Commission on Evidence-Based Policymaking: Privacy Perspectives

Marc Rotenberg
National Academies of Science
Washington, DC
September 9, 2016

Brief Background

EPIC is an "evidence-based" policy organization. We rely on government statistics and reports for our work.

EPIC also supports the development of new laws and new techniques that enable the use of data while minimizing privacy risks

Served on many expert panels - AAAS, ABA, IOM, IWG, NAS, OECD - with goal of promoting appropriate policy responses to emerging challenges. Currently working with NAS on "Big Data and Privacy" and OECD on Risk Assessment

Speaking for EPIC and not for NAS or OECD

Case Study I: Federal Wiretap Reports

In 1968 Congress created legal authority for electronic surveillance in the United States

Multiple safeguards were established - criminal predicates, application requirements, internal accounting, judicial review and public reporting

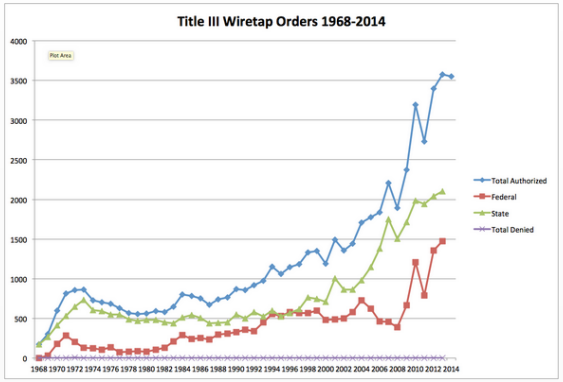
The reporting requirement provides a common data set that allows researchers, advocates, and government officials to describe the scope of lawful electronic surveillance in the United States

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

Policy Issues Our Work Press EPIC Bookstore

Title III Wiretap Orders - Graphs

Title III Wiretap Orders 1968-2015



Federal Wiretap Reports: Key Conclusions

Stable over time. Mandated by law, not voluntary or dependent on private sector data sources, such as "transparency reports"

Methodology is transparent and data is provable

No privacy risk (no PII collected or published)

Ongoing relevance to policy debate (crypto regulations, Apple v. FBI)

Model for evidence-based policy

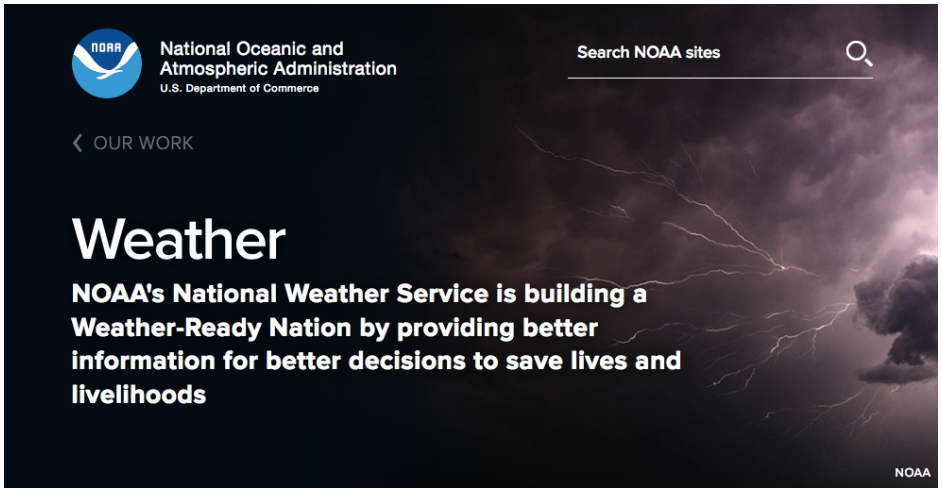
Case Study II: NOAA

Weather forecasting, climate data, and satellite imagery

NOAA data supports fishing, shipping, agriculture, and many associated industries

NOAA data also supports mission critical functions, emergency services, and local and state government

No PII!



Personally Identifiable Information (PII)

PII is core concept in modern privacy law.

PII = "Data that identifies or could identify a particular person"

PII creates obligations, "Fair Information Practices." Obligations are asymmetric. Custodian of data has responsibilities. Data subjects have rights.

Goal is to ensure fairness, transparency, accuracy, and accountability

New techniques may expand boundaries of PII but that does not diminish significance of concept. As PII becomes more readily identified, responsibilities necessarily follow.

Privacy Enhancing Techniques (PETs)

"Techniques that minimize or eliminate the collection of PII" (Burkhart 1998, Rotenberg 2000)

PETs should be robust, scaleable and provable

We support PETs but have also challenged poorly designed PETs (MD5, Ask Eraser, SnapChat)

CEBP could encourage the development of PETs

Risk of PII Collection

Data breach, identity theft, financial fraud

Identity theft is top consumer concern, 2001-2014 (FTC 2015)

Risks are increasing (voting systems)

Collection of PII poses risk to institutions and to data subjects

Data Minimization

Video Privacy Protection Act (1988)

18 U.S.C. 2710 (e)Destruction of Old Records.—

"A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order."

Hard Problems Ahead

Data is increasingly dynamic. It is more difficult to control use, anticipate outcomes, assess risks.

Data is also increasingly under attack from malicious actors. Even well intended data collection and analysis may end badly.

Increasing focus on “Big Data,” AI, and Data Analytics (“One Hundred Year Study on AI,” White House Report on AI)

Use of data for profiling and prediction has direct impact on individuals, even when not PII.

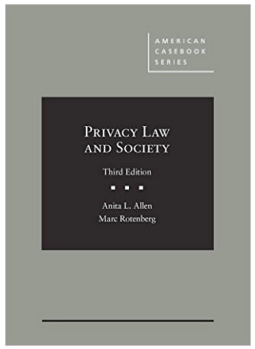
“Algorithmic transparency”

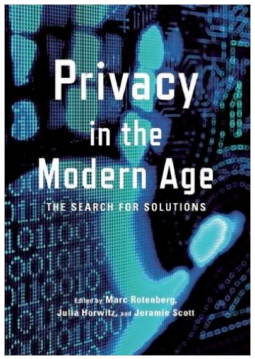
Data is the basis of research, innovation, economic growth, and informed policy decisions,

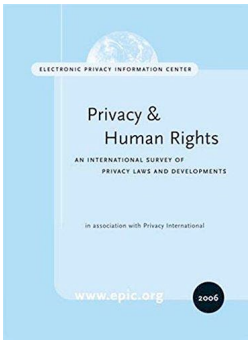
Data is also the basis for profiling, tracking, segmentation, and discrimination

Privacy protections for data are necessary to maximize the benefits and minimize the risks.

References







epic.org/bookstore

Notes on National Data Center (1965)

Proposal inspired by social scientists, rise of automation, opportunity to gather and analyze data collected by government agencies

Tremendous backlash (Packard, "The Naked Society," a NY Times bestseller)

Led to passage of Privacy Act of 1974 => compartmentalized records in federal agencies, established limitations on data matching

Particular concern about record linkages => additional limitations on collection and use of SSN

Renewed concerns in US about mass surveillance after 2013 disclosures of NSA program (led to end of domestic bulk telephone record collection)

EU countries have centralized record systems, but also have stronger laws for data protection

Privacy and Innovation: "Shifting the Curve"