A TAXONOMY OF PRIVACY

Paper by DANIEL J. SOLOVE
Presented By
Gayathri Subramanian
Neelima Harikrishna
Overview

- Background Information and an Overview of Idea Presented
- Taxonomy of Privacy
Privacy is a concept in disarray. Nobody can articulate what it means.

A simple definition – “right to control information about oneself”

Privacy means different things to different people

There is no privacy violation when a person consents to a particular act.

Often Privacy problems are stated in knee-jerk format – “This violates my privacy!”
Privacy and Society are inter-related

As sociologist Barrington Moore aptly observes, “the need for privacy is a socially created need. Without society there would be no need for privacy.”

Privacy is the relief from social frictions in the society.

People should be held accountable for their private activities.

Privacy is an individualistic right.

Privacy conflict should express conflict affecting everyone. It should make some contribution to welfare of the community.
The 9/11 Commission Report, for example, recommends that, as government agencies engage in greater information sharing with each other and with businesses, they should “safeguard the privacy of individuals about whom information is shared.”

“This violates my privacy and privacy must be protected” – it is unclear what they mean. This lack of clarity creates a difficulty when making a policy or resolving a case.
- A newspaper reports the name of a rape victim.
- Reporters deceitfully gain entry to a person’s home and secretly photograph and record the person.
- New X-ray devices can see through people’s clothing, amounting to what some call a “virtual strip-search.”
- The government uses a thermal sensor device to detect heat patterns in a person’s home.
- A company markets a list of five million elderly incontinent women.
- Despite promising not to sell its members’ personal information to others, a company does so anyway.
Privacy is far too vague a concept to guide law making.

These violations are clearly not the same. Privacy must make sense in multitude of problems which exists.

Courts and policymakers frequently have a singular view of privacy in mind when they access whether or not an activity violates privacy.

Paper aims to develop a taxonomy that shifts the focus away from vague term “privacy” towards specific activity that pose privacy problems.
Secrecy Paradigm – “privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data is[are] revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information.”

Prof. Solove argues that this is inadequate definition to guide privacy laws.
Types of Harms caused by privacy violations

- Physical injury
- Injury to the feelings
- Dignitary harm - reputational injury, harms of incivility, lack of respect
- Architectural problems - that create a risk that the person might be harmed in the future
In a legal context, a chilling effect is the term used to describe the inhibition or discouragement of the legitimate exercise of a constitutional right by the threat of legal sanction. Activities involving a person’s information, for example, might create a greater risk of that person being victimized by identity theft or fraud. The classic example is law enforcement officials having too much power, which can alter the way people engage in their activities. Surveillance can also have these effects.
Four basic groups of harmful activities:

1. Information collection
2. Information processing
3. Information dissemination
4. Invasion
INFORMATION COLLECTION

- Surveillance
- Interrogation

Aggregation
Identification
Insecurity
Secondary Use
Exclusion

DATA SUBJECT

INVASIONS

- Intrusion
- Decisional Interference

DATA HOLDERS

INFORMATION DISSEMINATION

- Breach of Confidentiality
- Disclosure
- Exposure
- Increased Accessibility
- Blackmail
- Appropriation
- Distortion
Gathering data

Information can create harm even if the collected information is not publically revealed.

Two forms of Information Collection

- Surveillance
- Interrogation
Watching, listening to or recording of an individual’s activities

Visual Surveillance

Peeping Tom law

Some states prohibit two-way mirrors in certain areas.

Audio Surveillance
Social control can be beneficial eg, CCTV
Continuous monitoring creates problem
Surveillance can lead to self-censorship and inhibition.
Too-much Social control can adversely impact freedom, creativity and self-development.
Covert surveillance creates similar kind of harm because of the fear of being under surveillance
Surveillance collects significantly more amount of data beyond what is originally sought for
A prime example is the FBI’s extensive wiretapping of Martin Luther King, Jr., widely believed to have been initiated in order to expose King’s alleged communist ties. Though the surveillance failed to turn up any evidence of such ties, it did reveal King’s extramarital affairs. The FBI then attempted to blackmail King with the information, and FBI officials leaked it in order to discredit King.
The Fifth Amendment provides that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.”

