CS 4873: Computing, Society & Professionalism

Munmun De Choudhury | Assistant Professor | School of Interactive Computing

Week 7: The Patriot Act/Privacy and the Government
February 19, 2020

Challenges of government information collection/processing and dissemination

Surveillance Camera Images of Boston Marathon Bombing Suspects

**

Wiretapping – J. Edgar Hoover

© Bettmann/CORBIS

First Director of FBI

6.5 US Legislation Authorizing Wiretapping

Title III

- Part of Omnibus Crime Control and Safe Streets Act of 1968
- Allows a police agency with a court order to tap a phone for up to 30 days
- In 1972 US Supreme Court again rejected warrantless wiretapping, even for national security

**

Electronic Communications Privacy Act

- Passed by Congress in 1986
- Allows police to attach two kinds of surveillance devices to a suspect's phone line
  - Pen register: displays number being dialed
  - Trap-and-trace device: displays caller's phone number
- Court order needed, but prosecutors do not need to show probable cause
- Allows police to do roving wiretaps (following suspect from phone to phone)

**

Do you think the government should have access to the phone calls and emails of suspected terrorists? How should it identify "suspected terrorists"?

Stored Communications Act

- Part of Electronic Communications Privacy Act

- Government does not need a search warrant to obtain from an Internet service provider email messages more than 180 days old

- Advent of cloud computing raises new privacy concerns

- Digital Due Process organization (nearly 50 companies and privacy rights organizations) lobbying Congress to change law

How would it make you feel if you found out that the government could access your phone calls and emails? Would you change what you said/wrote in any way?

6.6 USA PATRIOT Act

The USA Patriot Act

- Formal definition: the Uniting and Strengthening America by Providing Tools Required To Intercept and Obstruct Terrorism (USAPA)

**

Foreign Intelligence Surveillance Act

- FISA provides judicial and congressional oversight of covert surveillance of foreign governments and agents
- Allows electronic surveillance of foreign nationals for up to one year without a court order
- Amended in 2007 to allow government to wiretap communications to/from foreign countries without oversight by FISA Court

**

Terrorism In the U.S.

Courtesy KOCO

- The need to fight terrorism

- Relation to computing

Definition of Terrorism

- FBI defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government or civilian population"

Definition of Terrorism

- The Patriot Act defines terrorism differently.

- Expands notion of "domestic terrorism"

- Amends Computer Fraud and Abuse Act by stating that computer crimes are "terrorist offenses"

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 radical-ize individuals for political and social change has become increasingly popular as the Internet penetrates more of the world and mobile comput-ing 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

Some of the Major Provisions

**

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."

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?

Analysis of the USAPA by the EFF*

"It seems clear that the vast majority of sections included have not been carefully studied by Congress, nor was sufficient time taken to debate it or hear testimony from experts. The civil liberties of ordinary Americans have taken a tremendous blow"

* Electronic Frontier Foundation

**

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

Class Discussion 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.

Class Discussion 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.

Class Discussion 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

- PRISM is a code name for a program under which the United States National Security Agency (NSA) collects internet communications from various U.S. internet companies

- PRISM began in 2007 in the wake of the passage of the Protect America Act under the Bush Administration

The PRISM Program

- Its existence was leaked six years later by NSA contractor Edward Snowden

- Snowden warned that the extent of mass data collection was far greater than the public knew and included what he characterized as "dangerous" and "criminal" activities.

- The disclosures were published by The Guardian and The Washington Post on June 6, 2013

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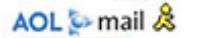
The 9/11 terrorist attacks forever change the balance between security and freedom. Will things ever go back to the way they were before the attacks? Would you want them to?