Privacy in the Information Age

Surveillance, Data, and the Boundaries of the Self

Computing and AI Ethics

Rochester Community and Technical College

Central Questions

- What is privacy, and why does it matter?
- Do we have a "right" to privacy? If so, where does it come from?
- How has information technology transformed privacy?
- When (if ever) is surveillance justified?
- Is privacy a universal value, or culturally contingent?

Discussion

What's the last thing you did to protect your privacy online?

What Is Privacy? Defining the Concept

Defining Privacy

Privacy is surprisingly difficult to define precisely:

- "The right to be let alone" (Warren & Brandeis, 1890)
- Control over information about oneself
- **Contextual integrity** (Helen Nissenbaum): Information flows appropriate to context

Key distinctions: Privacy $\neq$ Secrecy $\neq$ Anonymity (related but distinct)
Key insight: Privacy is not about having something to hide—it's about maintaining boundaries between self and world.

Types of Privacy (Taxonomy)

Type	Description	Example Violation
Informational	Control over personal data	Data breach exposing records
Physical/Spatial	Freedom from bodily intrusion	Warrantless search
Decisional	Autonomy over personal choices	Reproductive restrictions
Communications	Private correspondence	Wiretapping
Associational	Freedom to associate privately	Membership list disclosure
Intellectual	Private thoughts and beliefs	Compelled speech

Different privacy types may require different protections.

Discussion

Which type of privacy do you value most?

Why Privacy Matters—Instrumental Arguments

Privacy Serves Important Functions

1. Privacy provides space for **autonomy**—room to develop our identities without external pressure.
2. Selective sharing creates **intimacy**; we build relationships by choosing what to reveal.
3. **Democracy** depends on privacy: anonymous ballots, confidential sources, and dissent.
4. Privacy offers **security** against identity theft, stalking, and discrimination.
5. It maintains **power balance**—asymmetric surveillance enables abuse.

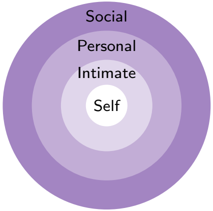
> "Arguing that you don't care about privacy because you have nothing to hide is like arguing you don't care about free speech because you have nothing to say." —Edward Snowden

Why Privacy Matters—Intrinsic Arguments

Privacy may have value *beyond* its consequences:

- Being observed without consent is degrading—privacy protects **dignity**.
- The "self" requires private boundaries; privacy is constitutive of **personhood**.
- Privacy acknowledges persons as ends, not means, expressing **respect**.

James Rachels: Privacy enables us to maintain different relationships with different people.



Privacy Zones

Legal Foundations of Privacy—United States

US Privacy Law: A Patchwork Approach

- **4th Amendment**: Protection against unreasonable searches
- **Griswold v. Connecticut** (1965): Privacy implied by "penumbras"
- **Katz v. United States** (1967): "Reasonable expectation of privacy"
- **Third-party doctrine**: Info shared with third parties loses protection

Sectoral approach: HIPAA (health), GLBA (finance), COPPA (children), FERPA (education)
Key gap: **No comprehensive federal privacy law** (unlike EU)

Legal Foundations—International Comparison

Jurisdiction	Approach	Key Law	Max Penalty
EU	Comprehensive right	GDPR (2018)	4% global revenue
USA	Sectoral, patchwork	Various (HIPAA, etc.)	Varies by sector
China	State control priority	PIPL (2021)	5% revenue
California	Consumer rights	CCPA/CPRA	$7,500 per violation

GDPR features: Right to erasure, consent requirements, data portability
Largest GDPR fine: €1.2 billion to Meta (2023) for illegal data transfers

Discussion

Should the US adopt GDPR-style comprehensive protections?

Philosophical Theories of Privacy Rights

Where Does the Right to Privacy Come From?

