Advances in Imformation Technology and its Implications on Privacy

Ismail A. Hassan

Abstract

Over the past three decades, computers and information technology in general have experienced an enormous growth and development. This amazing new technology is profoundly affecting and changing the functioning of societies worldwide. The issue of personal privacy and what is perceived to be an increasing invasion of it by advances in technologies have raised the publics concerns. Most individuals regard privacy as a basic right, but the problem is that people have different interpretations and thresholds on what they regard as private, and when/where that privacy is jeopardized or invaded. In this paper we will highlight existing and emerging technologies and their potential implication on privacy.

"The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding"

Olmstead vs. United States, 1928, Justice Lewis Brandies

1 Introduction

Over the past three decades, the technology of computers and communications systems has developed so rapidly that it has become difficult to foresee the associated social impact it will have on our lives [24]. This amazing new technology is profoundly affecting and changing the functioning of societies worldwide. The issue of personal privacy and what is perceived to be an increasing invasion of it by advances in technologies have raised the publics concerns. Most individuals regard privacy as a basic right, but the problem is that people have different interpretations and thresholds on what they regard as private, and when/where that privacy is jeopardized or invaded.

Privacy entails an individual's right to control the collection and use of his or her personal information, even after that information is disclosed to others with the consent of that individual. When information is disclosed to a doctor, a merchant, or a bank, one expects that those professionals or companies will collect the information they need to deliver a service and use it for that sole purpose. In the event that the information is to be used for other purposes, individual expect to be informed about it, and the right to object to its further use.

While privacy was also a problem in manual systems, modern computer-communication technology makes it economical to store and process large volumes of data, permits complex correlations at high speed, allows rapid access from distant locations and, thus, makes technically feasible for physically decentralized systems to become centralized logically [11, 28].

Vast amounts of personal information are routinely collected overtly and covertly by government agencies, corporate firms and private individuals. The more one ventures into the public realm and pursues interests with others, the more one inevitably risks privacy invasions [27]. In this paper we will highlight some of the existing and emerging technologies and their implication on privacy.

2 Existing technologies

Surveillance cameras

Surveillance cameras are setup in peculiar places and are often illusive in the sense that individuals don't realize that they are being filmed. For the most part these cameras are setup with good intensions namely for the benefit of public safety. They can be a vital tool in preventing or solving crimes. The problem is not that the individual is being filmed, but usually this is done without his or her consent. Often the legitimacy and purpose of these cameras cannot be verified thereby not knowing whether they are complying with the rules and regulation or plain simply spying on us. The Norwegian Data protection agency (Datatilsynet) has in their 2003 annual report unveiled several cases where surveillance cameras have been misused or setup without permission. Other data protecting agencies around the world report a similar frustration regarding unlawful use of these devices.

In an effort to fight terrorism the United States government has come up with several mechanisms such as the Government Surveillance via Passenger Profiling (CAPPS II) program. This is a controversial passenger profiling and surveillance system that would require passengers to give their birth date, home phone number, and home address before boarding a U.S. flight. Under CAPPS II, travel authorities would check these and other personal details against the information collected in government and commercial databases, then "tag" the passenger with a color-coded score indicating the level of security risk that the individual appear to pose. Each airline passenger will be classified with a color code such as a green, yellow or red risk level. Passengers classified as green will be subject to only normal checks, while yellow will get extra screening and red won't fly [6]. We do not have any guarantees that pictures taken from a peaceful demonstration against U.S war on Iraq for example will not be processed through face recognition equipment and correlated with other databases, thus tagging those individuals with yellow or red. Knowing that data gathered through surveillance could be used in other circumstances however innocent that data is, could have a profound affect on how we behave or express our opinions under the glazing eyes of the cameras.

Credit cards

The preferred means of payment these days in many industrialized countries are credit cards, and one might ask how widespread is their use? The Central Bank of Norway's annual report on payment system for 2002 shows that total Purchase of goods and services with the use of Norwegian payment cards in 1993 was 118.8 million transactions amounting to 57.8 billion NOK. In 2002 this figure rose to 516.5 transactions and an outstanding 201.9 billion NOK [3]. A similar trend is shown on almost all of the industrialized countries annual statistical reports. When we contemplate all the electronic data that is now gathered about each of us as we move through our everyday lives, there seems little doubt that we are leaving behind an electronic record of our activities. Every time we use a payment card at a grocery store, restaurant, bar, bookstore and any other purchases we make, our names are correlated with our purchases and entered into giant databases.

