CS 4873-A: Computing and Society

Munmun De Choudhury | Associate Professor | School of Interactive Computing

Week 7: Privacy and Governmental Surveillance
February 28, 2021

Big data meets Big Brother as China moves to rate its citizens

Rachel Botsman

23-29 minutos

On June 14, 2014, the State Council of China published an ominous-sounding document called "Planning Outline for the Construction of a Social Credit System". In the way of Chinese policy documents, it was a lengthy and rather dry affair, but it contained a radical idea. What if there was a national trust score that rated the kind of citizen you were?

A Balancing Act

- Federal, state, and local governments in United States have had significant impact on privacy of individuals

- Government must balance competing desires of citizens
  - desire to be left alone
  - desire for safety and security

Two case examples of this balancing act…

Solove's Taxonomy of Privacy

- **Information collection:** Activities that gather personal information

- **Information processing:** Activities that store, manipulate, and use personal information that has been collected

- **Information dissemination:** Activities that spread personal information

- **Invasion:** Activities that intrude upon a person's daily life, interrupt someone's solitude, or interfere with decision-making

1) Information collection – gathering personal information.
2) Information processing – storing, manipulating, using personal info that has been collected
3) Information dissemination – spreading personal information
4) Invasion – intruding upon a person's daily life, interrupting someone's solitude, or interfering with decision-making

a) Privacy is the right to be left alone (Warren & Brandeis).
b) Privacy is the state of being away from public attention (Gavison).
c) Privacy is control over who knows what about us (Rachels).
d) Privacy is the appropriate flow of personal information (Nissenbaum).
e) Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves (Fried).

Information Collection by the Government (Direct)

- Purpose: accountability and fairness

Census Records

- Census required to ensure every state has fair representation
- Number of questions steadily rising
- Sometimes Census Bureau has broken confidentiality requirement
  - World War I: draft resistors
  - World War II: Japanese-Americans

Internal Revenue Service Records

- The 16th Amendment to the US Constitution gives the federal government the power to collect an income tax

- IRS collects more than $2 trillion a year in income taxes

- Income tax forms contain a tremendous amount of personal information: income, assets, to whom you make charitable contributions, medical expenses, and more

- NCIC
  - Collection of databases related to various crimes
  - Contains > 39 million records
- Successes
  - Helps police solve hundreds of thousands of cases every year
  - Helped FBI tie James Earl Ray to assassination of Dr. Martin Luther King, Jr.
  - Helped FBI apprehend Timothy McVeigh for bombing of federal building in Oklahoma City

Discussion Point: What are the downsides of maintaining the NCIC database?

Closed Circuit Television Cameras

- First use in Olean, New York in 1968
- Now more than 30 million cameras in US
- New York City's effort in lower Manhattan
  - $201 million for 3,000 new cameras
  - License plate readers
  - Radiation detectors

Discussion Point: Are surveillance cameras effective?

Mixed opinion: ACLU opposition; London bombings in subway in 2005

Social Security Number

- Social Security cards first issued 1936
- Originally used only for Social Security purposes
- Use of SSN has gradually increased
- SSN is a poor identification number
  - Not unique
  - Rarely checked
  - No error-detecting capability

SSN -> National Identification Card -> Discussion in your section in two weeks (week after midterm)

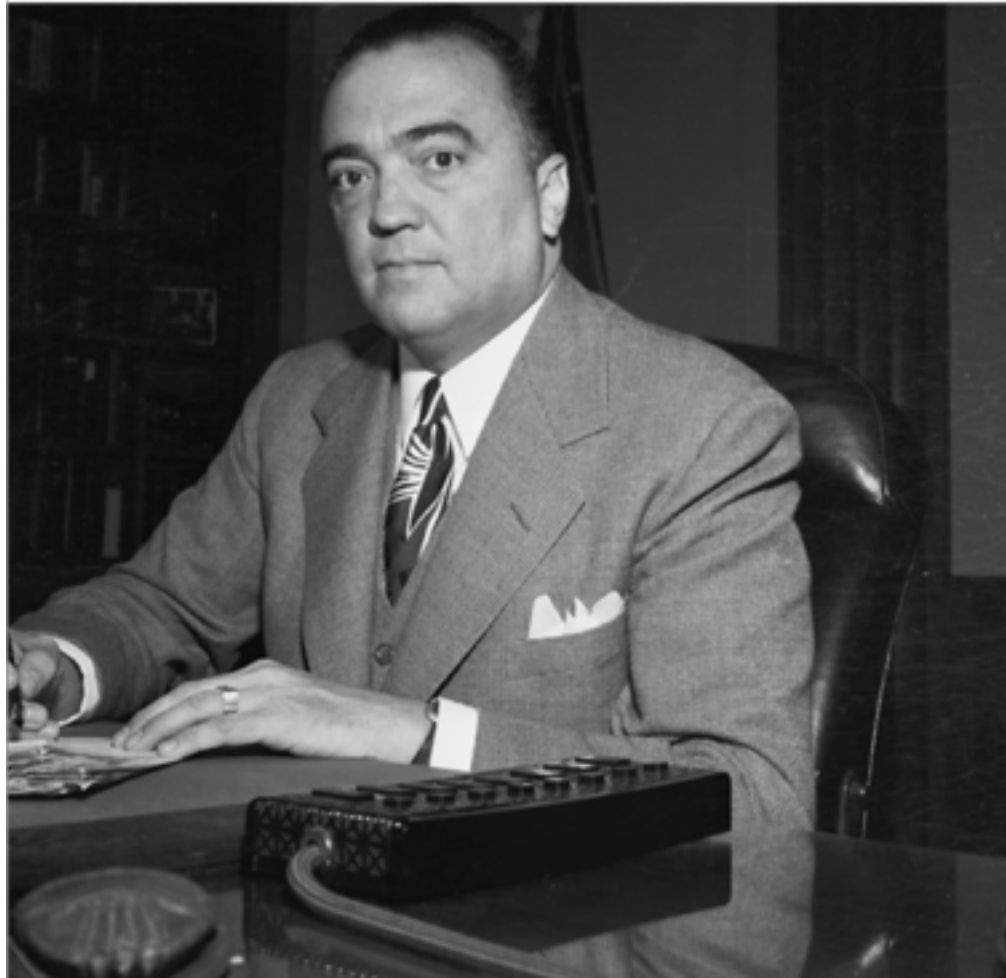# Challenges of government information collection

