



BIG DATA AND GEOSPATIAL PRIVACY
A TALE OF TWO REPORTS

KEITH C. CLARKE

NGAC meeting June 24-25, 2014

Podesta: Policy/Review

PCAST: Technological implications/Future



BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES

Executive Office of the President

MAY 2014



REPORT TO THE PRESIDENT BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

Executive Office of the President
President's Council of Advisors on
Science and Technology

May 2014



Podesta: Big Data: Seizing Opportunities, Preserving Values

- 90 day study to “examine how big data will transform the way we live and work and alter the relationships between government, citizens, businesses, and consumers”
- Raised questions about how our framework for privacy protection applies in a big data “ecosystem”
- “Big data analytics have the potential to eclipse longstanding civil rights protections in how personal data is used in housing, credit, employment, health, education and the marketplace.”
- Does not single out geospatial data or privacy, but its inclusion is implicit

Podesta: Big Data: Seizing Opportunities, Preserving Values

- Includes definitions of terms in text and in boxes
- Theme is that big data “create an asymmetry of power” between data providers and users
- Notes power to reverse anonymity
- Notes legal system lags technology and that existing law dates from era of mail and phone
- Reviews Obama initiatives: transparency, Open data etc
- Reviews legal history and key rulings and laws
- Consumer privacy Bill of Rights: individual control, transparency, respect for context, security, access and accuracy, collection focus and accountability
- Small data rules hard to apply to big data
- Case studies in health care, education, homeland security, law enforcement

Implications

- Fourth amendment protects people, not places
- Reasonable expectation of privacy
- Rules should apply to data and metadata
- Need to protect against insider threat
- “The big data revolution will take hold across the entire government”
- Big data creates value for companies and consumers
- Consumers have little understanding of the potential loss of privacy, individual and collective

Conclusions

- Estimated \$80M on privacy research across agencies
- Makes specific policy recommendations:
 - ▣ Advance consumer bill of rights
 - ▣ Pass National data breach legislation
 - ▣ Extend law to non-US persons
 - ▣ Protect educational big data
 - ▣ Expand technology to prevent discrimination e.g in pricing
 - ▣ Amend the Electronic Communications Privacy Act

Podesta: Policy/Review

PCAST: Technological implications/Future



BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES

Executive Office of the President

MAY 2014



REPORT TO THE PRESIDENT BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

Executive Office of the President
President's Council of Advisors on
Science and Technology

May 2014



Presidents Council of Advisors on Science and Technology (PCAST)

- Designed to complement Podesta report with technical literature and examples
- Key finding is that current emphasis on protecting data at point of collection is no longer valid, recommends a use-based privacy target
- Shifts from consent to analytics, consumer to company
- Government has role to create standards, educate, encourage markets, provide punishments

PCAST report structure



- Summary
- Introduction and background
 - Introduces new “harms”
- **Examples and Scenarios**
 - Healthcare
 - “Home” vs. cyberspace
 - Tradeoff: privacy, security and confidence
- Collection, Analytics and Supporting Infrastructure
 - Explicitly includes GPS, LiDAR, SAR, remote sensing, tracking data as “born analog”
 - Notes that image recognition can reveal “precise geolocation in imagery from satellites or drones”
 - Includes Google streetview, Bing Maps
- **Technologies and Strategies for Privacy Protection**
 - Identify, authorization, availability, confidentiality, integrity, auditability
 - Perfect information security may be unachievable
 - Suggests next generation improvements in existing methods
- Perspectives and Conclusions
 - Recommendations

Born digital vs. born analog

- Born digital: data created by us or a computer surrogate, specifically for use by a computer or data processing system
 - ▣ Example is e-mail
- Born analog: arises from the characteristics of the physical world
- Created when a device (e.g. camera, microphone) talks to a digital medium
 - ▣ Example is a digital photograph
 - ▣ Often involves overcapture
 - ▣ Becomes important to privacy when data are fused
- Again, geospatial by implication

PCAST report notes that:

- Some privacy protections exist and need enhancement: cybersecurity standards, encryption, audit control
- Many existing systems are not robust to big data analytics
- Anonymization, data deletion, separating data and metadata likely to fail
- Notice and consent already failing, “unworkable”

PCAST findings

- Notice and consent are a non-level playing field biased against the consumer
- Privacy protection profiles could be developed and become a market that would benefit all
- Shift obligation of privacy protection to the data user
- Need to impose standards for accuracy and integrity, e.g. right to access own data
- Privacy protection cannot be achieved by technical measures alone

PCAST recommendations

- Policy to focus on use, not collection or analysis
- Policies should not embed particular technologies and should focus on intended outcomes
- NITRD agencies should strengthen U.S. research on privacy technologies, including in social science
- OSTP should encourage increased education and training opportunities, including professional career paths
- US should lead in creating new policy, PCAST not convinced other nations are pursuing privacy in a comprehensive way

Some personal observations



- Geospatial probably under-covered, as many key legal decisions have involved tracking and GPS
- Elimination of overhead imagery resolution restrictions likely to have an impact
- Read Kevin Pomfret's "*Summary of Location Privacy in the United States*" and his memo "*Should this be a wake-up call*"
- Clear link between privacy rights and democracy
- Expect much attention on geoprivacy in the years ahead
- There exists a short-lived golden opportunity to combine practicality, study, law, government and business needs with technological solutions