CONSENSUS ON POLICY IMPLICATIONS

1

Privacy And Cybersecurity Today

2019 study & 2020 report

Part I: Changing views of privacy through time

Part II: Technological advances that will greatly benefit society also pose privacy risks

Part III: Election security, privacy in political activity and census privacy

Part IV: Key privacy and cybersecurity actors; their roles and activities

Key Findings: Policy Issues

Appendices: Additional resources and readings

2

Discuss Policy Implications Of This Study

- to come to consensus
- to develop a position statement

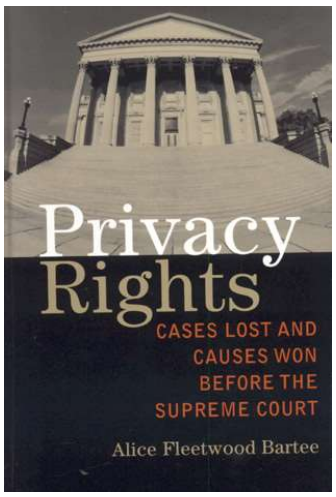
Source: European Digital Rights

3

Changing views of privacy and personal information security

- Privacy has meant different things at different times; it means different things in different contexts
- Can mean solitude, physical space, decision-making, or one's control over access, information or decisions
- Constitution does not define, nor do court rulings clearly define privacy as a right.
- Given the lack of a specific US individual privacy right, privacy in the cybersecurity context refers to *personal information privacy* and *personal data security*

➢ Thus, current US policy focuses on personal information security: data protection, not data privacy.



4

Technological advances that will greatly benefit society also pose privacy risks

Source: Mike Keefe, Denver Post, 2010

- Users eagerly supply many forms of personal information to platforms and applications which collect ALL of it
- Personal information and online behavior (e.g., likes, locations, transactions) are collected and used for profit
- Government and private enterprise easily access and analyze all forms of personal information—for new commercial uses and often with the capability to continuously monitor behavior
- Commercial internet activity is largely unregulated (due to weak regulations governing privacy definitions, data 'ownership,' sectoral regulation/self-regulation, third-party data transfers)

5

Known privacy threats are compounded by piecemeal regulation; reactive regulation is a whack-a-mole game

- New technologies & new platforms do not match conventional understandings of privacy, ownership and security
- New technologies increase vulnerability to data breaches and malware hacks
- Search engines are high-powered activity-tracking and -monitoring systems
- Social media are free to gather, analyze, and share sell/rent data—all provided by users
- Cloud computing obscures data ownership & is vulnerable to data breaches
- Mobile devices are linked to the internet and stream geo-located data
- Internet of things (IoT) connects all linked devices, providing a comprehensive view of one's behavior and activities

Source: Global Partners www.gp-digital.org › uploads › 2015/06 › GCCS-privacy-PP-final-3-1

6

Big Data – Underlies the Data Revolution

• Giant data sets analyze ALL forms of user information to construct patterns of human behavior and interaction—all without user knowledge or permission

• 'Unstructured' data include internet clicks, social media content, web server logs, mobile device records, customer emails and surveys, mobile phone records and IoT sensor data.

• Powerful analytics identify and profile individual users — despite initial data anonymization.

The Big Data technology stack is evolving rapidly

7

Fake News and Deep Fakes: Easy, Convincing Media Manipulation

AI for dummies – Rapid democratization of AI (artificial intelligence) means anyone can use sophisticated machine learning, neural networks, & AI systems

- Voice cloning and deceptive, synthetic videos may be used creatively & lawfully, or maliciously & illegally
- Image manipulation, faking or falsifying people's words or events
- Common uses: deep fake porn, deep fakes in political campaigns, deep fakes for commercial uses, creative deep fakes

➢ Pros/socially beneficial purposes: creative commercial uses to entertain, call attention to issues; creative expression (humor & parody)

➢ Cons/socially harmful purposes: tarnish people's reputations (e.g., revenge porn & political campaigns)
- violate privacy
- falsify events
- undermine political decisions, international relations, or national security

8

E-Commerce: consumer data is profitable

- Current US data policy prioritizes economic growth & internet expansion
- Users' detailed record of personal behavior is readily 'monetized' (i.e., converted to business revenues)
- Sharing data with third parties and transferring data across borders weakens data protections
- Advertising is the E-Commerce engine; it requires data on user behaviors and activities
- E-Commerce firms self-regulate; their consent policies may provide little meaningful privacy protection

9

KEY FINDINGS: Policy Issues

I. US Privacy Policy Is Not Uniform

- Patchwork of Federal and state laws and regulations does not provide comprehensive privacy protection

- Regulating specific violations and past abuses fails to provide the means to address emerging concerns

10

II. Individuals and Personal Data Protection: 'Different Strokes for Different Folks'

- Current laws emphasize personal data protections, based on which service provider holds and controls the data
- Regulating an individual's *personally identifiable information* (PII) is rapidly becoming obsolete
- When data privacy is violated, users have limited legal remedies to hold firms accountable for improper data use

HIPAA	REGULATES HEALTH CARE PROVIDERS' COLLECTION AND DISCLOSURE OF SENSITIVE HEALTH INFORMATION
COPPA	REGULATES ONLINE COLLECTION AND USE OF INFORMATION OF CHILDREN
GLBA	REGULATES FINANCIAL INSTITUTIONS' USE OF NONPUBLIC PERSONAL INFORMATION
FCRA	REGULATES THE COLLECTION AND USE OF DATA CONTAINED IN CONSUMER CREDIT REPORTS
FTC ACT	PROHIBITS "UNFAIR OR DECEPTIVE ACTS OR PRACTICES"

11

III. E-Commerce Data Protections

- E-Commerce is based on sector-specific, voluntary regulation; much personal information may be unprotected
- User choice and company notice-and-consent protocols often fail to provide meaningful personal data protection
- Data protection is often lost when personal data is transferred or shared with another firm or service
- The Federal Trade Commission (FTC) oversees consumer information privacy, lacks meaningful enforcement authority

12