Surveillance Camera Images of Boston Marathon Bombing Suspects

Covert Government Surveillance

Wiretapping – J. Edgar Hoover

© Bettmann/CORBIS

First Director of FBI

Privacy Post 9/11

- National security concerns increased significantly after 9/11 attacks

Privacy Post 9/11

- (2006 poll) 70% Americans supported "expanded camera surveillance on streets and in public places"

- 62% supported "law enforcement monitoring of Internet discussions in chat rooms and other forums"

- 61% supported "closer monitoring of banking and credit card transactions to trace funding sources"

- 52% supported "expanded governmental monitoring of cell phones and emails to intercept communications"

NSA Wiretapping Post 9/11

- President Bush signed presidential order
  - OK for NSA to intercept international phone calls & emails initiated by people inside US
  - No search warrant required
- Number of people monitored
  - About 500 people inside US
  - Another 5,000-7,000 people outside US
- Two al-Qaeda plots foiled
  - Plot to take down Brooklyn bridge
  - Plot to bomb British pubs and train stations

Information Processing/Mining by the Government

Syndromic Surveillance Systems

- Syndromic surveillance system: A data mining system that searches for patterns indicating the outbreak of an epidemic or bioterrorism
  - 911 calls
  - emergency room visits
  - school absenteeism
  - Internet searches

- Example: A system in New York City detected an outbreak of a virus in 2002

When can information processing/data mining by the Government go wrong?

THE NSA'S SECRET ROLE IN THE U.S. ASSASSINATION PROGRAM

Government Legislation restricting information dissemination

Family Education Rights and Privacy Act (FERPA)

- Rights given to
  - Students 18 years and older
  - Parents of younger students
- Rights include
  - Reviewing educational records
  - Requesting changes to erroneous records
  - Preventing release of records without permission

Health Insurance Portability and Accountability Act (HIPAA)

- Limits how doctors, hospitals, pharmacies, and insurance companies can use medical information

- Health care providers need signed authorization to release information

- Health care providers must provide patients with notice describing how they use medical information

CS 4873-A: Computing and Society

Munmun De Choudhury | Associate Professor | School of Interactive Computing

Week 7: The Patriot Act
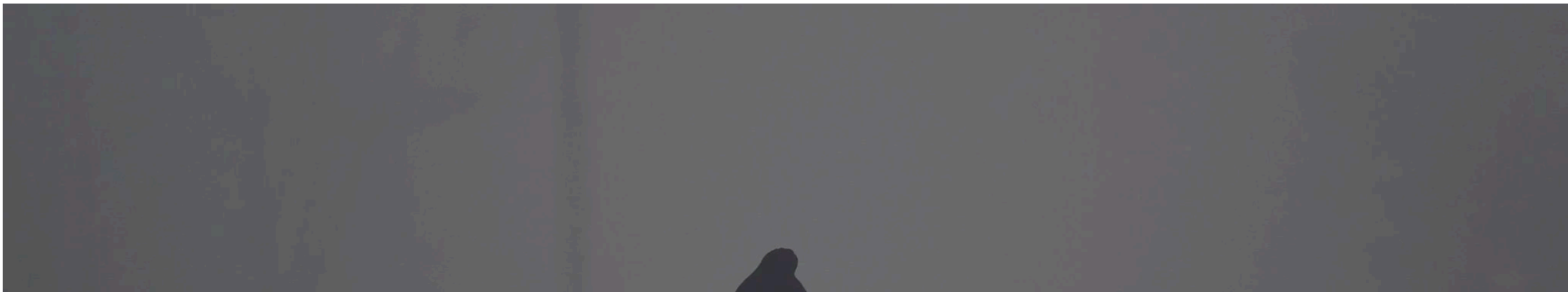## March 2, 2021

All This Dystopia, and for What?