The Internet

The Internet has enriched people with information and given them the opportunity to do business and shopping online. It offers a variety of services that are in most cases essential to individuals, and the ease at which those services are offered makes it convenient for many to use the internet. Connectivity and usage has exploded within the last decade. The Norwegian statistical gathering agency SSB, has in their 2002 yearbook indicated that the number of Internet subscribers increased from 381 342 in 1998 to 1 235 596 in 2001. Different governmental statistical bureaus around the world also report a huge increase in the number of people that are online. Concerns over consumers privacy has been raised by many since Internet Service Providers (ISPs) and Web sites now collect and sell data about on-line users at unparalleled rates [28]. There are a multitude of data-gathering tools available for everyone, and these are being used to monitor the activities of unsuspecting Internet users. What's alarming is that often these tools covertly collect the information without the user's knowledge.

Mobile phones

Subscriptions to mobile phones have also enjoyed a tremendous increase over the last 10 years. Out of a population of 4 million in Norway, there were 3 911 011 mobile subscribers in 2002 compared to 371 403 in 1993[3]. This is not unique for Norway, but rather a worldwide phenomenon.

One of the latest services offered by mobile phones is Location Based Services (LBS), which in its basic form will give individuals information about their location. Examples of such services are Friend-finder and Buddy which are currently offered by network operators Telia in Sweden and Netcom in Norway. People who signup for this service have the opportunity of locating their friends or loved ones as long as they are registered in their list. Location Based Services doesn't only give away the location of individuals, but gives a pattern on what services individuals are interested in. The ability to gather and pass on personal information about consumers has been a key selling point for interactive media. Marketers have been told they will be able to gain access to everything from what movie preferences a household has, to what it had for dinner last night. With that data, they plan to send marketing messages based on personal likes and dislikes [19]. This increases the quantity and value of personal information in the marketplace thus creating a conflict between those who feel they have a right to profit from such information and those who feel they have a right to privacy [28].

Toll Booths

Many cities around the world use Toll Booths to combat increasing traffic or simply collect more money for the authorities. Most of them are adapting a system that automates the passing through of cars by using a billing system which binds the vehicles identity to the owner, an example of this is the AutoPass system in Norway, EZPass system of United States east coast and Highway 407 in Canada. Fjellinjen AS which is the company responsible for operating the tollbooths around Oslo Norway, has an annual report that gives a clear picture of the number of people that choose to use AutoPass which is a small device mounted on the dashboard of the vehicle. This device which can be acquired through a subscription lets the driver pass automatically. The company had 75% of its traffic from subscribers while 10% used coins and 15% paid manually [2]. While these types of systems are beneficial in many circumstances, privacy could be jeopardized since they easily can facilitate the location of individuals [18].

3 Emerging Technologies

Radio Frequency IDentification (RFID)

RFID is an item-tagging technology which is already in use in the supply chain to track assets like containers and trailers. RFID tags are tiny computer chips connected to miniature antennae that can be affixed to physical objects. In the most commonly touted applications of RFID, the microchip contains an Electronic Product Code (EPC) with sufficient capacity to provide unique identifiers for all items produced worldwide. These tags are so small, which makes them ideal to place them into clothing, purses, shopping bags, suitcases, and more. The Electronic Product Code potentially enables every object on earth to have its own unique ID that can be linked to its purchaser or owner at the point of sale or transfer. The tags can be read from a distance, and are not restricted to line of sight. While there are beneficial uses of RFID, it could be deployed in way that threatens individual's privacy [20]. RFID tags can be embedded into or onto objects and documents without the knowledge of the individual who obtains those items. In their 2003 annual report The Norwegian Data protection agency (Datatilsynet) has raised concerns on RFID [8].

Biometrics

The identification or verification of someone's identity on the basis of physiological or behavioral characteristics is what biometrics is all about. It involves comparing a previously captured unique characteristic of a person to a new sample provided by the person. This information is used to authenticate or verify that a person is who they say they are by comparing the previously stored characteristic to the fresh characteristic provided [22].

After 9/11 the United States has put a lot of emphasis on the use of biometrics and started using the technology for either authentication purposes or just storing it on a database for later use. Citizens of many countries enjoy the benefits of the Visa Waiver Program (VWP) which entitles them the right to enter the US without the requirement of a visa, but as of 26/10/2004 they are required to posses a passport with biometric features in order to retain that right. To meet these requirements, the European Commission adopted on 18/02/2004 a proposal for a Regulation on standards for security features and biometrics in EU citizens' passports [9]. Biometric identifiers are biological in origin; this creates opportunities for collectors of such data who might glean additional (possibly statistical) personal information from scanned biometric measurements. For instance, certain malformed fingers might be statistically correlated with certain genetic disorders. With the rapid advances in human genome research, fear of inferring further information from biological measurements might also be on the rise. Such derived medical information could become a basis for systematic discrimination against segments of the population perceived as "risky" [15]. Biometric characteristics are not secrets. It is often possible to obtain a biometric sample, such as a person's face, without that person's knowledge. This permits covert recognition of previously enrolled people. Consequently, those who desire to remain anonymous in any particular situation could be denied their privacy by biometric recognition [15].

