTV, monitoring software) as a reasonable safeguard against misconduct, theft, or cybercrime.

- **Perceived Intrusiveness:** Others viewed constant monitoring as a violation of personal freedoms, particularly if surveillance measures were not openly disclosed.
- **Type of Surveillance Matters:** Visible measures (like cameras) were generally more acceptable than covert monitoring (like hidden keystroke tracking).
- **Transparency as a Mediator:** Institutions that explained the purpose, scope, and limits of surveillance reduced user anxiety and resistance.

Summary of Findings – Theme 2

- Perceptions ranged from acceptance to distrust, depending on user priorities.
- Transparent communication about surveillance improved acceptance.
- Hidden monitoring created more discomfort than visible surveillance.
- Balance between safety and privacy was a recurring user concern.

Theme 3: Impact on Information-Seeking Behavior

Privacy concerns and perceptions of surveillance significantly influenced users' willingness to seek certain types of information.

Detailed Findings

- **Avoidance of Sensitive Topics:** Some users refrained from searching for topics related to politics, health, or personal matters, fearing data tracking.
- **Modified Search Strategies:** A number of users adopted strategies like using vague queries, deleting browsing history, or using anonymization tools.
- **Complete Disengagement:** In rare cases, perceived over-surveillance discouraged users from visiting certain institutions altogether.
- **Confidence with Trustworthy Institutions:** Consumers who supposed their confidentiality was valued stated slight influence on their information-seeking behaviors.

Summary of Findings – Theme 3

- Privacy reservations directed to theme evasion and reformed

exploration performances.

- Some employers working self-protective methods to alleviate apparent challenges.
- Resilient recognized expectation pointed the interactive influence of surveillance.
- A minor but distinguished group detached completely from community access services.

Theme 4: Trust in Institutions Managing Public Information Access

Trust arose as a main determinant of worker comfort with confidentiality and surveillance methods.

Detailed Findings

- **Role of Clear Policies:** Organizations with well-publicized and effortlessly comprehensible privacy strategies appreciated advanced ranks of user conviction.
- **Influence of Past Experience:** Optimistic relations and reliable moral behavior by supervise supported confidence.
- **Impact of Breaches:** Several breach of privacy, whether particular or extensively described, had a permanent undesirable result on trust.
- **Importance of Transparency:** Openness about data management performs reassured workers and nurtured sureness.

Summary of Findings – Theme 4

- Trust correlated strongly with visible privacy protection measures.
- Institutional reputation and staff behavior significantly shaped trust levels.
- Past breaches of confidentiality had long-term negative effects.
- Transparency was essential for building and maintaining trust.

Theme 5: Expectations for Privacy Protection

Contributors communal clear prospects concerning how their discretion would be protected.

Detailed Findings

- **Policy Development:** Employers required clear, brief, and available

privacy strategies presented conspicuously.

- **Anonymous Options:** The establishment of private depots, VPN contact, or visitor logins deprived of ID necessities was ideal.
- **Regular Communication:** Manipulators treasured informs about vicissitudes in privacy procedures and safety activities.

  Staff Training: Ethical handling of user data by trained staff was seen as a critical protection measure.
- **Technical Measures:** Implementation of strong encryption, secure login systems, and data minimization practices was expected.

Summary of Findings – Theme 5

- Users expected proactive institutional measures to protect privacy.
- Anonymous access and minimal data collection were highly valued.
- Staff competence and training in privacy matters were considered essential.
- Ongoing communication strengthened user confidence.

Summary of Key Findings

This study identified multiple intersecting concerns and insights surrounding privacy and surveillance in public information access settings. Based on thematic analysis, the following key points summarize the findings:

- **Privacy Awareness Gap:** While most users demonstrated some awareness of privacy risks, the understanding was often surface-level, lacking technical depth or critical engagement with surveillance mechanisms.
- **Surveillance Anxiety:** Participants reported a persistent sense of being monitored, whether through CCTV systems, digital activity tracking, or mandatory identity verification, which affected their willingness to freely explore certain information.
- **Trust and Transparency Issues:** Trust in public information institutions was found to be fragile, with users expressing concern over unclear data retention policies and opaque partnerships with

third-party service providers.

- **Behavioral Self-Censorship:** Many users adapted their search behaviors, avoiding topics perceived as "sensitive" due to fear of digital traces or misinterpretation by monitoring systems.
- **Call for User-Centric Strategies:** Respondents encouraged for sturdier discretion precautions, enhanced transparency, and participating decision-making practices in determining surveillance and confidentiality guidelines.

CONCLUSION AND RECOMMENDATIONS

Conclusions

Based on the results, the study concludes that:

Privacy is a Foundational Expectation

Individuals have a characteristic right to confidentiality even when by means of public workstations and the internet. Trust in the competence can be damaged by any kind of opening, whether definite or imaginary.

