CS 4873: Computing, Society & Professionalism

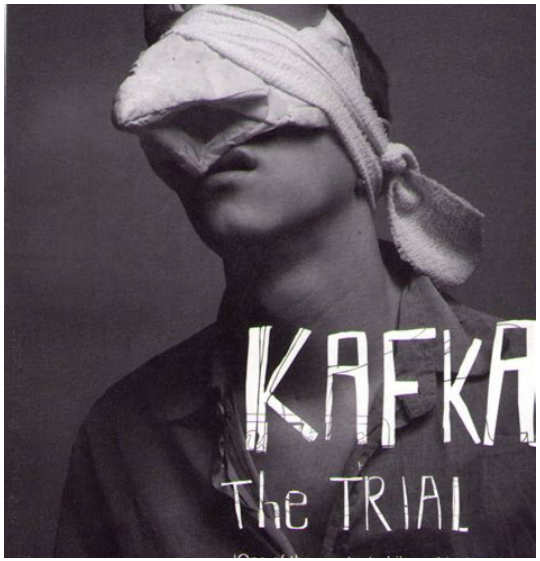
Blair MacIntyre | Professor | School of Interactive Computing

Week 9: The Patriot Act and Government Surveillance

March 15, 2021

Slides adapted from Sauvik Das, Munmun de Choudhury, and Amy Bruckman

“Surveillance” often brings up imagery and associations with Orwell’s Big Brother



Solove said a more apt metaphor might be Kafka’s The Trial

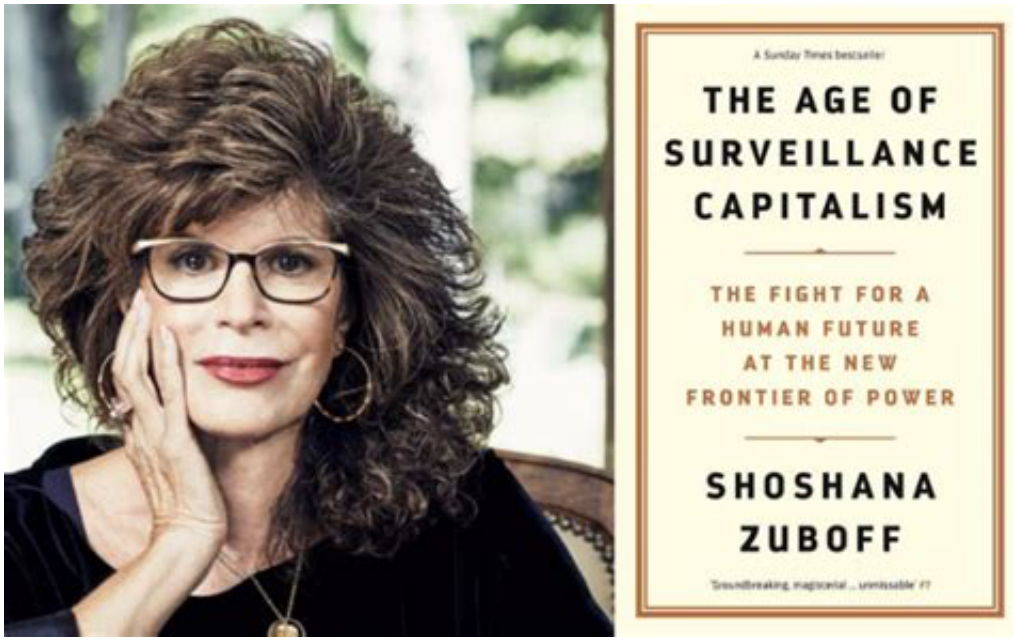
Neal Stephenson: 1984 is not the right metaphor for the current world we live in

- Neal Stephenson talk at Computers, Freedom and Privacy conference.