1. **Natural rights**: Privacy inherent to human dignity (Kantian)
2. **Utilitarian**: Privacy maximizes overall welfare
3. **Social contract**: Privacy necessary for civil society
4. **Property rights**: Personal data as property (Lockean)
5. **Relational**: Privacy constitutes relationships (Rachels, Nissenbaum)
6. **Feminist critique**: "Personal is political"—privacy can hide abuse

Key tension: Privacy as *protection* vs. privacy as *concealment*

The “Nothing to Hide” Argument

Common claim: “If you have nothing to hide, you have nothing to fear”

Responses to “Nothing to Hide”

1. Everyone has something to hide (legal but private matters)
2. Innocence doesn’t guarantee safety (false positives, changed laws)
3. **Chilling effects** on speech and behavior
4. Power asymmetry: “You show me yours first”
5. **Aggregation problem**: Innocuous data combines into sensitive profiles
6. Future unknown: Today’s normal may be tomorrow’s suspicious

Daniel Solove: The problem isn’t isolated data, but the “aggregation problem.”

The Privacy Paradox

The Paradox

People say they value privacy but act as if they don't.

Evidence: Studies show high stated concern, yet people readily share data for small conveniences.

Possible explanations:

- Privacy decisions are too complex to evaluate rationally (**bounded rationality**)
- We favor immediate gratification over abstract future harm (**temporal discounting**)
- Many feel resigned: "Privacy is dead anyway"
- Often there's no real alternative—take it or leave it

Discussion

Do your privacy behaviors match your stated privacy preferences?

Case Study: The "Right to Be Forgotten"

Google Spain v. AEPD (2014)

Mario Costeja González: Wanted old newspaper links about debt removed from Google search results.
EU Court ruling: Individuals can request removal of "inadequate, irrelevant, or excessive" information.

Now in GDPR Article 17: The "right to erasure"
Scale: Google has received **2+ million removal requests** since 2014
Tensions: This ruling pits privacy against free speech and press freedom, and raises questions about memory versus forgetting in the digital age. The EU and US take fundamentally different approaches.

Discussion

Should people be able to erase their digital past?

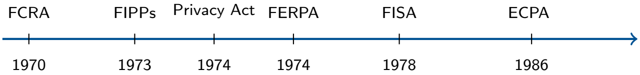
Pre-Digital Privacy Concerns

Privacy concerns predate computers:

- **1890**: Warren & Brandeis "The Right to Privacy"—response to photography and tabloid journalism
- **1928**: *Olmstead v. United States*—wiretapping (Brandeis dissent)
- **1949**: Orwell's *1984*—totalitarian surveillance state
- **1960s**: Government databases spark concern (Social Security numbers)
- **1970**: Fair Credit Reporting Act—first major US data privacy law
- **1974**: Privacy Act—governs federal agency records

Key insight: Each new technology triggers new privacy concerns.

The Computer Revolution (1970s–1980s)



1973 HEW Report: Established **Fair Information Practice Principles** (FIPPs):

- Notice, Choice, Access, Security, Enforcement

1978 FISA: Created secret court for surveillance warrants

1986 ECPA problem: Stored communications >180 days get less protection (outdated assumption)

The Internet Age (1990s–2000s)

- **1991**: World Wide Web transforms information sharing
- **1995**: EU Data Protection Directive—comprehensive approach
- **1998**: COPPA—children's online privacy
- **1999**: Gramm-Leach-Bliley Act—financial privacy
- **2001**: USA PATRIOT Act—expands surveillance post-9/11
  - Section 215: Bulk collection of phone metadata
  - National Security Letters without judicial oversight

New technologies emerge: Cookies, web tracking, behavioral advertising

The Social Media Era (2004–2012)

- **2004**: Facebook launches
- **2006**: Twitter; Facebook goes public
- **2007**: iPhone—smartphones ubiquitous
- **2010**: Facebook privacy policy controversies
- **2011**: Location tracking scandals

Business model: "If it's free, you're the product"

Platform	**Data Types**
Facebook	Posts, location, contacts
Google	Searches, emails, YouTube
Amazon	Purchases, Alexa, browsing

Table: *

Data collected (indefinite retention)

Case Study: The Snowden Revelations (2013)

Edward Snowden: NSA Contractor Turned Whistleblower

Key revelations:

- **PRISM**: Direct access to tech company servers
- **Upstream collection**: Tapping fiber optic cables
- **Bulk phone metadata**: Section 215 collection
- **XKeyscore**: "Nearly everything a user does on the Internet"

Impact: Global debate, USA FREEDOM Act (2015), encryption push
Current status: Snowden received Russian citizenship (2022), remains in Russia
Ongoing debate: Hero or traitor?