This is to create “privilege against self-incrimination”

Why do we want to protect a potentially guilty person from having to divulge his/her criminal activities?
What about questions for purposes other than criminal prosecution?

In the late nineteenth century, the U.S. census began including more and more questions relating to personal affairs, such as marital status, literacy, property ownership, health, and finances.
A poem in The New York Sun in 1890 humorously criticized the census:

I am a census inquisitor.
I travel about from door to door,
From house to house, from store to store,
With pencil and paper and power galore.
I do as I like and ask what I please.
Down before me you must get on your knees;
So open your books, hand over your keys,
And tell me about your chronic disease.
These two examples involve a similar practice—“interrogation.”

Interrogation is the pressuring of individuals to divulge information.

The harm interrogation can create depends on degree of coerciveness involved. (Fifth amendment protects against highly coercive interrogation)
Interrogation creates discomfort even if the information is barely disseminated. It creates harm even if there is no compulsion to answer. (not answering a question might create an impression that they have something to hide)

It has potential for resulting in a distortion (The information is elicited by another)
B) Information Processing

- Refers to use, storage and manipulation of data collected.
- Five forms of information Processing
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion
In 1965, professor Richard Ruggles recommended consolidation of government data system. This idea was supported by bureau of budget. This plan was quickly attacked in Congress and scrapped.

In 1974, the General Services Administration proposed FEDNET, to link all computers maintained by the federal government. Vice President Ford immediately halted the plan.
These data are already recorded in Government systems. Why is it a problem to combine into one gigantic database?

This is problem of “Aggregation”
courts have recognized aggregation as violating a privacy interest.

The rap sheets contained extensive information about individuals compiled from a variety of criminal records.

The Supreme Court concluded that the disclosure of FBI “rap sheets” was an invasion of privacy.

Court observed, there is a “distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole.”
- Creates Architectural and Dignitary harms.
- Dignitary Harms - Aggregation in unanticipated ways may reveal facts about a person that are not readily known
  - Indirect form of data acquisition
- Architectural Problems - it can increase the power that others have over individuals
- They reveal facets of our lives, but the data is often disconnected from the original context in which it was gathered. This leads to distortion.
National Identification Card had been explicitly rejected many times in US.

Social Security card would be kept confidential and would not be used for identification purposes.

In 1973, the influential report, Records, Computers, and the Rights of Citizens, concluded

*We take the position that a standard universal identifier (SUI) should not be established in the United States now or in the foreseeable future. By our definition, the Social Security Number (SSN) cannot fully qualify as an SUI; it only approximates one. However, there is an increasing tendency for the Social Security number to be used as if it were an SUI*

What is the problem with identifying people?
 Identification is used for verifying the identity.

 Identification involves the disclosure of true information.

 Aggregation creates a “digital person,” a portrait composed of information fragments combined together.

 Identification links the digital person directly to a person in real space.
a French citizen who had surgically changed her sex from male to female sought to have her identification documents (birth certificate, identity card, passport, and voting card) changed from listing her former male name to a female one. Since gender was “indicated on all documents using the identification number issued to everyone” and since this “number was used as part of the system of dealings between social security institutions, employers and those insured,” it prevented her from concealing the fact she was a transsexual and effectively assuming a female identity.

The Commission concluded that the applicant, “as a result of the frequent necessity of disclosing information concerning her private life to third parties, suffered distress which was too serious to be justified on the ground of respect for the rights of others.”
Identity Theft – fraud is done using victim’s name. It is made possible because information about us are stored by various companies and institutions.

Identity theft is a subclass of a much bigger issue “Insecurity.”

Insecurity is the problem caused by the way information is handled and protected.
- Threat of disclosure
- Threat of distortion - can result in one’s records being polluted with false data.
- Courts are reluctant to find harm simply from the insecure storage of information.
- Although insecurity increases the possibility of disclosure, courts will often not recognize a harm unless there has been actual disclosure.
Board of Education v. Earls, a school district in Tecumseh, Oklahoma adopted a drug testing policy that required all middle and high school students to undergo drug testing before participating in any extracurricular activity. Some of the students challenged the policy under the Fourth Amendment, but the Supreme Court upheld the testing.