Big Brother	Domination Systems
One threat	Many threats
All-encompassing	Has edges
Abstract	Concrete
Centralized	Networked
Irredeemable	Redeemable

The Corporate "Zones of Domination"

Engineering Consent



Much like large industrial manufacturers exploited the work of individual laborers for disproportionate profits in the Industrial age, “big data” companies exploit the data of individual Internet users for disproportionate profits in the Information Age.

Engineering the Public
Tufekci (in optional readings)

The rise of big data

The shift away from demographics to individualized targeting

The opacity and power of computational modeling

The use of persuasive behavioral science

Digital media enabling dynamic real-time experimentation

The growth of new power brokers who own the data or social media environments

3. Power of computational modeling

- Combining otherwise “benign” pieces of data
- Multiple types of data aggregated together
- Individualized modeling
  - Facebook “likes” is sufficient to model and accurately predict a striking number of personal attributes including “sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender” (Kosinski, et al., 2013)
  - Identify “likely voters”, beyond surveys like Gallup

Once Upon a Crime: Towards Crime Prediction from Demographics and Mobile Data

Andrey Bogomolov
University of Trento,
Telecom Italia SKIL Lab
Via Sommarive, 5
I-38123 Povo - Trento, Italy
andrey.bogomolov@unitn.it

Bruno Lepri
Fondazione Bruno Kessler
Via Sommarive, 18
I-38123 Povo - Trento, Italy
lepri@fbk.eu

Jacopo Staiano
DISI, University of Trento
Via Sommarive, 5
I-38123 Povo - Trento, Italy
staiano@disi.unitn.it

Nuria Oliver
Telefonica Research
Torre Telefonica, Diagonal 00
Barcelona, Spain
nuriao@tid.es

Fabio Pianesi
Fondazione Bruno Kessler
Via Sommarive, 18
I-38123 Povo - Trento, Italy
pianesi@fbk.eu

Alex (Sandy) Pentland
MIT Media Lab
20 Ames Street
Cambridge, MA, USA
pentland@mit.edu

Automatic Crime Prediction using Events Extracted from Twitter Posts

Xiaofeng Wang, Matthew S. Gerber, and Donald E. Brown

Department of Systems and Information Engineering, University of Virginia
{xw4u,msg8u,brown}@virginia.edu

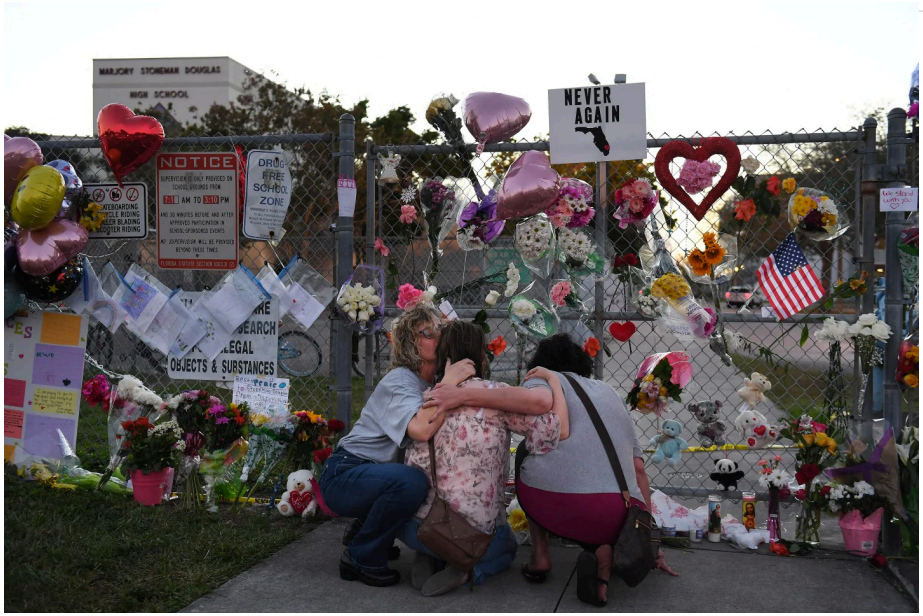
(a) Three samples in criminal ID photo set S_c.

