Privacy Online – Naked in Cyberspace

Kimberley Heitman, Electronic Frontiers Australia Inc

Kimberley James Heitman, B.Juris, LLB, AACS, Barrister and Solicitor,Western Australia. Chairman, Electronic Frontiers Australia Inc (http://www.efa.org.au/), a non-profit organisation concerned with online rights and freedom of speech. Kim is in-house legal counsel for iiNet Limited (http://www.iinet.net.au), a Perth ISP, and a Board member of auDA, the TIO and AdultShop.com. Kim has published and lectured widely on Internet regulation and online legal issues. His home page is at (http://www.kheitman.com/).

Prologue

It's a balmy summer evening, and you are enjoying surfing the Net. You visit a few web sites, post a few messages to your favourite Usenet newsgroup, chat with friends on IRC and write a message to a web-based chatroom. Why then, are you inundated with unsolicited commercial email the next time you log on?

The web sites you visited employed secret data mining technologies such as cookies, web bugs and collated web logs, all of which allows profiling of visitors to the web site – including which web sites you went to before and after visiting that site. The Usenet newsgroup is data-mined for email addresses by automatic software that skims the daily Usenet feed for email addresses for sale to mass-mailing companies, often sorted by reference to the sorts of newsgroups. Thus posting to rec.autos.ford will result in unsolicited offers for cars, posting to alt.sex invites offers for pornography and many other shonky, illegal and deceptive businesses. The use of Internet Relay Chat invites similar harvesting of addresses by automatic programs (called "bots"), as do posts to web-based chat forums. For computer users who routinely browse the Web without security measures in place, the same protocols that allow the Internet to direct traffic also allow commercial interests and the police to monitor Internet activity to an extent that would be seen as intolerable in the offline world.

The online environment, vigourously regulated in relation to controversial or illegal content, is unprotected from the predations of commercial interests. Data aggregation and profiling is a booming business, offering advertisers and crooks an unparalleled access to millions of personal and business email addresses and personal details. As e-tailers and content sites search for possible revenue streams, the misuse of personal data has emerged as the most pressing need for firm privacy regulation. Right now, the ordinary Internet user is virtually unprotected from intrusions into privacy by commercial interests, and conduct illegal offline flourishes in the online environment.

Some of these privacy intrusions seem built into the architecture of the Net. All domain names, for example, have records at the relevant registry with the owner's identity and contact details which can be retrieved and collated by anyone who cares to do so. In using the Net, unique identifiers are allocated to users, machines and services and can be retrieved by those who have the skills, tools or legislation to do so.

Bugs, spiders and cookies

Since most Internet users do not have enough of a technical background to understand exactly how Internet tools work, privacy exploits have become entrenched in the online environment. First among the privacy-intrusive practices is the use of "cookies" – a small file downloaded from a web site onto the visitor's home computer.[1] The "cookie" then remains on the visitor's hard drive for whatever purpose the designer requires – either to confirm a session visit (for audit purposes), to verify the identity of the visitor or, in some cases, to execute a program without the permission of the owner – including in one memorable instance a program which formatted the victim's hard drive. While unauthorised access to a computer is a crime in every State and Territory, the cookie technology bypasses the criminal law by being "voluntary" – if one sets up the web browser program to refuse cookies then no intrusion occurs. It is therefore arguable by the designers of cookie-ridden sites that if visitors do not choose to refuse cookies then they are volunteers for whatever consequences follow.

Web-bugs are another secret technology – usually existing as a 1 pixel picture file on a web page, too small to be seen with the naked eye. The web bug is therefore loaded by the visitor's web browser unintentionally, giving the web site a separate logfile of the Internet addresses of visitors to the page in question. A web site can therefore use web-bugs to spy on the personal details of visitors to the web site without the visitor even being aware that it has happened.

The web is also mined for email addresses and other personal details by "web-spiders", programs which search the Net for web pages which may or may not be linked to search engines. Any page in a web directory can be reviewed by these programs, whether or not they are linked to search engines and indices. These programs, used by search engines to retrieve links, also provide to commercial and security interests a rich vein of personal data, suitable for profiling or sale.