When privacy-eroding technology doesn't deliver on its promises.

By **Charlie Warzel**
Mr. Warzel is an Opinion writer at large.

Feb. 18, 2020

6.6 USA PATRIOT Act

National Security Letters

Analysis of the USAPA by President Bush

"Surveillance of communications is an essential tool to pursue and stop terrorists. The existing laws were written in the era of rotary telephones. This bill met with an overwhelming support in Congress because it upholds and respects civil liberties."

Terrorism In the U.S.

Courtesy KOCO

- The need to fight terrorism

- Relation to computing

The Dark Side of Social Media:
Review of Online Terrorism

Dr. Geoff Dean, Peter Bell, Jack Newman

Abstract

This paper lays the conceptual foundation for understanding the significant role that social media can and does play in relation to spreading the threat and growth of terrorism, especially 'home-grown' terrorism. The utility of social media applications (eg. Facebook, Twitter, You Tube) to recruit, communicate and train terrorists is explored through the perspective of Knowledge-Managed Policing (KMP). The paper concludes with the implications this conceptual analysis of terrorism as a new dot.com presence on the internet has for law enforcement and the global cyber community.

Introduction

The advent of social media (eg. Facebook, Twitter, You Tube) has created new opportunities for terrorist organisations and brought with it growing challenges for

Radicalization and the Use of Social Media

Robin Thompson
National Aeronautical and Space Administration
dr.robin.thompson@gmail.com

Abstract

The use of social media tools by individuals and organizations to radicalize individuals for political and social change has become increasingly popular as the Internet penetrates more of the world and mobile computing devices are more accessible. To establish a construct for radicaliza-

Terrorism In the U.S.

Courtesy KOCO

- Domestic vs. International terrorism

- The need to fight terrorism

- Relation to computing

- The government's solution

Patriot Act Successes

- Charges against 361 individuals
    - Guilty pleas or convictions for 191 people
    - Shoe-bomber Richard Reid
    - John Walker Lindh
- More than 500 people removed from United States
- Terrorist cells broken up in Buffalo, Seattle, Tampa, and Portland ("the Portland Seven")

Does knowing the government has far-reaching powers to gather information on individuals phone calls, emails, Internet usage, etc. suppress free speech?

Patriot Act Failure

- March 11, 2004 bombings in Madrid Spain
- FBI makes Brandon Mayfield a suspect
    - Claims partial fingerprint match
    - Conducts electronic surveillance
    - Enters home without revealing search warrant
    - Copies documents and computer hard drives
- Spanish authorities match fingerprint with an Algerian
    - Judge orders Mayfield released
    - FBI apologizes
- Civil rights groups: Mayfield was targeted for his religious beliefs

Who Are the Stakeholders?

- Computer users in the public

- Internet Service Providers

- Libraries

- Law Enforcement

- Terrorists

Discussion Point 1A: Ethical Question

- The Patriot Act allows for ISPs to "voluntarily" disclose information to law enforcement, how will the public view the ISP who "might" have had information which could have prevented a terrorist act?

    - Use an act utilitarian and social contract theory perspective.

Discussion Point 1B: Ethical Question

- Is it ethical to allow ISPs to make the determination of whether or not there is an emergency involving immediate danger of death or serious physical injury to any person?

  - Use a Kantian and virtue ethics perspective.

Discussion Point 1C: Ethical Question

- Is it ethical that the Patriot Act makes law enforcements job of apprehending criminals easier at the cost of affecting a greater number of innocents?

The PRISM Program
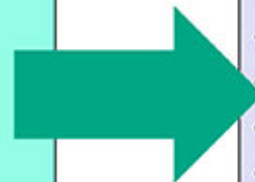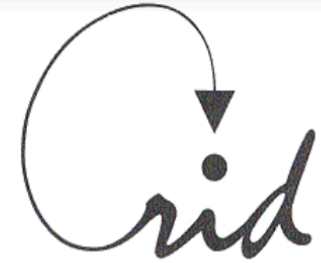
The Airline Passenger Data Disclosure Case
and the EU-US Debate

María Verónica Pérez Asinari* and Yves Poullet**
Centre de Recherches Informatique et Droit (CRID)
University of Namur
Belgium
http://www.crid.be
September 2003

Introduction

In the aftermath of the events of 11th September 2001, decisions have been taken unilaterally by US authorities requiring air line companies to provide direct access or transfer of data concerning passengers and cabin crews flying to, from or within the US to certain US administrations. These decisions have been challenged by EU authorities

The 9/11 terrorist attacks forever change the balance between security and freedom. Will things ever go back to the way they were before the attacks? Would you want them to?