PERSONAL PRIVACY
AND
COMPUTER TECHNOLOGIES

- what do we mean by ‘privacy
- why do we value our privacy?
- How is our privacy affected by what other people know about
- What kind of information is held about us by different Organizations, government and Private companies?
- who should have the rights to access and use this information?

Digital technology is not necessary for the invasion of privacy; however technology is continually making new threats possible and old threats more potent. Digital technologies—databases, digital cameras, the Web, smartphones, and global positioning system (GPS) devices, among others—have profoundly changed what people can know about us and how they use that information. Understanding the risks and problems is a step towards designing systems with built-in privacy protection and less risk.

Valuing Privacy

The right to privacy is arguably a basic human right – like that of freedom of speech.

It includes the right to;

- Confidentiality (to limit the spread of knowledge about oneself);
- Right to anonymity (to be free from unwanted attention);
- Right to solitude (a lack of physical proximity to others, in other words the right to one's own space).

When we take away someone's privacy, we take away essential elements of their freedom and autonomy as human beings. It has often been said that 'knowledge is power' and, to a large extent, the more someone knows about us, the more vulnerable we are to manipulation and control.

There are three key aspects of privacy:

Can we expect complete privacy? What amount of information can conceal privacy? How much do you want to hide?

1. Freedom from intrusion—being left alone (With friends, family and acquaintances, are you guaranteed of no intrusion?)
2. Control of information about oneself (What do people know about you? Can you control them?
3. Freedom from surveillance (from being followed, tracked, watched, and eavesdropped upon)

Where do you live? Small or big town? What benefits do you need to give up to deal with strangers (landlords, banks etc)?

Privacy threats come in several categories:

1. Intentional, institutional uses of personal information (in the government sector primarily for law enforcement and tax collection, and in the private sector primarily for marketing and decision making)
2. Unauthorized use or release by "insiders," the people who maintain the information
3. Theft of information
4. Inadvertent leakage of information through negligence or carelessness
5. Our own actions (sometimes intentional trade-offs and sometimes when we are unaware of the risks)
6. Add more……

New Technology, New Risks

Computer technology has had a profound impact on what information is collected about us, the quantity of that information, who has access to it, and how it is used. In general terms, information technology has made possible the collection and the exchange of personal data on an unprecedented scale, such that there is now a computerized record concerning practically every aspect of our lives.

Computerized data is easier to collect than paper data. More importantly perhaps, it is easier to collate, manipulate, and analyze. Taken together, computer databases, the Internet and the Web make the collection, searching, analysis, access to, and distribution of, large amounts of information easier, cheaper and faster than before.

Some of this information, such as our specific purchases at supermarkets and bookshops, was simply not recorded before. Our communications by e-mail and discussion groups, and our online activities (where we went, what we did, and how long we stayed on a particular page) can all be recorded, logged, distributed and read by others – even years later.

More Risks with New Technologies

- Photos, videos, documents, and financial statements in a cloud of remote servers
- Internet of Things Technologies
- The wireless appliances we carry enable others to determine our location and track our movements.
- Law enforcement agencies have very sophisticated tools for eavesdropping, surveillance, and collecting and analyzing data about people's activities, tools that can help reduce crime and increase security—or threaten privacy and liberty.
- Technologies in data matching
- Extremely complex softwares that Organizations use are collecting and storing some of these personal information
- Smart apps collecting location and phone ID

A summary of sources of risks

- Anything we do in cyberspace, even briefly, can be recorded and linked to our computer, phone, and possibly our name. This includes use of household Internet-connected appliances.

- With the huge amount of storage space available, companies, organizations, and governments save huge amounts of data that no one would have imagined saving in the recent past.

- People often are not aware of the collection of information about them and their activities.

- Software is extremely complex. Sometimes businesses, organizations, and website managers do not even know what the software they use collects and stores.

- Leaks happen. The existence of the data presents a risk.

A summary of sources of risks

- A collection of many small items of information can give a fairly detailed picture of a person's life.
- Direct association with a person's name is not essential for compromising privacy. Reidentification has become much easier due to the quantity of personal information stored and the power of data search and analysis tools.
- Information on a public website is available to everyone; people other than those for whom it was intended will find it.
- Once information goes on the Internet or into a database, it is almost impossible to remove it from circulation since people and automated software may quickly make and distribute copies.
- It is extremely likely that data collected for one purpose (such as making a phone call or responding to a search query) will find other uses (such as business planning, tracking, marketing, or criminal investigations).
- The government sometimes requests or demands sensitive personal data held by businesses and organizations.
- We often cannot directly protect information about ourselves, so we depend on the businesses and organizations that manage it to protect it from thieves, accidental collection, leaks, and government prying.

What if this data were to find its way into the hands of drugs companies, insurance companies or potential employers? What are the possibilities of such information being misused?

For instance a bank; Once they have health data of you and it does not look good, why should they give you a long term loan?

Internet Technologies and Privacy

Cookies raising concern about possible violations on Privacy

Text files that websites store on the personal hard drive of user's computer; Contains passwords and usernames so that users do not keep retying their credentials in each loading (good eeeeh, be forewarned!)

Cookies can be used for datamining purposes where it tracks user's motions through a website, time spent, what advertising banners one clicked on etc. All these are now used for target marketing.

As the user visits other sites, previously stored cookies are detected, read, and matched with a profile of the user's previous browsing activity. On this basis, an advertising network selects and displays a 'banner ad',(that captures one attention as its info you have searched for before) which is not actually part of the web page the user is viewing, but is instead separately supplied by the advertising network.

