Privacy

Dr. Hassan Abdalla

College of Computer and Information Sciences
King Saud University,

The Questions

- What information should one be required to disclose about one's self to others? Under what conditions?
- What information should one be able to keep strictly to one's self?
- These are among the questions that a concern for privacy raises today more than ever before.
- Cautious citizens must be asking these questions.

What is Personal Privacy

- Privacy is a concept that is neither clearly understood nor easily defined.
- Sometimes we speak of one's privacy as something that has been:
  - "lost,"
  - "diminished,"
  - "intruded upon,"
  - "invaded,"
  - "violated,"
  - "breached," and so forth.

Two Scenarios

- Scenario 1: Someone walks into the computer lab and sees you using a computer.
  - Your privacy is lost but not violated.

- Scenario 2: Someone peeps through the keyhole of your apartment door and sees you using a computer.
  - Your privacy is not only lost but is violated.

The right of privacy

- Privacy is human value consisting of four rights:
  - Solitude: the right to be alone without disturbances
  - Anonymity: the right to have no personal identity in public
  - Intimacy: the right to do something privately
  - Reserve: the right to control personal info about oneself
- The problem of piracy involves the following areas:
  - Territorial Privacy: limiting intrusion into domestic envts
  - Location Privacy: managing geolocation technologies (GPS)
  - Bodily Privacy: respecting the integrity of individual's body
  - Personal Privacy: protection against undue interferences
  - Communication Privacy: privacy of emails, voice telecom
  - Information Privacy: concerned with the collection and compilation of personal info like credit card & medical info

Three Theories of Privacy

Accessibility Privacy	Privacy is defined in terms of one's physically "being let alone," or freedom from intrusion into one's physical space.
Decisional Privacy	Privacy is defined in terms of freedom from interference in one's choices and decisions.
Informational Privacy	Privacy is defined as control over the flow of one's personal information, including the transfer and exchange of that information.

Two Forces Threaten Our Privacy

1. The growth of information technology (IT), with its enhanced capacity for observation, communication, computation, storage, and retrieval.
2. The increased value of information in decision making.
   - Information is increasingly valuable to policy makers; they want it even if acquiring it invades other's privacy.

Methods of privacy violation

Intrusion & misuse of information	Wrongful entry or acquiring of other's info for illegal use & unauthorized purposes
- Interception of info - Cookies	unauthorized access by a third party to a private communication. Cookies are files that Web sites send to and retrieve from the computer systems of Web users.
Data Merging	A data-exchanging process in which personal data from two or more sources is combined to create an image of an individual that would not be possible if the pieces of data was scattered.
Data Matching	A technique in which two or more unrelated pieces of personal information are cross-referenced and compared to generate a match or "hit," that suggests a person's connection with a specific group.
Data Mining	Compiling of masses of data into one or more databases to extract new information or knowledge that were previously hidden (KDD).

Surveillance technologies

- Database Surveillance: Blacklist databases & data theft
- Internet Surveillance: Tracking users' info through cookies
- Video Surveillance: CCTV cameras to discourage criminals
- Satellite Surveillance: GPS take images of our personal lives
- Mobile Surveillance: 4G mobiles with video camera & internet
- ID Cards Surveillance: ID cards include microchips with personal & biometric info of user's authentication

Information Gathering

- Computers make it possible to gather detailed information about individuals to an extent never possible before
- Government agencies now maintain extensive records of individual behavior
- When individuals believe they are being watched, they are compelled to behave differently than they might if they weren't being observed.
- Record-keeping is far from a new phenomenon

Information Gathering – cont.

- Computer technology has changed record-keeping activities in a number of undeniable and powerful ways:
  - First, the amount of information gathering has changed.
  - Second, the kind of information that can be gathered has changed.
  - Third, the speed of exchange of information has changed enormously
  - Forth, the duration of time in which the information can be retained

Information Gathering – cont.