The students contended that the school was careless in protecting the security of the test results. Files were not carefully secured and were left where they could be accessed by unauthorized people, such as other students. The Court dismissed this contention because there were no allegations of any improper disclosures.
“Secondary use” is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject’s consent.

Fair Information Practices states that “[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.”

This is ‘purpose specification principle’
The Privacy Act of 1974
The Fair Credit Reporting Act of 1970
The Driver’s Privacy Protection Act of
The Cable Communications Policy Act of 1984
Gramm-Leach-Bliley Act of 1999
The Video Privacy Protection Act of
The Health Insurance Portability and Accountability Act

What is the concern over secondary uses of information beyond those purposes for which it is collected? Why are there so many legal attempts to limit secondary uses of data?
It creates a dignitary harm, as it involves using information in ways to which a person does not consent and might not find desirable. People cannot control future use of the data they provided.

People might not give out data if they know about a potential secondary use, such as for telemarketing, spam, or other forms of intrusive advertising.

Fear due to Insecurity

Architectural Harms- Information collected in one context is being used in another context.
Fair Information Practices implies the following:
1. The existence of record systems cannot be kept secret.
2. An individual must be able to “find out what information about him is in a record and how it is used.”
3. An individual must be able to “correct or amend a record of identifiable information about him.”

*The failure to provide individuals with notice and input about their records is exclusion.*

- Merely a factor that leads to downstream harms like information dissemination.
- Exclusion creates a sense of vulnerability and uncertainty in individuals.
A broadest grouping of Privacy harm.
Includes revelation of personal data or the threat of spreading information.
What is there to protect us?
Breach of confidence: The revelation of secrets about a person, accompanied by violating the trust in a specific relationship.

Breach of confidence Tort: is a common law that protects private information that is conveyed in confidence.

For example, a doctor and patient or a Banker and customer.
Case 1

Dr. Kent England

Sally McCormas

The husband

Judge

Child/ren
Mrs McCormas sues her doctor for publicizing information that was revealed in confidence by her.

Court reasoned that public disclosure tort focuses on “content” than the “source”. Granted custody to Father.

Here tort of disclosure over-rode the tort of breach of confidentiality. Why?
Case Name: SIMONSEN v. SWENSON

Highlights of the case (1920):
Court Ruling:
“The private privilege ends where the public peril begins.”
Case 3:

- Doctor and the police were charged by the court for not letting the involved party know there was a threat.

- **Highlights of the case:**
2. Disclosure

- The spreading information beyond existing networks of information flow
- Tort to Public Disclosure: a cause of action for one who publicly discloses a private matter that is “highly offensive to a reasonable person” and “is not of legitimate concern to the public.”
- Highlights of the case:
- The website gave bit and pieces of personal information.
- Putting all this together, they should have foreseen, the harm it might cause the subject.
- www.docusearch.com
Hightlights of the case:
- Court ruled that this was not a privacy concern as she herself has revealed her location to a few people.
- So the news would have spread through any of those people or the press.
3. Exposure:

- Exposure involves the exposing to others of certain physical and emotional attributes about a person.
- Difference between Disclosure and Exposure?
- Tort law does not recognize a separate cause of action for exposure.
Highlight of the case:

Court ruled: the picture was not private because “[the student] was voluntarily participating in a spectator sport at a public place.”
Having records of an individual easily accessible.

For eg: Court case records.
5. Blackmail

- involves coercing an individual, by threats to reveal secrets, unless and until the individual pays off a ransom (usually money).
- How is it different from breach of confidentiality, disclosure and exposure?
6. Appropriation

- The use of one’s identity or personality for the purposes and goals of another.
- Case 1: Roberson v. Rochester Folding Box Co.
- Why is wrong?
7. Distortion

- The manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public.
- How is distortion different from disclosure.
Intrusions of privacy

- There are two types of Invasion:
  - Intrusion
  - Decisional interference
- **Intrusion**
  - Intrusion is an unwanted social invasion.

- **Decisional Interference**
  - Applies to incursions on the individual decisions that affect aspects of life that are most private.

  - How does it differ from Intrusion?
Privacy of an individual is important and should be preserved.

When information is in a public domain, individual privacy is not important.

Privacy problems are not caused by technology alone. But also due to activities of people, government and businesses.
What part of the computer seems to be causing the security problem?

The nut at the keyboard!