Privacy Tradeoffs in the Digital Era
Public Views on Data Use, Monitoring, and Accountability

Jonathan Hanon
The Graduate Center
The City University of New York
jhanon@gc.cuny.edu

Chi Zhang
The Graduate Center
The City University of New York
CHI.ZHANG06@gc.cuny.edu

Ping Ji
Hunter College & The Graduate Center
The City University of New York
ping.ji@hunter.cuny.edu

Abstract

Digital privacy is often framed as a problem of limiting collection. The harder problem is that cybersecurity and accountability often require records. Identity-theft victims need screenshots, transaction histories, police reports, vendor contacts, and account logs; public records support oversight while exposing identity trails; geofence warrants can identify suspects while sweeping in uninvolved people; audit logs can reveal misuse while becoming sensitive repositories. This first-phase dissertation work organizes those cases around an **evidence threshold**: the point at which data moves from private trace to accountable proof. It turns a broader user, legal, and technical review into an IRB-approved, scenario-based survey of public cybersecurity awareness and tolerance. The survey asks what ordinary users know about data collection, when they accept privacy-invasive monitoring for end-user protection or mal-behaviour accountability, and what safeguards they require. The long-term goal is to connect public judgment to privacy-aware monitoring, audit design, retention rules, notice, consent, and cybersecurity education.

1 The Core Problem

Privacy and security are often discussed as if they naturally move in the same direction. The original research draft begins from a more difficult observation: some privacy protections, such as anonymity or strict data minimization, can make accountability for cybercrime harder, while security measures such as monitoring, logging, identity checks, or location tracking can compromise privacy. The project therefore asks how to protect end users while still making visible where their data is routed, stored, retained, and used.

This is a human-centered security problem, not only a legal or technical policy problem. Defensive cyber deception and honeypot-style systems already raise questions about transparency, fairness, no-harm, and notice [23]. Developers need to know what monitoring users can understand and tolerate. Educators need to know what users misunderstand about cybercrime, evidence, and protection practices. The study therefore asks three linked questions: what ordinary users know about cybersecurity; what level of privacy invasion they tolerate for accountability; and how survey results can guide monitoring protocols and public cybersecurity education.

2 Users as Evidence Holders

The first layer is the user perspective. Users are often treated as the weak point in security because they reuse passwords, fail to encrypt documents, or abandon protective practices over time [24]. Yet when harm occurs, the same users may become evidence holders. Identity-theft victims may need screenshots, transaction records, notices, police reports, vendor contacts, and account logs to reconstruct where a stolen identity was used [20]. Even with this evidence, vendors and law enforcement may not act without a formal investigation [9].

This burden explains why a survey cannot ask only whether users value privacy. That misses the moment when data becomes useful to the user. A survey also cannot ask only whether users support monitoring, because that misses the fear that monitoring can become surveillance. Prior work on mobile Internet monitoring and user tolerance is a useful starting point [5], but this project extends the question beyond network traffic to identity misuse, public records, location data, legal access, online harassment, and audit logs. The survey must therefore use concrete scenarios rather than abstract privacy attitudes.

3 Law as Access Boundary

The second layer is legal and policy context. Legal availability does not always match ordinary expectations. Information many people consider private, such as voter-registration data, can be available through state freedom-of-information processes [15]. Voter registration security, absentee-ballot risk, registration groups, and election-worker roles also show that ordinary citizens participate in systems where identity, records, and accountability matter [4, 6]. These cases show a recurring pattern: public access can support transparency while also exposing identity trails.

Privacy regulation adds a second pattern. GDPR frames

consent, erasure, portability, and the costs of privacy rights [11, 22]. Yet formal consent or legal availability does not always mean meaningful user understanding. A user may not expect a record to be public, may not know when a platform shares data with law enforcement, or may not understand whether data can be modified or erased.