Pervasive computing

Ubiquitous computing or Pervasive computingis is an area that has experienced an intensive research lately. The idea was first conceived by Mark Weiser and his colleagues at Xerox Park Alto Research center where they envisioned a world with specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence [16]. The term pervasive computing signifies computers and sensors "everywhere" in devices, appliances, equipment, in homes, workplaces and factories, and in clothing. Devices and sensors may be mobile, such as wireless PDAs or smart phones, or may be embedded in the environment, such as sensors and computer chips in walls or furniture.

Add reliable wireless communications and sensing functions to the billions of physically embedded computing devices around the world for a new universe of ubiquitous networked computing. Some of these technologies are, unbeknownst to us, already ubiquitous in our lives; an astounding 98% of all processors on the planet are not in traditional desktop computer systems but in house- hold appliances, vehicles, and machines on factory floors [13].

The technology is at its infancy and if not designed with privacy in mind, it could have a profound implication on personal freedom. We are pushing toward making it easier for computation to sense, understand, and react to phenomenon in the physical world and to record those phenomena. These enabling technologies carry with them numerous dangers, e.g., making it too easy for people to build systems that effectively spies on others without any controlling authority [7].

Brain fingerprinting

Brain fingerprinting was developed and patented in 1995 by Lawrence A. Farwell, Ph.D., chairman of the Brain Wave Institute in Fairfield, Iowa, and former Harvard University research associate. Brain fingerprinting is based on the theory that throughout a crime, the brain plans, records, and executes all of the criminal's actions. Such details, all concealed within the brain, can now be revealed through brain fingerprinting. This technique measures how brain waves respond to crime-specific words or pictures flashed across a screen. Pictures, both relevant and irrelevant to the crime, are shown. The relevant images should trigger memories of the crime in guilty suspects [26].

Existing methods such as polygraphs rely on measurement of heart rate and palm sweating. Brain Fingerprinting on the other hand measures electrical brain activity. The procedure is said to be more accurate in detecting "guilty" knowledge distinct from the false positives of traditional polygraph methods, but since the technology is at its infancy much work remain to be done in order to verify this assumption.

Die Gedanken sind frei
My thoughts freely flower,
Die Gedanken sind frei
My thoughts give me power.
No scholar can map them,
No hunter can trap them,
No man can deny:
Die Gedanken sind frei!

I think as I please
And this gives me pleasure,
My conscience decrees,
This right I must treasure;
My thoughts will not cater
To duke or dictator,
No man can deny–
Die Gedanken sind frei!

And if tyrants take me
And throw me in prison
My thoughts will burst free,
Like blossoms in season.
Foundations will crumble,
The structure will tumble,
And free men will cry:
Die Gedanken sind frei!

This is part of an old German poem which has its origins from the 12th century by the lyric poet Dietmar von Aistwhich. The poem praises the freedom of thought, and how it can't be taken away from us. Recent advances in technology such us Brain Fingerprinting threaten this very notion of having free thought. While brain fingerprinting is still in its infancy, the potential for exploitation in a number of governmental and civil contexts makes this new technology of important consequence for anyone concerned with the protection of personal, autonomous thought [29].

History has shown that governments do not need high-tech equipment to conduct surveillance of citizens. However, technology has provided new surveillance tools and facilitated surveillance of a magnitude that could only be dreamed of in the past [4].

Deborah Johnson, professor of applied ethics at the University of Virginia said: *"We are building the infrastructure for a totalitarian control and once its setup in place; it will only take a slight shift in political ideology to be used in other ways"*. Countries such as U.S and many European countries have passed laws which take advantage of this infrastructure of totalitarian control on the grounds of fighting terrorism in the aftermath of 9/11.

4 Conclusion

Through the history of mankind, people have been worried about what implications new technologies would have on their lives, and those mentioned in this paper are no exceptions. The aim here is not to list all the existing or emerging technologies that have some sort of implication on privacy, but rather highlight some of them thereby indicating their flaws towards privacy and the potential misuse of that flaw. In some situations users can take some precautions and protect themselves from privacy breaches, while in other situation users do not have that luxury and have to hand over personal information.

Doctors have to get access to patient's health records, tax authorities require citizen's to disclose all sorts of information about their finances and the banks have to know about a customer's credit history to see if the individual is eligible for loan. Like cigarette smokers that get all kinds of warnings about the danger of smoking, yet continue to smoke, some users will knowingly jeopardize their privacy and wouldn't care about the consequences of their actions. The issue of privacy cannot be settled by a single entity, but demands the cooperation of all parties involved in order to succeed.