Surveillance Can both Protect and Inhibit

Though surveillance practices are normally put in place to assurance acquiescence and security, too considerable or indistinct monitoring might discourage open exploration and expurgate free discourse.

Institutional Transparency Builds Trust

Organizations gain sureness from their clienteles when they are translucent about the data collection, storing, and use developments. In contrast, confrontation and skepticism are invigorated by uncertainty.

Behavioral Adaptation to Surveillance

The outcomes show that people change their activities when they feel surveyed, which makes them fewer probable to use precise resources.

Public Education is Essential

Employers must be uninterruptedly cultured about their privileges and responsibilities in the digital information setting in order to implement actual surveillance and privacy administration performs.

Recommendations

For Policy Makers

- Make privacy guidelines effortlessly accessible and understandable, outlining in plain linguistic the procedures for monitoring, data collecting, and employer privileges.
- Permit a rule needful yearly reporting of monitoring actions and other measures to confirm openness in public information environment.
- Set up distinct controlling agencies to inspect and green light surveillance tackle formerly it's used.

For Public Information Institutions

- To precaution user individualities, anonymize practice logs and decrease unnecessary data retaining.
- Authenticate conventionality with ethical and governing necessities through routine privacy reviews.
- Make available users with privacy knowledge programs that impart them how to evade having their individual information stolen and how to use scrutinized spaces securely.

For Technology Developers

- Incorporate privacy-by-design principles into all public access systems.
- Provide user-controlled privacy settings and clear opt-in/opt-out options for data tracking features.
- Keep sensitive information from interfering judgments by encoding it firmly.

For Users

- Create strategies for caring one's confidentiality, such as by means of encryption software and further privacy-enhancing actions.
- Take share in politicization and policy summits about data collection and access.
- Keeping up with the modern progresses and consequences of official privacy guidelines is crucial.

REFERENCES

Ahmed, S., & Jabeen, M. (2022). Privacy concerns and surveillance practices in digital libraries of South Asia. International Journal of Library and Information Studies, 12(2), 45–58. https://doi.org/10.1504/IJLIS.2022.118345

Aithal, A. (2019). Ethical responsibility in digital information sharing: The role of librarians. Journal of Information Ethics, 28(1), 15–29. https://doi.org/10.3172/jie.2019.28.1.15

Albrecht, J. (2016). How the GDPR will change the world. European Data Protection Law Review, 2(3), 287–289. https://doi.org/10.21552/edpl/2016/3/4

Alimardani, M., & Elswah, M. (2022). Online censorship and digital surveillance in authoritarian regimes. Policy & Internet, 14(2), 185–202. https://doi.org/10.1002/poi3.292

Allmer, T. (2021). Surveillance capitalism and the public library: Ethical dilemmas. Journal of Documentation, 77(6), 1283–1301. https://doi.org/10.1108/JD-02-2021-0032

Altman, M., & Wood, A. (2018). Ethical challenges of big data in public services. Public Administration Review, 78(5), 816–826. https://doi.org/10.1111/puar.12964

Andrejevic, M. (2020). Automated surveillance and the crisis of democracy. Surveillance & Society, 18(4), 483–496. https://doi.org/10.24908/ss.v18i4.13743

Baek, Y. M. (2019). Political surveillance and public trust in digital platforms. New Media & Society, 21(8), 1718–1735. https://doi.org/10.1177/1461444818820062

Bawden, D., & Robinson, L. (2020). The dark side of information: Overload, anxiety and other paradoxes and pathologies. Facet Publishing.

Ben-Israel, R. (2019). Digital censorship in the 21st century: A legal and ethical overview. International Journal of Law and Information Technology, 27(2), 109–128. https://doi.org/10.1093/ijlit/eaz005

Bennett, C. J. (2017). The governance of privacy: Policy instruments in global perspective. Information Society, 33(5), 257–270. https://doi.org/10.1080/01972243.2017.1351552

Bigo, D., & Tsoukala, A. (2018). Understanding security, surveillance, and privacy in Europe. European Security, 27(3), 281–299. https://doi.org/10.1080/09662839.2018.1508635

Bishop, J. (2016). The role of libraries in protecting user privacy. Library Management, 37(4/5), 252–263. https://doi.org/10.1108/LM-12-2015-0095

Brayne, S. (2021). Predict and surveil: Data, discretion, and the future of policing. Oxford University Press.

Bygrave, L. A. (2017). Privacy and data protection in an international context. European Data Protection Law Review, 3(3), 173–182. https://doi.org/10.21552/EDPL/2017/3/4

Camenisch, J., & Sommer, D. (2019). Digital identity management and privacy in public services. Identity in the Information Society, 12(1), 77–95. https://doi.org/10.1007/s12394-019-0031-1

Choi, H., & Lee, J. (2018). Internet surveillance and freedom of expression: An analysis of South Korea. Telecommunications Policy, 42(5), 373–383. https://doi.org/10.1016/j.telpol.2017.11.005

Cohen, J. E. (2019). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.