(b) Three samples in non-criminal ID photo set S_n

Figure 1. Sample ID photos in our data set.

Technology

Parkland school turns to experimental surveillance software that can flag students as threats



4. Behavioral science

- Habermas' (1989) ideal of the public sphere imagined status–free actors carrying out rational conversations based on merit
  - Political practitioners have long recognized that the "rational voter" model did not correspond to their experience in the world.
- Fear tactics appeal to the irrational, but have rarely been successful in the past
  - Fear tactics can be creatively manipulated
- Persuasion models (targeting the "irrational") using big data to sway public opinion
  - Obama campaign found white envelopes signaled credibility
  - Wage disinformation campaigns

6. Power of platforms and algorithmic governance

- Much political and civic speech occurs in the “fifth estate”
  - Data owned by private corporations
  - Platforms operate using opaque algorithms
  - Proprietary algorithms assess visibility of content
- Political “apps” of the 2012 Obama and Romney campaigns
  - Political actors’ attempts to “game” these algorithms (Tufekci 2013) or wondering how to censor them (Lotan 2011)
  - (Political) groups without funds to promote their content will become hidden from public view, or will experience changes to their reach that are beyond their ability to control
- A biased platform could decide to use its own store of big data to model voters and to target voters of a candidate favorable to the economic or other interests of the platform owners

The Government “Zone of Domination”: USA PATRIOT Act

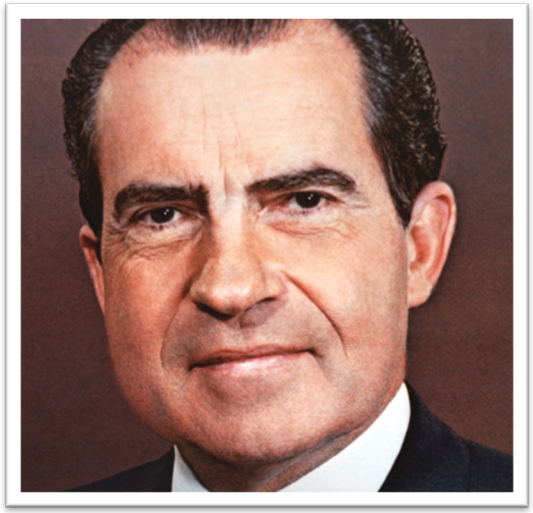
Assumptions in the U.S.A.

- Need protection from terrorism and unlawful activity.
- BUT, don't want to give up all civil liberties as a result.
- Checks and balances between branches of government help maintain balance between the two goals.

Chain of legislation

- FISA – Foreign Intelligence Surveillance Act (1978, post-Watergate)
- Modified by the Patriot Act (2001, post 9/11)
- Modified by the Protect America Act (2007), expired in 2008
- Modified by the FISA Amendments Act (2008)
- Modified by the USA Freedom Act (2015)
- Modified by the USA Freedom Act (2020)

Foreign Intelligence Surveillance Act (FISA) (1978) (changes 2007)



- Watergate: Nixon spied on political opponents

- Not the most legal thing he could have done
  - But begs question: What kind of spying is legal?
  - Clearly need some so that law enforcement can detect material threats
  - Thus, FISA
    - Provides oversight but also secrecy
    - Checks and balances

- Government goes to FISA Court for: “approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes”

FISA

- Without a court order, President (through Attorney General) may:
  - Authorize surveillance for one year
    - "no substantial likelihood" that it will include communications with U.S. person
- With court order (from FISA court):
  - If U.S. person is party, need a court order within 72 hours of starting surveillance
  - Must demonstrate probable cause
  - Target must be affiliated with a foreign power