References

[1] Stone Adam. The dark side of pervasive computing. *IEEE Pervasive Computing*, vol. 2:pp. 4–8, Jan.-March 2003.

[2] Fjellinjen AS. http://www.fjellinjen.no/Dokumenter/Fjellinjen_aarsrapport_2003.pdf.

[3] Norges Bank. http://www.norges-bank.no/english/publications/annual_report/.

[4] Simons Barbara. Building big brother. *COMMUNICATIONS OF THE ACM*, vol. 43:pp. 31–32, 2000.

[5] Statistics Norway 2003 Year Book. http://www.ssb.no/english/yearbook/tab/t-070110-271.html.

[6] Kantarcioug Murat; Cliff Chris. Assuring privacy when big brother is watching. In *DMKD03:8th ACM SIGMO Workshop*, June 2003.

[7] Abowd Gregory D.;Mynatt Elizabeth D. Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction*, vol. 7:pp. 29–58, March 2000.

[8] Datatilsynet. http://www.datatilsynet.no/arkiv/andreforsideoppslag/v2004/pvrapp04.pd

[9] eGoverment News. http://europa.eu.int/ida/en/document/1915/544.

[10] Estrin Deborah; Culler David; Pister Kris; Sukhatme Gaurav. Connecting the physical world with pervasive networks. *IEEE Pervasive Computing*, vol. 1:pp. 59–69, Jan.-March 2002.

[11] Moor James H. Towards a theory of privacy in the infromation age. *ACM SIGCAS Computers and Society*, vol. 27:pp. 27–32, Sept. 1997.

[12] Want Roy; Pering Trevor; Borriello Gaetano; Farkas Keith I. Disappearing hardware. *IEEE Pervasive Computing*, vol. 1:pp. 36–47, Jan.-March 2002.

[13] Estrin Deborah; Govindan R.; Heidemann J. Embedding the internet. *Communications of the ACM*, vol. 43:pp. 38–41, May 2000.

[14] Stanley Jay. Bigger monster, weaker chains: The growth of an american surveillance society. http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39. The American Civil Liberties Union.

[15] Prabhakr Salil; Pankanti Sharath; Jain Anil K. Biometrics recognition: Security and privacy concerns. *IEEE Security & Privacy*, vol. 1:pp. 33–42, March-April. 2003.

[16] Weiser Mark. The computer for the 21st century. *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 3:pp. 3–11, July 1999.

[17] Caloyannides Michael. Online monitoring: Security or social control. *IEEE Security & Privacy*, vol. 2:pp. 81–83, Jan.-Feb. 2004.

[18] Caloyannides Michael. The cost of convenience:a faustian deal. *IEEE Security & Privacy*, vol. 2:pp. 84–87, March-April. 2004.

[19] Guynes Carl S.; Vedder Grichard G.; Vanecek Michael. Privacy and security. *ACM SIGCAS Computers and Society*, vol. 26:pp. 11–13, March 1996.

[20] Juels Ari; Rivest Ronald L.;Szydlo Michael. The blocker tag: Selective blocking of rfid tags for consumer privacy. In *Proceedings of the 10th ACM conference on Computer and communication security*, October 2003.

[21] Dern Daniel P. Privacy concerns. *IEEE Security & Privacy*, vol. 1:pp. 18–23, March-April 2003.

[22] Privacy and Human Rights. http://www.privacyinternational.org/survey/phr2003/.

[23] Beckwith Richard. Designing for ubiquity: The perception of privacy. *IEEE Pervasive Computing*, vol. 2:pp. 40–46, April-June 2003.

[24] Rosenberg Richard S. Yesterday, today, and tomorrow. *ACM SIGCAS Computers and Society*, vol. 29:pp. 10–11, Sept. 1999.

[25] Tavani Herman T. Privacy online. *ACM SIGCAS Computers and Society*, vol. 29:pp. 11–19, Dec. 2003.

[26] Abdollah Tami. Brain fingerprinting picture-perfect crimes. *Berkeley Medical Journal Issues 2003*, Spring 2003.

[27] Gregory J. Walters. Privacy and security: An ethical analysis. *ACM SIGCAS Computers and Society*, vol. 31:pp. 8–22, june 2000.

[28] Marie A. Wright and John S. Kakalik. The erosion of privacy. *ACM SIGCAS Computers and Society*, vol. 27:pp. 22–25, Dec. 1997.

[29] Sententia Wrye. Brain fingerprinting: Databodies to databrains. *The Journal of Cognitive Liberties*, vol. 2:pp. 31–46, 2002.