Case Study: Cambridge Analytica (2018)

The Data Harvesting Scandal

What happened: Political consulting firm harvested **87 million** Facebook profiles via personality quiz app "This Is Your Digital Life"—collected data from users AND their friends.
Use: Psychographic profiling for targeted political ads (Brexit, 2016 US election)

Consequences:

- Mark Zuckerberg testified before Congress.
- The FTC levied a $5 billion fine—the largest ever for privacy at the time.
- The scandal accelerated GDPR implementation (May 2018).
- Public awareness of data practices increased dramatically.

Lesson: "Move fast and break things" meets democracy

The Current Landscape (2020s)

New technologies:

- AI and machine learning power facial recognition and predictive systems.
- The Internet of Things puts sensors in our homes, on our bodies, and in our cars.
- Biometric identification now extends to faces, voices, and DNA.
- Generative AI systems train on vast troves of personal data.

COVID-19 impact: Contact tracing, health passports, remote work surveillance

Data Broker Stats	
Market size (2024)	$280B+
Brokers globally	∼5,000
Avg databases/American	1,500+
Data points/profile	1,500+

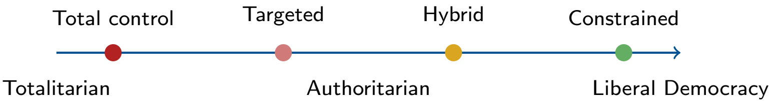
The Attention Economy and Surveillance Capitalism

Shoshana Zuboff's Framework (2019)

1. **Human experience** as raw material for data extraction
2. **Behavioral surplus**: Data beyond service improvement → prediction products
3. **Prediction products** sold to business customers (advertisers)
4. **Behavioral modification**: Nudging users toward desired outcomes
5. **Instrumentarian power**: Shaping behavior at scale

> "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data."

Surveillance and Regime Type



Total control

Targeted

Hybrid

Constrained

Totalitarian

Authoritarian

Liberal Democracy

Key insight: Technology has made comprehensive surveillance far cheaper and more effective than ever before.

Central Question

Can liberal democracies use these technologies without becoming authoritarian?

China—The Surveillance State Model

The Most Comprehensive Surveillance System in History

- **1.4 billion people**, world's largest population
- **Social Credit System**: Scoring citizens on "trustworthiness"
- **600–700 million CCTV cameras** nationwide
- **Great Firewall**: Blocks Google, Facebook, Twitter, foreign news
- **Real-name registration**: Required for internet, phone, transit

Social Credit consequences:

- High scores bring rewards like fast-track services and better loan rates.
- Low scores trigger punishments: travel bans, public shaming, and job restrictions.

China—Facial Recognition and AI

System	Function	Scale
Skynet/Sharp Eyes	Urban camera network	600M+ cameras
Golden Shield	Database integration	1.4B citizens
Great Firewall	Internet censorship	All traffic
Social Credit	Behavior scoring	National

AI capabilities:

- These systems can identify faces in crowds and track individuals across cities.
- Some claim to detect suspicious behavior through “emotion recognition” and gait recognition—though the science is dubious.
- Integration of cameras with phones, apps, and payments creates comprehensive tracking.

Tech exporters: Huawei, Hikvision, SenseTime, Megvii

Case Study: Xinjiang and the Uyghurs

Surveillance-Enabled Persecution

Xinjiang Uyghur Autonomous Region: ∼12 million Uyghur Muslims
Mass detention: 1+ million detained in "re-education camps" (2017–present); ∼500,000 currently in prisons/detention (2025 estimate)

Surveillance intensity:

- In some areas, checkpoints appear every 100 meters.
- Residents must install mandatory smartphone apps and submit to DNA collection.
- The IJOP predictive system flags "suspicious" behaviors—including praying, traveling abroad, or having certain contacts.

International response: US sanctions on Hikvision, genocide determinations by US, UK, Canada, EU Parliament
Lesson: Technology enables persecution at unprecedented scale

Russia—Selective Surveillance and SORM

SORM: System of Operative-Investigative Measures

- Requires ISPs to install FSB monitoring equipment
- Real-time access **without judicial warrant**
- SORM-1 (phones), SORM-2 (internet), SORM-3 (all communications)

Russia's system is less comprehensive than China's but highly targeted:

- Primary targets include political opposition, journalists, activists, and LGBTQ+ individuals.
- Moscow alone has over 200,000 facial recognition cameras.
- Since the 2022 Ukraine invasion, the crackdown has intensified—spreading "false information" now carries a 15-year sentence.