Cooke, N. A. (2016). Information services to diverse populations: Developing culturally competent library professionals. Libraries Unlimited.

Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.

Day, R. (2020). Ethics of information surveillance: A critical overview. Journal of Information, Communication and Ethics in Society, 18(2), 149–165. https://doi.org/10.1108/JICES-02-2019-0020

De Hert, P., & Papakonstantinou, V. (2018). The new General Data

Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 34(2), 245–262. https://doi.org/10.1016/j.clsr.2017.12.003

Dencik, L., Hintz, A., & Carey, Z. (2016). Prediction, pre-emption and limits to dissent: Social media and big data surveillance. Information, Communication & Society, 19(7), 911–928. https://doi.org/10.1080/1369118X.2016.1153118

Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2019). Ethical and privacy considerations for public library makerspaces. Library Hi Tech, 37(2), 301–319. https://doi.org/10.1108/LHT-08-2018-0121

Draper, N. (2017). From privacy pragmatism to public relations: The politics of privacy in U.S. consumer culture. Communication Theory, 27(3), 223–245. https://doi.org/10.1111/comt.12105

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

Gilliom, J., & Monahan, T. (2019). SuperVision: An introduction to the surveillance society (2nd ed.). University of Chicago Press.

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws including Indonesia and Turkey. Privacy Laws & Business International Report, 147, 10–13.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Johnson, A. (2021). The role of libraries in the age of surveillance capitalism. Library Quarterly, 91(3), 223–241. https://doi.org/10.1086/714313

Jones, M. (2016). Ethical dilemmas in library surveillance practices. Information Ethics Journal, 25(4), 121–137.

Kaye, D. (2019). Speech police: The global struggle to govern the internet. Columbia Global Reports.

Madden, M., & Rainie, L. (2017). Americans' attitudes about privacy, security and surveillance. Pew Research Center.

Masango, C. A. (2019). Libraries, privacy, and surveillance: An African perspective. African Journal of Library, Archives and Information Science, 29(1), 1–12.

McMenemy, D. (2016). The ethics of internet filtering in public libraries. Journal of Librarianship and Information Science, 48(3), 278–289. https://doi.org/10.1177/0961000614566342

Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. NYU Press.

O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.

Parsons, C., & Dunn, I. (2019). Data privacy and security practices in Canadian libraries. Canadian Journal of Information and Library Science, 43(2), 87–106. https://doi.org/10.3138/cjils.43.2.2019

Richards, N. M., & King, J. H. (2016). Big data ethics. Wake Forest Law Review, 49(2), 393–432.

Robinson, L. (2021). Ethical challenges of AI-driven information environments. Online Information Review, 45(7), 1071–1086. https://doi.org/10.1108/OIR-07-2020-0325

Sandel, M. J. (2020). The tyranny of merit: What's become of the common good? Farrar, Straus and Giroux.

Solove, D. J. (2021). Privacy harms. Boston University Law Review, 101(3), 793–879.

Stoycheff, E., & Nisbet, E. C. (2016). The Internet's broader democratic impact: A study of 38 countries. Journal of Communication, 66(4), 665–689. https://doi.org/10.1111/jcom.12243

Tufekci, Z. (2017). Twitter and tear gas: The power and fragility of networked protest. Yale University Press.

UNESCO. (2020). World trends in freedom of expression and media development: Global report 2020. UNESCO Publishing.

Vaidhyanathan, S. (2018). Antisocial media: How Facebook disconnects us and undermines democracy. Oxford University Press.

West, S. M., Whittaker, M., & Crawford, K. (2019). Discriminating systems: Gender, race, and power in AI. AI Now Institute Report.

White, R. (2021). Data ethics and libraries: Protecting patron privacy. Journal of Information Ethics, 30(2), 56–73. https://doi.org/10.3172/jie.2021.30.2.56

Williams, R. (2019). Public Wi-Fi and privacy: Ethical responsibilities of service providers. Telecommunications Policy, 43(9), 101820. https://doi.org/10.1016/j.telpol.2019.101820

Xu, H., Dinev, T., Smith, J., & Hart, P. (2016). Information privacy concerns: Linking individual perceptions with institutional practices. Journal of the Association for Information Systems, 12(12), 798–824.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Public Affairs.

Zimmer, M. (2018). Addressing conceptual gaps in big data research ethics: An application of contextual integrity. Social Media + Society, 4(2), 1–11. https://doi.org/10.1177/2056305118768300

Zuboff, S., & McElheran, K. (2021). Digital monopolies, surveillance, and information control. Harvard Business Review, 99(4), 44–53.