Most cookies are read only by the ones who created them but third parties come along and cookie-share (cookie sharing rings) which is then shared with other organizations.
Kind of information gathered include; name, email address, home addresses, mobile phone, transactional data, phrases typed in search engines etc

Contd.....

Spam raising concern about possible violations on Privacy

Unsolicited bulk email consisting of marketing and advertising e-mails junk mail (such as get-rich-quick scams and pornography), chain letters, and occupational spam (inter-office memos and global e-mails within an organization)

Do not open mail purporting to winnings that you did not even participate in

The volume of spam is increasing because companies have found it to be effective as they collect people's emails from websites, newsgroups etc. Its principal advantage is its low cost compared to other forms of advertising. A company can hire an Internet marketing firm to send an advertisement to a million different e-mail addresses. An email advertisement is estimated to be more than 100 times cheaper than a traditional flyer sent via regular post.

Contd…..

Invisible information gathering

- Collection of personal information without the person's knowledge; unfortunately people are not given an opportunity to consent or withhold consent.

Examples:

- *Event data recorders in cars record information, such as driving speed and whether or not the driver is wearing a seatbelt, for use in investigating crashes.*
- *History sniffers are programs that collect information about a person's online activity based on the different colors a browser uses to display sites recently visited.*
- *Spyware that unsuspectedly collect info about a persons' activity and data on his/her device then sends the information over the internet to the person or company that planted the software*

- Have you checked your phones, computers and other devices when connecting to different websites ? Have these sites provided information about their configuration?
- Both collection of configuration information and building of activity profiles are invisible, so we are unlikely to know when someone is using these techniques to build marketing profiles.

Secondary use

- Use of personal information for a purpose other than what it was intended for (for what the person applied for)

  Examples

  - *sale of consumer information to marketers or other businesses,*
  - *use of information in various databases to deny someone a job or to tailor a political pitch,*
  - *use of a person's text messages by police to prosecute that person for a crime,*
- What degree of control should people have over secondary uses of information about them? (Remember Prof David Carroll in The Great Hack Documentary?)
- After informing people about what personal information an organization collects and what it does with that information, the next simplest and most desirable privacy policy is to give people some control over secondary uses.
  - Opt in and Opt out policies
- Responsible, consumer-friendly companies and organizations often set the default so that they do not share personal information and do not send marketing emails unless the person explicitly allows it—that is, they have an opt-in policy.
- On the other hand, many websites inform visitors that using the site is considered to be acceptance of its privacy policy—which most visitors do not read and which may allow tracking and sharing of data about the visitor's activity

Data Mining

- Searching and analyzing masses of data to find patterns and develop new information or knowledge: *Data cost is higher than oil nowadays*
  - *Read: http://www.cs.cmu.edu/~bishan/papers/sigmod09-bishanyang.pdf*

Example

The retail chain had its data miners analyze purchases by women who signed up for baby registries. The retain chain discovered that pregnant women tend to increase their purchases of a group of 25 products. So when a woman began to purchase more of those products (e.g., unscented lotions and mineral supplements), the retain chain sent coupons and ads for pregnancy and baby products—even timing the coupons for stages of the pregnancy.

Matching

Matching means combining and comparing information from different databases often using a unique identifier of an individual to match different records.

Profiling

Analyzing data to determine characteristics of people likely to engage in a certain behavior (Case of Cambridge Analytica on persuadable in a population)

Businesses use these techniques to find likely new customers, and government agencies use them to detect fraud, to enforce other laws, and to find terrorists. Data mining, computer matching, and profiling are, in most cases, examples of secondary use of personal information.

- Some organizations have developed various sets of principles for protection of personal data. These principles cushion users of their sites to secondary use. Fair information principles/practices have been included in data protection laws of various countries
- These principles/practices are reasonable ethical guidelines that include
  - *Inform people when you collect information about them, what you collect, and how you use it.*
  - *Collect only the data needed.*
  - *Offer a way for people to opt out from mailing lists, advertising, and other secondary uses. Offer a way for people to opt out from features and services that expose personal information.*
  - *Keep data only as long as needed.*
  - *Maintain accuracy of data. Where appropriate and reasonable, provide a way for people to access and correct data stored about them.*
  - *Protect security of data (from theft and from accidental leaks). Provide strong protection for sensitive data.*
  - *Develop and publish policies for responding to law enforcement requests for data.*

It can be difficult to apply the fair information principles to new technologies and applications. Example, a tweet, Facebook/Instagram post put up for thousands of people, how do we determine the purpose for which he or she supplied the information? Can any recipient use the information in any way? How widely distributed must information be before it is public in the sense that anyone can see or use it?

Our Social and Personal Activity

- There are two aspects of social networks to consider: our own responsibility for what we share (how we risk our privacy and that of our friends) and the responsibilities of the companies that host our information.

  Example:
  A woman enjoyed the feature on a social network site that told her which members read her profile, but she was surprised and upset to find that people whose profiles she read knew that she read them. This incident illustrates a common phenomenon: people often want information about others, but they do not want others to have access to the same kinds of information about themselves.

- This incident shows us that some people do not know or understand or think enough about information sharing policies to make good decisions about what to do in cyberspace
- What are you posting online? Is it too much information to potential stalkers, a future job hunt, etc?

Polls show that people care about privacy. Why don't they act that way?

#Ian Kerr

What do Organizations do with our data on social media?

Following The Great Hack documentary, would you list how social data has been exploited?

1.
2.
3.
4.
5.
6.
……