Web sites more and more demand "registration", or proof of identity such as a credit card number. These demands have no function for the use of a web site, but are instead required for a new revenue stream based on the aggregation and sale of personal information by web sites. In the absence of privacy legislation outlawing such secret data mining, even "reputable" companies find the lure of the trade in private information irresistible and seek to incorporate the sale of personal details in the business model. These privacy abuses are often concealed by self-serving "privacy policies" which, deep in the fine print,

permit the site owner to collate and sell personal information to others.

What about the Australian Competition and Consumer Commission (ACCC)?

It might be hoped that the ACCC would take action against these misleading, deceptive and intrusive abuses of consumers' privacy. However, such hopes were dashed when the ACCC approved the registration of the Australian Direct Marketers' Association **(AMDA)** Code of Practice as the "industry standard" for online marketing. Despite the ADMA's limited credentials to represent online e-commerce, the ACCC approved a Code of Practice which permits so-called "opt-out" mailing lists rather than the opt-in system that is widely acknowledged as the only appropriate standard for the Internet. What this means is that a marketer is free to assemble an electronic mailing list however it pleases, by using data mining or web page tricks, or by purchasing such lists from data cheats and thieves worldwide. So long as the unhappy recipients of mass commercial email (or "spam") are provided with a valid Internet contact which receives requests to "unsubscribe" from the particular commercial email sent, mass commercial email is legal in Australia and enjoys the protection of the ADMA Code for the purposes of the Trade Practices Act 1974 and the Privacy Act 1988.

Of course, "opt-out" lists only work on the basis that one is intruded upon first – and there is little if any control over whether the "opt-out" process is completed. In fact, long time experience is that the list of email addresses that have elected to "opt-out" is even more valuable than an unsorted list of email addresses – all the "opt-out" email addresses are likely to be current and active. While the ACCC has accepted that theft of privacy is only unlawful after the first attack, EFA asserts that theft of privacy should be prosecuted in all cases as a deterrent to mass-marketers who steal Internet resources, forge reply addresses and (as several studies have demonstrated) quite often fail to deliver the services advertised in any event. A marketer who will steal privacy and Internet resources by the sending of spam may have no compunctions about stealing credit card details and cheating those Internet users innocent enough to reply with an order.

Surveillance by the State

Whenever a user of the Internet is surfing online, their Internet Service Provider ("ISP") has allocated to them a unique Internet Protocol ("IP") address that provides a form of electronic fingerprinting for all online activities. This leaves an electronic trail from web site to web site, through IRC and ICQ, to every download and picture viewed. While the user may feel safe in an anonymous environment, every keystroke is capable of being logged and identified with a particular person by reference to the IP address and matching data such as Caller Line Identification or registered user details.

The ISP, of course, has the technical capacity to read a user's emails and create a logfile of all web sites visited and sites downloaded. The Telecommunications Act[2] places certain privacy controls over the release of this information, however there are several major loopholes under Division 3 of the Act which have eroded whatever value these protections may have.

Division 3—Exceptions to primary disclosure/use offences

Subdivision A—Exceptions

279 Performance of person's duties

(1) Section 276 does not prohibit a disclosure or use by a person of information or a document if:

(a) the person is an employee of:

(i) a carrier; or

(ii) a carriage service provider; or

(iii) a telecommunications contractor; and

(b) the disclosure or use is made in the performance of the person's duties as such an employee.

(2) Section 276 does not prohibit a disclosure or use by a person of information or a document if:

(a) the person is a telecommunications contractor; and

(b) the disclosure or use is made in the performance of the person's duties as such a contractor.

(3) Section 277 does not prohibit a disclosure or use by a person of information or a document if:

(a) the person is an employee of:

(i) a number-database operator; or

(ii) a number-database contractor; and

(b) the disclosure or use is made in the performance of the person's duties as such an employee.

(4) Section 277 does not prohibit a disclosure or use by a person of information or a document if:

(a) the person is a number-database contractor; and

(b) the disclosure or use is made in the performance of the person's duties as such a contractor.

(5) Section 278 does not prohibit a disclosure or use by a person of information or a document if:

(a) the person is an employee of:

(i) a recognised person who operates an emergency call service; or

(ii) an emergency call contractor; and

(b) the disclosure or use is made in the performance of the person's duties as such an employee.

(6) Section 278 does not prohibit a disclosure or use by a person of information or a document if:

(a) the person is an emergency call contractor; and

(b) the disclosure or use is made in the performance of the

person's duties as such a contractor.

Thus section 279 gives a blanket defence for the release of personal information "in the course of one's employment", resulting in an imponderable question as to how a consumer could ever restrict the circulation of their personal data within a workplace. Worse, communications between ISPs or carriers, Internet Content Hosts and moderators are plausibly covered as "in the course of employment", giving rise to the outcome that exchange of information within the telecommunications industry is not restricted.

However, of recent notoriety has been the practice of law enforcement authorities to issue requests to carriers and ISPs for release of information to aid the investigation of criminal offences. Police are able to engage in "fishing expeditions" - merely by sending a "section 282 certificate" they are able to require the ISP or carrier to release login and call records, personal and billing details (and in the case of ISPs, full details of email sent and received and full details of sites visited and all online communications). Section 282 in fact extends beyond investigation of criminal investigations – it provides the same process for civil collection agencies and Government agencies to obtain information that may lead to the imposition of a fine, copyright charge or other pecuniary penalty.

Recently[3], Parliament was informed during a Senate budget committee hearing that the Australian Communications Authority had recorded 998,548 occasions in 1999-2000 where police had sought telecommunications interceptions from carriers and ISPs, a 12.6 per cent increase on 886,151 interceptions the previous year. It's perhaps notable that this only covers the limited number of carriers that are required to forward statistics to the ACA – a thousand Australian ISPs are not (as yet) required to report to any public authority the details of such requests from police. This is an epidemic of privacy intrusion created by weak laws and a lack of respect for privacy by the Federal Government.

So what is wrong with intrusions on privacy?

Naturally, law enforcement agencies claim that intrusions on privacy only affect criminals and their use of private information is tightly controlled. Frankly, the history of the use of police databases does not support this contention – whether by accident or corruption the data aggregated by police has and will in the future be passed on to commercial and criminal interests. The online environment needs a higher degree of privacy than the offline world because only electronic means of verification of identity is possible in cyberspace – leakage of personal information can lead to effective impersonation, fraud, cyber-stalking and theft of confidential information. Few people would willingly hand over their passport, credit cards or wallets – but in the online environment, the possessor of the personal identifiers of a person may for all intents and purposes appear to be that person in online transactions.

Since the Federal Government has utterly failed to protect online privacy with the passage of the business-friendly Privacy Act 1988, it remains the responsibility and task of users of the Internet to protect their own privacy. Some countermeasures can help a great deal – turning off cookies, caching web bugs in traps, programming against web-spiders and being careful about where and under what circumstances one gives out one's email address. The use of anonymisers and anonymous remailers, personal encryption and firewalls, careful choice of software that enhances privacy and security and Acceptable Use policies in organisations can considerably reduce the incidence of privacy intrusions with few if any adverse affects on enjoyment of the Internet.

However, with millions of Australians now online – often without basic training or access to privacy-friendly software – it is regrettable that the Government does not protect its people against commercial exploitation and security intrusion with a tough Privacy law and vigourous standards for law-enforcement and civil claimants' access to telecommunications data without warrant.

In the meantime, only self-help and security-consciousness can abate the flood of commercial marketing and data mining on the Internet, at considerable cost to the ordinary Internet user. The Government's commitment to the online future is equivocal in the current circumstances where industry advice is ignored, and the particular privacy abuses running rampant in the online environment receive no penalties. For the time being, it is a case of "shields up!" and waiting for a Government prepared to seriously tackle spammers, marketers and crooks on the Internet.

---

1 For a detailed examination of cookies, see Roger Clarke's article "Cookies", online at <http://www.anu.edu.au/people/Roger.Clarke/II/Cookies.html>

2 Telecommunications Act 1997 (Commonwealth) Division 3, especially ss.280 and following.

3 Reported in "The Age" (Melbourne) 4th February, 2001, online at <http://theage.com.au/news/2001/02/04/FFX73146QIC.html>