Cases: Alexei Navalny tracked extensively; Memorial liquidated (2021)

Other Authoritarian Surveillance States

Country	Key Systems	Primary Targets
Iran	Internet shutdowns, SIAM	Protesters, women, minorities
Turkey	ByLock prosecutions	Gülenists, Kurds, journalists
Hungary	Pegasus spyware	Journalists, opposition
Saudi Arabia	Pegasus, social media	Dissidents, women activists
UAE	Pegasus, ToTok app	Dissidents, foreign residents
Belarus	Russian tech, facial rec.	Protesters, opposition

Common thread: Commercial spyware enables surveillance without building own capabilities

Case Study: The Pegasus Spyware Scandal

NSO Group's "Lawful Intercept" Tool

Pegasus: Spyware sold to governments for "terrorism and crime"
Capabilities: Full smartphone access—messages, calls, camera, mic, location
Zero-click exploits: No user action required for infection

2021 Pegasus Project revelations:

- **50,000+ phone numbers** on leaked target list
- 180+ journalists in 20+ countries targeted
- Jamal Khashoggi's fiancée's phone infected *after* his murder
- 14+ heads of state targeted (including Macron)

Customers: Mexico, Saudi Arabia, UAE, Hungary, India, Morocco, others
US response: NSO Group blacklisted (2021)

Exporting Authoritarianism—China's Tech Diplomacy

Belt and Road Includes Surveillance

- **Safe City projects**: Huawei systems in 100+ countries
- **Training**: China trains foreign officials in "internet management"
- **Recipients**: Zimbabwe, Venezuela, Ecuador, Pakistan, Philippines, many African nations

Concerns:

- Technology transfer enables local authoritarianism.
- Data may flow back to Beijing.
- Recipient countries become dependent on Chinese tech ecosystems.
- The practice normalizes mass surveillance globally.

Digital Authoritarianism—Lessons

Key Patterns

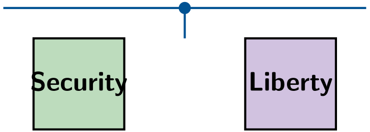
1. **Comprehensiveness**: Multiple overlapping systems
2. **Integration**: Linking databases for complete profiles
3. **Automation**: AI enables scale impossible with human monitors
4. **Normalization**: Gradual expansion of acceptable surveillance
5. **Chilling effects**: Self-censorship without direct enforcement

The authoritarian toolkit: Internet shutdowns, content filtering, real-name registration, facial recognition, location tracking, spyware, social credit

Discussion

At what point does surveillance cross from "security" to "control"?

The Core Tension



The "balance" framing is itself contested

Traditional framing: Security vs. Liberty tradeoff
Alternative framing: False dichotomy—privacy *enables* security (from abuse of power)
Question: How do we evaluate surveillance in democracies?

Arguments FOR Surveillance (Security Perspective)

Pro-Surveillance Arguments

1. **Crime prevention**: Deterrence through visibility
2. **Crime solving**: Evidence for prosecution
3. **Terrorism prevention**: Identifying threats before attacks
4. **Public safety**: Finding missing persons, emergency response
5. **Efficiency**: Faster, more accurate than human observation
6. **Consent**: Public spaces have no expectation of privacy

Common refrain: "If you've got nothing to hide, you've got nothing to fear"

Arguments AGAINST Surveillance (Liberty Perspective)

Anti-Surveillance Arguments

1. **Chilling effects**: People self-censor when watched
2. **Power asymmetry**: Government sees citizens, not reverse
3. **Mission creep**: Systems expand beyond original purpose
4. **Function creep**: Data used for unintended purposes
5. **Error rates**: False positives harm innocent people
6. **Bias**: Algorithms encode and amplify discrimination
7. **Abuse potential**: Tools *will* be misused (history shows this)

Neil Richards: "A society in which everyone is watched by everyone else is less a utopia than a nightmare."