- Technology no longer limits what can be done
- Now only time and money and perhaps, human capabilities impose limits on the quantity of information that can be gathered and processed.
- The kind of information that is now possible to collect and use is also novel to researchers
- One particularly important new form of information is referred to as transaction generated information (TGI)

TRANSACTION GENERATED INFORMATION (TGI)

- TGI seems to be fragmented and, therefore, seems not to pose the threat of Big Brother
- As far as the technology goes, the distribution of information can take place with or without the knowledge of the person whom the information is about
- It can take place intentionally as well as unintentionally
- When computers are connected via telecommunications lines, the possibilities of data being tampered with or stolen are increased

Accuracy

- Misinformation has a way of messing up people's lives, especially when the party with the inaccurate information has an advantage in power and authority.
- Consider the difficulty of John A. Smith's

Record-Keeping

- In summary, while record-keeping is, by no means, a new-activity, it appears that computer and information technology has changed record-keeping activities in the following ways:
  - (1) it has made a new scale of info gathering possible
  - (2) it has made new kinds of information possible, especially transaction generated information;
  - (3) it has made a new scale of information distribution and exchange possible
  - (4) the effect of erroneous information can be magnified
  - (5) information about events in one's life may endure much longer than ever before
- These five changes make the case for the claim that the world we live in is more like a panopticon than ever before.

Is it computers problem?

- You may be tempted to say that computers are not really the problem or the cause of the problem.
- It is individuals and organizations that are creating, gathering, exchanging, and using information.
- Computers, according to this argument are simply tools.
- If someone to be blamed, it is the people who use computers, not the computers themselves.

THE BALANCING SCALES

- Personal privacy is generally put on the other side of the balancing scales.
- The issue is framed so that we have to balance all the good things that are achieved through information gathering and exchange against the desire or need for personal privacy.
- From a legal and constitutional point of view, we have, at most, a limited and complex right to privacy.

Possible Counterarguments

The case for privacy seems powerful and suggests that there are serious dangers with the amount and kind of data gathering that now goes on.

However, some people may still not be convinced that there is much of a problem based on the following arguments:

1. That the situation is not so bad. Individuals who have done nothing wrong, have nothing to fear. This argument might even go as far to say that privacy only protects people who have something to hide.
   - Unfortunately, this argument does not work because erroneous information can dramatically affect your life (e.g. stolen car case).

Possible Counterarguments– cont.

2. Individuals in our society do have some power to control their relationships with private and public organizations. Many have simply opted to give up their privacy. They could refuse to give out information about themselves.
   - This argument contains a little of truth, but hides a much more complicated situation.
   - Yes, I can choose not to do any thing that might disclose my privacy e.g. not to buy using credit card so that there is no information gathered about my buying activities
   - However, I will have to give up a great deal; I have to pay a high price for my privacy.

Possible Counterarguments– cont.

3. Finally, someone might still insist that we have nothing to worry about because we are protected by a wide array of legislation against abuses of information.

   Moreover, you could argue that we have voluntarily given up our privacy by supporting legislators who believe we prefer less privacy to better law enforcement and more efficient organizations.

   - This argument raises the question of whether the legislation system we have today is good enough.

Protecting privacy

- With regard to the storage of personal data, individuals should be aware of the following questions:

1. Collection of data: who collects the data and using which methods
2. Integrity of data: is the storage of data accurate and verified? How regularly updated and checked?
3. Access of data: can individuals access, change or correct their personal data?
4. Protection of data: are data secured from unauthorized access and use? And how reliable the security procedures are?

Role of Computer Professionals

- Computer professionals can play an important role, individually and collectively.
- First and foremost, individual professionals must not wash their hands off privacy issues.
- A computer professional can point out privacy matters to clients or employers when building databases containing sensitive information.

Role of Computer Professionals – cont.

- The original ACM Code of Professional Conduct (passed by the ACM Council in 1973) specified that: An ACM member, whenever dealing with data concerning individuals shall always consider the principle of the individuals‘ privacy and seek the following:
  - To minimize the data collected.
  - To limit authorized access to the data.
  - To provide proper security for the data.
  - To determine the required retention period of the data.
  - To ensure proper disposal of the data.

Role of Computer Professionals – cont.

- The Guidelines ACM Code of Ethics explain that: "It is the responsibility of the professionals to maintain the privacy and integrity of data describing individuals".
- This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals.