



Romel Cabiling ▾



Home

Home > My courses > Social And Professional Issues > 11 Personal Privacy And Computer Technologies > Lesson Proper for Week 11

Lesson Proper for Week 11

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); the right to anonymity (to be free from unwanted attention); and the 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. One of the main contemporary privacy issues is the disclosure and use of our personal information. Personal information includes any information relating to, or traceable to, an individual person. Personal information includes information which identifies us (our name, address and age) and information which says something about us and our lifestyles (for example, our interests and shopping habits). Personal information can be defined by contrasting it with public information – however, the boundaries between the two are increasingly blurred. Public information is information that someone has provided to an organization that has the right to share it with other organizations. An example of public information is a listing in a telephone directory. Most of us allow our name, address, and phone number to appear in telephone directories. Personal information is information that is not public, nor part of a public record. You may rightly consider your religion to be personal information. It remains personal information as long as you never disclose it to an organization that has the right to share it. However, if you do disclose your religious affiliation to such an organization, it then becomes public information.

In the UK, the office of the Information Commissioner has been established to protect personal information. Their mission is stated as:



We shall develop respect for the private lives of individuals and encourage the openness and accountability of public authorities:

- By promoting good information handling practice and enforcing data protection and freedom of information legislation
- By seeking to influence national and international thinking on privacy on information access issues.

The Impact of Computer Technology

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.

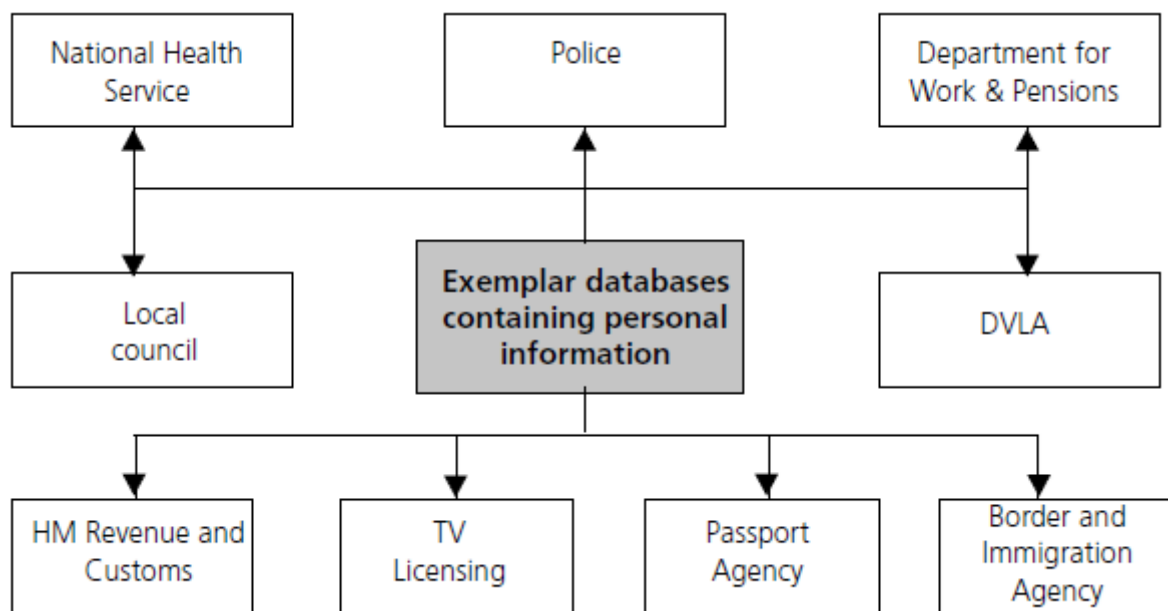


Figure 6.1: Examples of UK government departments that employ databases storing personal information in relation to UK citizens

Today there are thousands of databases, both government and private, containing personal information about us. For example, in the UK, records for most citizens will exist in many of the following government or local state databases: the National Health Service, the local council, the Inland Revenue, the Passport Office, Immigration, the



Driver and Vehicle Licensing Agency, the Department of Social Security, the TV Licensing Office and the Police. See Figure 6.1.

Some of the most extensive databases of personal information, however, are held by private corporations, such as credit-checking companies. One of the world's biggest credit-checking companies is Experian. Experian has detailed records of over 40 million people in the UK and carries out checks for the police, various government departments, private companies and other organizations. The kinds of personal information held by credit-checking companies will include names and addresses, former addresses, and current credit ratings, among many other items of information. The information in these databases has invariably been collected from a wide range of sources, and organized so that it constitutes a history, and an assessment, of our trustworthiness as debtors.

Supermarkets are now also compiling vast databases of information about their customers. They do this through their loyalty cards, in conjunction with records of credit card transactions at their stores. British supermarket chain Tesco, for example, has over 10 million names on its Clubcard database. Information in these databases is used to analyze the shopping patterns of customers and to target them with specific advertising based on their demographic profile and spending patterns.

The foregoing are all examples of the secondary use of personal information, that is, the use of information for a purpose other than the one for which it was supplied. It is difficult for individuals to control their personal information if it is collected by one business, organization or government agency and shared with or sold to others. This information is gathered from a number of different sources, from product guarantee cards, customer details recorded when purchasing a product, and increasingly through online transactions. A number of private companies now exist with the sole purpose of buying and selling databases of personal information. In 2003 the list industry in the UK was valued at £2bn. These databases are sold particularly to marketing companies and used in profiling, where the data in computer files is used to determine characteristics of people most likely to engage in certain behavior. Businesses use profiling to find people who are likely customers for particular products and services.

Another trend in the use of personal information is that of data matching. Data matching involves combining and comparing information from different databases. Personal information that is supplied or collected for one purpose, and stored in a particular database, is cross referenced to information in other databases, where data may have been gathered for an entirely different purpose. An individual's details can thus be searched across a number of different databases, enabling a fairly detailed picture to be built up about that person. This is a trend that has concerned privacy advocates and civil liberties groups, because of the potential misuses of such information. Health data, for example, in the form of people's medical records, constitutes highly sensitive information. What if this data were to find its way into the hands of drugs companies, insurance companies or potential employers? The possibilities for abuse of such information are endless – vetting people for jobs, or denying someone a bank loan, based on their current health, their propensity to certain health conditions, or their family medical history.

Internet Technologies and Privacy

In this section, we briefly consider the following concepts:

- **Cookies**



- **Spam**
- **Encryption**
- **Radio frequency identification (RFID)**

Cookies

Cookies are text files that websites store on the hard drive of the user's computer. They may store passwords and user names, so that the user does not have to keep retyping them every time they revisit the site that issued the cookie. However, the function of some cookies may not be readily apparent, especially those which redirect the user to sites other than the one they are trying to visit, or which reside permanently on the user's hard disk.

Cookies can be used for 'data mining' purposes, to track the user's motions through a website, the time they spend there, what links or advertising banners they click on and other details that the company wants to record, usually for marketing purposes. 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', a rectangular advertisement which is not actually part of the web page the user is viewing, but is instead separately supplied by the advertising network.

Most cookies can be read only by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie-sharing rings. The information that they collect about different users is shared with all of their client websites (who may number in the hundreds, or even thousands). The kind of information that is transmitted to these client sites or companies might include someone's name, their e-mail addresses, their home address and telephone phone number, and transactional data – for example, the names of products they purchased online, details of plane trip reservations and phrases typed into search engines.

The use of cookies to gather data and track a user's online activities has raised a number of concerns about possible violations of privacy. Chief among these is the fact that data collected about Internet users can be recorded and shared with third-party companies for marketing purposes, without knowledge or consent.

Spam

Spam is unsolicited bulk e-mail 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). The term 'spam' can be traced back to a *Monty Python* sketch, in which a group of Vikings drown out a cafe conversation by loudly and continuously chanting the word 'spam'!

Dealing with spam has become one of the Internet's biggest problems. As recently as 2001, spam accounted for only about eight per cent of all e-mail. By 2003, about 40 per cent of all e-mails were spam (Quinn, [2004]). Spam consumes a large percentage of the Internet's bandwidth and huge amounts of storage space on mail servers and individual computers. The fact that most spam is unsolicited (that is unwanted or unasked for), and that it clogs up the inbox of a user's e-mail program has led to it being seen as an intrusive invasion of privacy.



The volume of spam is increasing because companies have found it to be effective. 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.

Direct marketing firms build up e-mail lists with millions of addresses. They do this using 'robot' software that collects e-mail addresses from websites, message boards and newsgroups. One way that spammers collect e-mail addresses is through 'dictionary attacks'. The term comes from programs that try to guess passwords by trying every entry in an online dictionary of e-mail addresses. Spammers bombard Internet service providers (ISPs) with millions of e-mails sent to made-up or guessed e-mail addresses.

Most of these e-mails will bounce back, because the addresses are not valid. However, if an e-mail does not bounce, the spammer knows there is a user with that e-mail address and adds it to their mailing list. To keep networks from being flooded with spam, ISPs have installed spam filters to block spam from reaching users' mailboxes. These filters look for a large number of messages coming from the same e-mail address, messages with suspicious subject lines, or messages with spam like content. However, spammers are changing their tactics to confound the efforts of spam blockers, by changing e-mail and IP addresses to disguise the sending machine.

Another way spammers can obtain e-mail addresses is through opt-in lists. In order to make a purchase online, very often the user has to agree to the terms and conditions of the vendor, which include agreeing to be sent promotional e-mails, both from the company and their 'marketing partners'. This is known as 'opting in' on the part of the consumer.

By law, customers should be given a choice about whether data collected about them is distributed to other businesses or organizations and is used to send advertisements. The two most common ways of providing such choices are called opt out and opt in. Under an opt-out policy, one must check a box on a contract, membership form, or agreement, or call or write to the organization to request removal from distribution lists. If the consumer does not take action, the presumption is that his or her information may be used. Under an opt-in policy, personal information is not distributed to other businesses or organizations unless the consumer has explicitly checked a box or signed a form permitting disclosure.

The UK follows the 'opt-in' scheme, under the provisions of The Privacy and Electronic Communications (EC Directive) Regulations, 2003. In essence it states:

- Senders cannot send marketing messages unless they have the recipient's prior consent unless the recipient's e-mail address was collected in the course of a sale, or negotiations for a sale
- The sender sends only mail related to similar services or products
- And when the address was collected, the recipient was given the opportunity to opt out, which they did not take.

It also provides two new rules for e-mail marketing:

- The sender must not conceal their identity



- The sender must provide a valid address for opt-out requests.

The sending of unsolicited marketing material also applies to the mobile phone industry; since 11 December 2003 it has been unlawful to send an unsolicited SMS marketing message to an individual.

Complaints regarding the receipt of such messages can be made via the Office of the Information Commissioner at their website (www.informationcommissioner.gov.uk). This website gives advice on what to do if the message contains a premium rate number, and links to the Telephone Preference Service where individuals or businesses can register to 'opt out' (www.tpsonline.org.uk).

Encryption

Encryption concerns the conversion of data into a form that cannot be understood without the correct decryption 'key'. We saw that encryption/ decryption is especially important in any kind of confidential communication or sensitive transaction, such as a credit card purchase online, or the discussion of company secrets inside an organization. Encryption is thus one way to ensure privacy in communication. Relatively easy to use e-mail and file encryption software is available, such as Pretty Good Privacy (PGP) which runs on almost all computers and integrates with most major e-mail software. PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations.

Access to, and control of, encryption technology touches on a number of privacy issues. We saw in the previous chapter how the potential intrusiveness of the clipper chip raised fears about unwarranted invasions of individual privacy by the US government. In its efforts to balance national security needs with privacy rights, this technology put too much emphasis on national security by creating a system in which the risks to privacy invasions were unacceptable, and unnecessarily high. As a result of this overwhelming criticism and negative publicity, the original clipper chip proposal was soon defunct.

Controversy has continued over so-called 'strong encryption'. This refers to ciphers that are essentially unbreakable without the correct decryption keys. Some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including the US, want to set up a key escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if supported by a court order.

Opponents of this scheme argue that criminals could hack into the key escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption. The use of encryption, and the control of encryption technologies, continues to be a highly controversial issue in the wake of the terrorist attacks on the US in September, 2001. (See Section 6.4: Privacy legislation – The Regulation of Investigatory Powers Act, 2000, and The USA Patriot Act, 2001.)



RFID

RFID (radio frequency identification) is a wireless transmitter technology. RFID tags are tiny microchips attached to an antenna that receive and transmit location information by means of radio waves. Some manufacturers have started to replace barcodes with RFIDs, because they give more information about a particular product and are easier to scan. An RFID can contain specific information about the particular item to which it is attached, or in which it is embedded. Proponents of the technology argue that by replacing barcodes with RFIDs, checkouts are quicker and companies can track their inventory more accurately, such as where the product was manufactured, where it was shipped to, and in which store it was sold. RFIDs can also help reduce shoplifting in retail outlets.

However, because RFIDs are not turned off when an item is purchased, the new technology has raised privacy concerns. RFID tags can be read from a distance so that if there are enough sites outside a shop capable of reading the signals given off by the RFID tags, retailers and manufacturers would be able to track the location of the RFID tag as the consumer carried the product from place to place. It is this aspect that has caused most concern. In particular, campaigners are concerned about the use of RFID tags within clothing since this opens up the possibility of retailers and manufacturers being able to track the movements of consumers. Some privacy advocates say consumers should have a way to remove or disable RFIDs in the products they purchase.

One of the legal questions that has arisen from the use of RFIDs is whether the data that is gathered from RFIDs constitutes 'personal data' under the provisions of the Data Protection Act. This Act defines personal data as 'data which relates to a living individual who can be identified from those data', and some legal experts have argued that RFID does indeed constitute personal data. If this is the case, it means that the data that is processed as a result of using RFIDs should conform to the principles of the Data Protection Act. (Brown, (2003).

◀ Preliminary Activity for Week 11

Jump to...



Analysis, Application, and Exploration for Week 11 ▶



Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Ojt/Practicum 1

Social And Professional Issues

Participants



General


06 - Preliminary Examination

10 Regulating Internet Content (Cont.)


11 Personal Privacy And Computer Technologies


 Preliminary Activity for Week 11

 **Lesson Proper for Week 11**

 Analysis, Application, and Exploration for Week 11

 Generalization for Week 11

 Evaluation for Week 11

 Assignment for Week 11

System Integration And Architecture 2

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.


COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

 Assignments

 Forums

 Quizzes

 Resources