Facial Recognition—The Debate

Pro Arguments

- Identifies suspects, missing persons
- Faster than manual review
- Real-time response capability

Con Arguments

- Higher error rates for darker skin, women
- Face is public—permanent ID
- Chilling effect on protest
- No consent mechanism

ACLU study: 28 members of Congress falsely matched to mugshots
Status: Bans in San Francisco (2019, first US city), Boston, Oakland, 16+ municipalities

Case Study: Clearview AI

The Controversial Facial Recognition Company

Database: Scraped **30+ billion photos** from social media (CEO claims 50B)
Product: App for police to identify anyone from a photo
Customers: 2,400+ law enforcement agencies (often without official approval)

Legal battles:

- Sued by ACLU; settled with ban on sales to private businesses
- Fined €30.5M (Netherlands), €20M (Italy), £7.5M (UK)
- Banned in Australia, Canada

CEO claim: “First Amendment right” to collect public photos

Discussion

Should police be able to identify anyone, anywhere, anytime?

Predictive Policing

Using Data to Predict Crime

Place-based: Predict crime hotspots (PredPol, HunchLab)
Person-based: Predict who will commit/be victim of crime (Chicago “heat list”)

Criticisms:

- **Feedback loops**: Police go where predicted → more arrests → more predictions
- **Historical bias**: Trained on biased enforcement data
- **Pre-crime problem**: Punishing predicted future acts
- **Opacity**: Proprietary algorithms can’t be challenged
- **Efficacy**: Limited evidence it actually reduces crime

Case: Los Angeles ended PredPol (2020) after bias concerns

Workplace and Consumer Surveillance

Workplace monitoring:

- Keystroke logging, screenshots
- Productivity scoring
- Location tracking
- Amazon "time off task"
- Remote work: Webcam, mouse tracking

Stats: 80% of major companies monitor employees

Consumer surveillance:

- Smart home devices (Alexa recordings reviewed by humans)
- Connected cars (location, driving)
- Insurance apps (health tracking)
- Retail facial recognition

Key point: Government isn't the only surveillor—private companies too

The “Nothing to Fear” Response—Revisited

Sophisticated Responses to Surveillance

1. **Definitional problem**: Who decides what’s “wrong”? Laws change.
2. **Contextual integrity**: Info appropriate in one context isn’t in another
3. **Aggregation**: Combining innocuous data reveals sensitive information
4. **Chilling effects**: Even innocent people change behavior
5. **Power**: “Show me yours first” (government transparency)
6. **Equality**: Surveillance falls disproportionately on marginalized groups

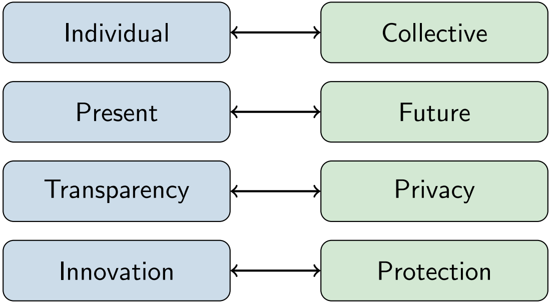
Bruce Schneier: “Too many wrongly characterize the debate as ‘security versus privacy.’ The real choice is liberty versus control.”

Possible Frameworks for Democratic Surveillance

Constraints for Democratic Surveillance

1. **Judicial oversight**: Warrants required, meaningful review
2. **Transparency**: Public knows what systems exist
3. **Purpose limitation**: Only for specified uses
4. **Minimization**: Collect only what's necessary
5. **Retention limits**: Delete after time period
6. **Audit trails**: Record who accesses what
7. **Accountability**: Consequences for misuse
8. **Sunset clauses**: Programs expire without reauthorization

Privacy in the Balance—Key Tensions



Individual ↔ Collective

Present ↔ Future

Transparency ↔ Privacy

Innovation ↔ Protection

These tensions cannot be fully “resolved”—they must be navigated case by case.

Conclusion: Framework for Evaluation

Questions to Ask About Any Surveillance System

1. **Who benefits** from this surveillance?
2. **Who bears** the risks and costs?
3. What **oversight and accountability** exists?
4. Is this the **least invasive means** to the goal?
5. What happens **when (not if)** it's abused?

Final Discussion

Where do you draw the line? What surveillance, if any, is acceptable in a free society?

Remember: Privacy is not about having something to hide—it's about maintaining the boundaries that make us human.