6.805/6.806/STS.085, Ethics and Law on the Electronic Frontier

Lecture 8: Anonymity vs. Transparency

Lecturer: Danny Weitzner

Transparency & Accountability

Think of this as a review of what has been covered regarding privacy and electronic surveillance. We will have a lecture followed by a mock congressional hearing.

(Brin reference)
We're now living in a world that has more transparency challenges. We are also trying to understand what kind of accountability (of others, universities, etc) we should have of others. As a result, there is another paradox that results. This transparency paradox is counterintuitive to the current thoughts on the subject.

Steps

1. The End of "Stove-Pipes"
- stovepipes are different collections of information. They are independent and do not intersect. From a privacy standpoint, stove-pipes have limited the access that gov. even has. These stove-pipes are gradually coming to an end

2. Cost of Storage is approaching zero.
   Google is now saying don't delete your email. Previously, companies were really concerned about document-retention policies that were partly driven by costly document-retention policies and also by the fact that ISPs did not want to be document repositories.
- Now Google and others are going to keep everything as opposed to engaging in the costly endeavor of trying to figure out *what* to delete.

3. Cheap-query: institution-wide and Web-wide
- It has become easier and easier to do large-scale queries. Yahoo and Google have made this a business. It has also become uncool for a website not to have a search feature.

4. Location-aware Sensor Nets
- Once you stamp a piece of data with a location and time-marker then you can use it to associate with other pieces of information.

All of these things cause a huge problem for those that are worried about privacy.

There is a real risk regarding technological determinism when we think about privacy. Privacy thinking, in general, is attached to images.

- Image example of Jeremy Benett's Penoptecon, which is a prison. He thought that this design was great because you only needed to put one person at a certain location and they could see everyone and everything at that location. This was thought to be an idea of prison reform, but has now come to signal the representation of privacy.

- Technical designs are not what they seem to be. For privacy, we have to think beyond what the policies and threats appear to be.

We should not think that we should separate ourselves off from others and shut down our email accounts and cell-phones. Instead the key challenge we need to face is that the intrusions deal with data-mining and other techniques over large collections of data. We focus a lot on limiting the privacy information and limiting evidence, but what I think we should be worried about is the kind of inferences that can be drawn from the vast amount of information that is out there about us. Also what kind of controls we want to place on those inferencing controls.

Privacy law and 4th amendment law has really been about what information can be collected not about what can be inferred from the information collected. Those laws require that the collector of the information specify a purpose and stay within the bounds of that purpose.

In general, we're not good at putting bounds on purpose collected information.

Jumping ahead to The Transparency Paradox….

We are going to have to get comfortable with the idea that information is directly relatable or inferable about us. Inferencing laws are complicated.

Are we prepared to do this intrusive inferencing policies with data collection?

- Someone getting on airplane…not a terrorist, but owes back tax and having IRS waiting once they get off the plane.

Fundamentals of European law is that anyone who holds database information must register that information with government. In the U.S. this is not the case, probably because we don't trust the government. The lack of trust centers on the commercial sector in Europe as opposed to the government in the U.S.

There is a whole range of cryptographic theory that is being developed to enhance privacy. (ie. Data obscuring)

One of the models we will come to look at is the Fair Credit Reporting Act. The model they have adopted doesn't try to restrict who has the information, but the trade-off is that there are higher accountability levels. Fair Credit Reporting Act came into existence in the 70s.

Format for Congressional Hearing:

- All witnesses will have written statements that the committee has read. Each witness should prepare a 5 minute opening statement to the committee.

####
Profiling and Transparency Exercise: Yahoo Secure Traveler

Opening Statements:

<u>Michael Shirton</u>
After 9/11, the commercial companies were able to use this information to track down the terrorists. Information is already available and accessible. We want to

entirely eliminate searches. We'd like the make the airline system more efficient and consistent across airports. This will be more standardized.

Jerry Yodle

Sharing YahooPoint Method (blackboard diagram)

- This technique is Secure Function Computation. Name only sent but cannot be decrypted to YahooPoint. Secure name record is transmitted to TSA.
- Technique also used by Israeli airlines

ACLU

- Broad, efficient-less searches
- Should we replace this system with entire profiling system?
- We are concerned with the safety of passengers
- Some devices cannot be caught by profiling system, so this puts the passengers at risk
- Profiling system should be audited and should have strict restrictions.
- Could be ineffective until advised and need further consideration

Hal Abelson

- Carnival Booth Effect Paper: some will try to reverse engineer the algorithm and terrorists will target those that are less likely to be searched.
- Kirchoff's Principle
- Any system should be reviewed under academic scrutiny before being deployed.

David Flyer

- System not secure
- False Positives: Individuals identified as terrorists that are not and there is no method for regress for those consistently profiled as terrorists
- False Negatives: Worst Case! Inviting Terrorists to get through system without being searched. There are some terrorists that may take advantage of the system.
- Can also slip weapons into unprofiled passengers bag, then regain access of weapon once on the plane.

Jon Gilmore

- Think system is ineffective
- Concerned about dangers of no searches and non-anonymity of passengers with profiling system

Questions from Committee:

What is the benefit of allowing people to travel anonymously?
It's a right. You should only be required to do a reasonable search. So to travel that just means checking for bombs or safety violations…no more. There is no need to check other personal information.

Shirton- Having access to information needs to be done. Searching is not enough.

To ACLU, what do you think makes the system not accountable?
Past track-record. Privacy should be reserved for passengers and private contractor should be regulated via government. We would also like to review the algorithm scheme along with the academic community.

How do we know that the cloud of “Secure function computation” is secure?

How are you going to address international flyers? In advance of 2004, all flights that fly into the U.S. would undergo security clearance. So this would also play into our system.

Data by ChoicePoint is 63% incorrect from source in 2004. This is a serious concern as it relates to the efficiency of the program.

To John Gilmore:
To remain anonymous, are you suggesting that we do physical searches for every single person? Yes.

Closing Statements:
System is a good start, but definitely needs to implement additional measures to make the YahooPoint system more secure.

Recommendation to supplement Yahoo Point system. We cannot eliminate searches at this time.

Don’t believe system will make the current system more secure, but it instead invite more terrorist activity. Should also be a redress system implemented within Yahoo system.