Law-enforcement examples sharpen the threshold. Geofence warrants raise questions about the third-party doctrine, location privacy, probable cause, and overbroad search regions [1, 10, 17]. Location data can solve crimes or support public accountability, but it can also sweep in uninvolved people or become public through secondary use, as illustrated by data-broker reporting on device locations tied to the Epstein investigation [14]. Stalking, revenge porn, and AI deepfake abuse show the opposite problem: digital evidence may exist while legal categories lag behind lived harm [2, 3, 12, 18]. Broader work on ethical cybersecurity law and AI national-security law reinforces the need for human oversight, accountability, and clearer legal boundaries [13, 19]. For this project, these are not legal quizzes. They are source material for plain-language scenarios about consent, access, retention, harm, and accountability.

4 Logs as Technical Evidence

The third layer is technical. The user and legal cases lead directly to monitoring and auditing. Digital identity federation [21], IoT auditing [16], and privacy accountability work on incomplete audit logs [7, 8] point to the same implementation problem: systems may need records to prove what happened, but those records also create privacy risk. Incomplete logs can hide policy violations; complete logs can become sensitive repositories. Both problems matter for humanist security policy.

The technical contribution of this phase is to identify variables that can later become design requirements: logging level, data minimization, retention period, access control, user visibility, auditability, and explanation. The same mechanism can be interpreted differently depending on these variables. A limited, purpose-bound log for account recovery may be acceptable; an indefinite, hidden log with unclear access may be perceived as surveillance. These are engineering choices, but they require evidence about public expectations.

5 Survey Design and Ethics

These three layers motivate the current artifact: an IRB-approved survey instrument. It will measure public understanding of cybercrime, vulnerability factors, and tolerance for monitoring or data collection when the stated goal is end-user protection or accountability. Following prior work on survey recruitment [24], recruitment is planned through Prolific. Measured background factors include technical experience, legal familiarity, public influence, and demographic information such as age, gender, education, income, ethnicity, language, and disability.

The survey is scenario driven. Prompts can include identity-theft evidence, suspicious account activity, school or employer network monitoring, geofence investigation, public-record reuse, platform sharing with police, deepfake abuse, and IoT-device auditing. Each prompt can name the actor requesting or holding data, state the purpose of collection, and vary safeguards. Participants can then answer awareness questions, tolerance questions, and design-preference questions.

The instrument separates three ideas that are often blurred: what users know, what users accept, and what users want systems to do. Awareness items ask whether participants understand what data exists and how it might become evidence. Tolerance items ask whether collection feels acceptable under a stated purpose. Design-preference items ask which safeguards matter: shorter retention, clearer notice, explicit consent, access limits, user review, or independent oversight. The first survey should treat responses as exploratory unless sampling supports stronger claims; its immediate goal is to refine constructs and scenario language. Consultation with social-science experts will support instrument design, recruitment, and analysis.

Ethically, CUNY Graduate Center IRB approval has been obtained. Participants will provide informed consent, directly identifying information will be minimized, and early results will be interpreted as exploratory rather than prevalence evidence unless recruitment and sampling support stronger claims.

6 Future Technical Plan

The long-term technical goal is to translate awareness and tolerance findings into design requirements for monitoring and auditing systems. A later phase can map scenarios to concrete choices: what to log, what to minimize, what to keep as evidence, what requires consent, what users should see, and what should be reserved for accountable investigation.

The technical plan has three outputs. First, a design matrix can link survey scenarios to logging, retention, access, and consent rules. Second, a lightweight prototype or policy engine can demonstrate privacy-aware audit modes, such as minimal logs, user-visible logs, investigation-only evidence packages, and expiring records. Third, developer and public-education guidelines can explain monitoring choices in plain language.

The contribution is a case-grounded survey framework for a problem the long draft identifies across several domains. Public privacy tolerance depends on evidence thresholds, not only on general attitudes. The expected results should support both technical design and education: users should understand when data is collected, why, where it is stored, who can access it, and when it may become evidence.

References

[1] *Matter of Search of Information Stored at Premises Controlled by Google (481 F. Supp. 3d 730 (N.D. Ill. 2020))*. 08 2020.

[2] Afaq Ashraf, Taha, Nida ul Habib Bajwa, Cornelius J. König, Mobin Javed, and Maryam Mustafa. "stalking is immoral but not illegal": Understanding security, cyber crimes and threats in pakistan. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 37–56, Anaheim, CA, August 2023. USENIX Association.