The Protect America Act of 2007

- Removed warrant requirement for government surveillance of foreign intelligence targets "reasonably believed" to be on foreign soil, even if target is “US person”
  - If "target" is foreign, can get all their communications whether they are in US or not
- Removed warrant requirement for any communication which was “foreign-related”, even if it involved a U.S. location.
- Gives civil & criminal immunity to companies for complying with this
- Six month sunset provision (auto self-destruct)

FISA Amendments Act (2008)

- Bush administration had been engaging in warrantless wiretapping
  - Telephone companies helped
- Reauthorizes Protect America Act
  - Of special note: immunity for companies that comply with warrantless wiretapping requests
- FISA Court can give permission to wiretap Americans overseas
- Section 702: Requires telcos (e.g., ATT) to turn over all data that matches court-approved search terms

The USA PATRIOT Act (2001)

*The **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism*

- Passed immediately after 9/11 with little debate
  - Signed into law by President Bush on 10/26/01
  - Only one senator voted against it
  - Not enough time for legislators to actually read it

Provisions of the PATRIOT Act

- Gives federal gov't and intelligence agencies more authority to monitor communications
- Gives secretary of treasury greater powers to regulate banks
  - To prevent money laundering
- Makes it more difficult for terrorists to enter the US
- Defines new crimes and penalties for terrorist activities

Patriot Act

- Can track information online without probable cause
  - Just need to state it's relevant to an "ongoing investigation"
- Extends jurisdiction of wiretaps to whole US
  - NY judge can authorize wiretapping in CA
- Warrantless search
- Sneak 'n peek
  - Enter premises without letting anyone know you were there (declared unconstitutional in 2007)
- Broadens "roving" surveillance
  - Associates surveillance with person, not device
  - Don't have to prove person is actually using device
- Lone wolf provision
  - Target of surveillance no longer needs to be affiliated with a foreign power

Section 215 of Patriot Act

- FBI can collect records of businesses, libraries, medical, educational and religious institutions
- Don’t need to demonstrate probable cause
  - Institution can’t reveal existence of warrant, or tell anyone what info they gave

- Reduced attendance and donation to mosques immediately after

Section 505: National Security Letters

- Subpoena of personal records w/o probable cause
- Originally aimed at espionage suspects
  - Now can be used on anyone, even if not suspected of criminal activity
- Gag order prevents recipient of request for info from revealing the NSL
  - Ruled unconstitutional by lower court in 2007
  - FBI doesn't appeal, continues doing it
  - EFF still appealing constitutionality

Uptick in NSLs post-Patriot Act

- Pre-patriot act, about 8,500 NSLs issued.
- Post-patriot act, between 2003-2005:
  - 2003: 39,346 – 39% on US persons
  - 2004: 56,507 – 51% on US persons
  - 2005: 47,221 – 53% on US persons
- For:
  - Counter-terrorism (73.6%)
  - Counterintelligence (26%)
  - Foreign Cyber Investigations (0.4%)

USA Freedom Act (2015)

- Renews key provisions of the Patriot Act
- Instead of US collecting bulk communications data (under section 215), telcos will hold it and hand it over if they get a court order

Patriot Act successes

- Charges against 361 individuals
  - Guilty pleases or convictions for 191
  - Including: shoe-bomber Richard Reid
- More than 500 people linked to 9/11 attacks removed from US
- Terrorist cells broken in Buffalo, Seattle, Tampa and Portland

Example of patriot act failure

- Brandon Mayfield
  - FBI convicts him for the 3/11/04 train bombings in Madrid based on a partial fingerprint match
  - Conducts electronic surveillance
  - Enters home without search warrant
  - Copies documents and hard drives
- Later, Spanish authorities match fingerprint with someone else
  - Judge orders Mayfield release and FBI apologizes
- Mayfield may have been targeted for his religious beliefs
  - Converted to Islam and has an Egyptian-born wife

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

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN