

IN YOUR !!

Primer 1 - Surfing or Surveillance?

There are many ways in which new technologies can be used to "watch" and collect personal information.

IP Addresses

Websites are always collecting information about you. Sometimes, you provide them with your personal information when you sign up for a service, enter a draw or promotion, or complete a survey. Other times, it is without your knowledge. Some websites collect information by recording your IP – Internet Protocol address – this is an address that is unique to your computer and can be traced back to you. While many websites do not use your information as a surveillance mechanism, an IP address can be used to keep track of the websites that you have visited.

Electronic mail

Email is an easy, fun and quick way to communicate with your friends. You probably have the impression that your emails are private communications – and rightfully so, your email address and the information contained within the email itself contains your personal, private information. However, sending an email is like writing a note on a postcard without an envelope. Anyone along the chain of delivery has the opportunity to intercept or read it. In addition, email is persistent. Once emails are sent, they never completely disappear, even once deleted from your inbox or sent mail. The email leaves a "print" on the hard drives of both the senders' and receivers' computers, and users have no control over this. While no one normally accesses these hard drive "prints" they are accessible and could be tracked down by your school, your teacher or even your parents.

Spam

Spam is unwanted junk email messages which are sent to you in large numbers and in an intrusive fashion. The collection, use and disclosure of your email address without your consent are growing privacy concerns. Sometimes, these unsolicited email messages may seem to "know" you – sometimes they include your name or might make reference to one of the names in your address book, or may even be targeted to your personal interests. This demonstrates that "spammers" have already compiled an extensive amount of personal information about you. They have done their research, collected data, and created a profile of the person that you are – often long before you have even received your first message from them. Sometimes the purpose of the spam is just to see if your email address is even active, and clicking on any link at all lets them know that the address is in use. Even if the spammers do not use the profile they create, they may sell it to marketers without your consent. Most times, you will never even know. The best way to deal with spam is to delete it without opening it and never reply to it.

Web Bugs

Web bugs are also used in emails, which send information back to the sender when opened. The bugs might record how much attention you have paid to the email, how

long it was open on your computer, or confirm that your email address is active. Some web bugs can also collect other information about you from your computer and even plant cookies and pop-ups on your computer.

Phishing

Have you ever received an email saying you have won the lottery? This is called “phishing” and is a means of committing identity theft and fraud on the Internet. An individual may send an email that appears to come from a company or business indicating that there is a problem with your account or that you have received money. The email will ask you to forward them an account number or other personal information. It is best to just ignore and delete these phishing scams.

Viruses/Worms

In a worst-case scenario an email message may introduce viruses, worms and Trojans into your computer system. Messages may contain attachments that embed malicious code into your computer to corrupt files or hijack your home page or Internet connection. This code may spread itself to other computers using your email address book. Remote surveillance tools can be installed that monitor and transmit your online behaviour, record your keystroke pattern, or open backdoors on your computer system which allow hackers to actually take control from a distance.

Users find solutions

- Make sure you are dealing with a real company before you reveal your email address.
- Use disposable email addresses for mailing lists, contests, etc.
- Read all your email messages offline. If possible, read them in text only format.
- Do not respond to spam in any way. For legitimate businesses, choose to opt out as soon as possible.
- Install and use anti-spam, firewall, anti-virus and other privacy and security enhancing software, and keep it up to date.
- Download and install critical security patches from your operating system.
- Use email encryption for particularly sensitive messages.
- Do not open attachments from unknown senders.
- Regularly change your password for accessing your email accounts.
- When forwarding messages, delete the previous recipients’ email addresses.

For more information, see chapter 4 in the *Techno-tonomy* privacy textbook.

© Alberta Civil Liberties Research Centre, 2006. Reproduced with permission.