[3] Claire Benn. Deepfakes, pornography and consent. *Philosophers' Imprint*, forthcoming.

[4] Jack Cable, Andrés Fábrega, Sunoo Park, and Michael A Specter. A systematization of voter registration security. *Journal of Cybersecurity*, 9(1):tyad008, 06 2023.

[5] Cormac Callanan, Borka Jerman-Blažič, and Andrej Jerman Blažič. User awareness and tolerance of privacy abuse on mobile internet: An exploratory study. *Telematics and Informatics*, 33(1):109–128, 2016.

[6] Alistair Clark and Toby S James. Electoral administration and the problem of poll worker recruitment: Who volunteers, and why? *Public Policy and Administration*, 38(2):188–208, 2021.

[7] Anupam Datta. Privacy through accountability: A computer science perspective. In Raja Natarajan, editor, *Distributed Computing and Internet Technology*, pages 43–49, Cham, 2014. Springer International Publishing.

[8] Deepak Garg, Limin Jia, and Anupam Datta. Policy auditing over incomplete logs: theory, implementation and applications. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, page 151–162, New York, NY, USA, 2011. Association for Computing Machinery.

[9] Stephen V. Gies, Nicole Leeper Piquero, Alex R. Piquero, Brandn Green, and Amanda Bobnis. Wild, wild theft: Identity crimes in the digital frontier. *Criminal Justice Policy Review*, 32(6):592–617, 2021.

[10] Shamona Joseph. The unconstitutionality of geofence warrants. *University of Central Florida Department of Legal Studies Law Journal*, 6:71–112, 2023.

[11] T. Tony Ke and K. Sudhir. Privacy rights and data security: Gdpr and personal data markets. *INFORMS Management Science*, 69(8), 12 2022.

[12] Paul J Larkin Jr. Revenge porn, state law, and free speech. *Loy. LAL Rev.*, 48:57, 2014.

[13] Manish Kumar Sharma Mamraj Sain. Ethical Implications of Cybersecurity Legislation. *International Journal of Computer Networks and Wireless Communications (IJCNWC)*, 2019.

[14] Dhruv Mehrotra and Dell Cameron. Jeffrey epstein's island visitors exposed by data broker, 03 2024.

[15] New York State Board of Elections. Freedom of information subject matter list – revised january 1, 2023.

[16] Syed Rizvi, Tatiana Zwerling, Benjamin Thompson, Shawn Faiola, Shakir Campbell, Stephen Fisanick, and Codi Hutnick. A modular framework for auditing iot devices and networks. *Computers & Security*, 132:103327, 2023.

[17] Josh A. Roth. Drawing lines: geofence warrants and the third-party doctrine. *International Cybersecurity Law Review*, 4(2):213–233, 6 2023.

[18] Michael Salter and Thomas Crofts. Responding to revenge porn: Challenges to online legal impunity. *New views on pornography: Sexuality, politics, and the law*, pages 233–256, 2015.

[19] Yogita Upadhayay and Dr. Rituja Sharma. Cybersecurity and legal considerations in ai applications for national security. *Educational Administration: Theory and Practice*, 29(3):474–480, 09 2023.

[20] Megan Wyre, David Lacey, and Kathy Allan. The identity theft response system. *Trends and Issues in Crime and Criminal Justice [Electronic Resource]*, (592):[1]–[18], 2020.

[21] Prashant Madhukar Yawalkar, Deepak Narayan Paithankar, Abhijeet Rajendra Pabale, Rushikesh Vilas Kolhe, and P. William. Integrated identity and auditing management using blockchain mechanism. *Measurement: Sensors*, 27:100732, 2023.

[22] Razieh Nokhbeh Zaeem and K. Suzanne Barber. The effect of the gdpr on privacy policies: Recent progress and future promise. *ACM Trans. Manage. Inf. Syst.*, 12(1), 12 2020.

[23] Quanyan Zhu. The doctrine of cyber effect: An ethics framework for defensive cyber deception, 2023.

[24] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–15, New York, NY, USA, 2020. Association for Computing Machinery.