JITTA
JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

GAPS BETWEEN POLICY AND PRACTICE IN THE PROTECTION OF DATA PRIVACY

SOPHIE COCKCROFT, University of Queensland
UQ Business School, St Lucia, Queensland 4072, Australia. Email: sophie@business.uq.edu.au

ABSTRACT

A common casualty of poor information security is the privacy of the individual. Much has been written about formulating privacy policies, and there has been some work in identifying privacy abuses. This paper brings the two areas together by reviewing some of the key aspects of privacy policy. It presents a taxonomy of privacy abuses distilled from publicly available online reports issued during 2001. The gaps between policy and practice are identified and some solutions put forward to fill those gaps.

INTRODUCTION

Poor information security can have a severe impact on an organisation. The major risk in consumer to business e-commerce is that security concerns will result in a lack of consumer confidence resulting in a loss of business. Information Security is defined by Parker (2001) as: "The preservation of confidentiality and possession, integrity and validity, and availability and utility of information".

With reference to the definition above, privacy is incorporated in the first two items; confidentiality and possession. A recent report suggested that only one in three businesses implement formal privacy policies (Computer Economics 2001). Even when policies are in place they are often not rigorously applied until a significant security breach forces management to focus on them (Fonseca 2000; Milberg, Smith et al. 2000).

This study is confined to privacy abuses relating to computerised data assets of an organisation or an individual, and any channels through which this data is transmitted.

Before any meaningful discussion of privacy abuses and their remedies can occur, it is necessary to acknowledge the complex backdrop against which such a discussion takes place. There are three dimensions to the space in which privacy policy and safeguards are developed; first, a plethora of regulatory approaches to assuring privacy exist worldwide. These approaches stem at least in part from the culture of the country in which they are developed. Second, new technologies are changing the landscape of privacy, but also the way organisations function, and third,

Gurpreet Dhillon acted as senior editor for this article.

Cockcroft, S., "Gaps Between Policy and Practice in the Protection of Data Privacy," *The Journal of Information Technology Theory and Application (JITTA)*, 4:3, 2002, 1-13.

organisational issues, including the structure of the organisation itself and the policies that evolve within it. This conceptual space is illustrated in Figure 1.

The paper is organised into four sections. First a review of the current research into the regulatory, technological and organisational policy aspects of privacy is given. The purpose of this review is to develop an understanding of how privacy policy evolves within an organisation. In the second section a content analysis of a cross section of news stories is carried out. From this, a taxonomy of privacy abuses is distilled, these are compared to the results of existing studies. Third, using the taxonomy and guidelines for managing information security from section 1, gaps or representational deficiencies are identified which suggest where the weaknesses in current thinking on information privacy exist. Each of these abuses is discussed in turn. Finally some technical data management solutions are put forward.

Laws, regulations and ethics

Laws and regulations

Balancing different privacy perspectives within the realm of increasingly connected global e-commerce presents a significant challenge to managers. Whilst privacy as an individual right is a very old concept, the information age has brought confusion about what is ethically right or wrong in the realm of privacy. Many privacy abuses do not break any law – it depends under which jurisdiction they occur. Even at the ethical level, opinions differ about what constitutes an abuse of privacy. Henderson (1999) gave the example of mailbox clutter or spam as something that could be seen as merely inconvenient rather than damaging to an individuals privacy. Eliminating spam was, however identified as one of the top five objectives for assuring privacy in a recent study (Dhillon and Moores 2001).

CONTRIBUTION

Although many researchers identify personal privacy as an issue of concern, there is little by way of suggestions as to how privacy could be improved. This paper makes a contribution in suggesting means to fill the gap between policy and practice. The research objective is to identify issues of importance to the online security community and systematically identify where current thinking on privacy policy is inadequate. It should be of interest to practitioners and researchers in information security management.

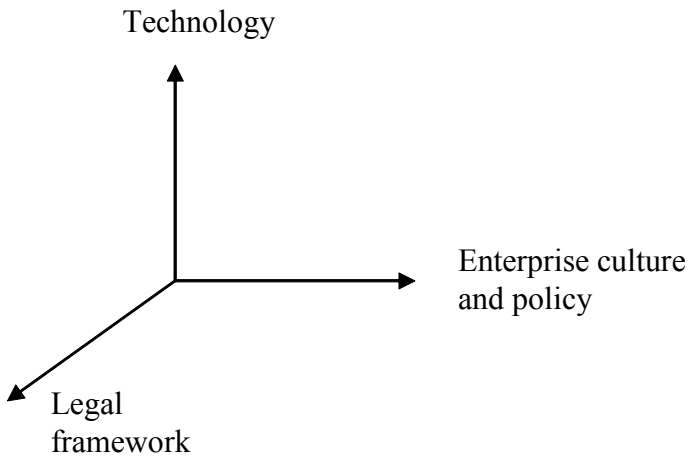

Figure 1. Space within which information privacy exists

Given the plethora of combinations under which an enterprise could find itself in the space described by Figure 1, it is not surprising that the current state of the law of privacy has been described as a "discordant morass of domestic and foreign regulation" (Davidson and Bryant 2001). The fact that privacy regulations around the world are an eclectic mix provides companies with opportunities, but they should also be aware of pitfalls (Leizerov 2001). Leizerov (2001) suggests that whilst there may be perceived advantages to setting up business in a country with lax privacy laws, the residents of such countries are often less inclined to provide companies with accurate information. The spectrum of privacy regulation approaches is well described in the work of Milberg, Burke, Smith, & Kallman (1995). This spectrum is encapsulated in

Figure **2**. Countries at the lower end of the scale, with lower levels of government involvement, such as the US rely more on self-regulation and market factors to implement privacy. Countries in the middle such as New Zealand and Australia employ a data commissioner. Countries at the higher end of the scale require that databases containing personal information be licensed. EU countries have the strictest regulations with respect to information privacy following the implementation of the EU privacy directive (EU 1998). This is causing some problems with doing trade with the U.S. (Anon 2001), (Leizerov 2001) (Davidson and Bryant 2001). The safe harbour approach (US Department of commerce 1998) is in place to tackle this mismatch, but it is proving arduous implement. It has been suggested that Europe's Privacy Laws may become a global standard (Thibodeau 2001) due to the regressive impact on international commerce of the mismatch, and the overwhelming preference of US citizens for stronger privacy rules.

Technology

Enhanced capacity for storing and transmitting data has transformed the face of access control. Sensitive information is no longer held under lock and key. Increasingly organisations rely on electronic communication and data sharing, for example in Enterprise Resource Planning (ERP) tools and Corporate Intranets.

Typically e-commerce applications have front-end servers that provide Internet network services, this is all that the customer sees. It is supported by backend infrastructure providing online transaction processing. This can include ERP systems. Security is a concern for IT managers who are exposing ERP applications to the Internet for the first time. An example of such a concern is the security of information on public or shared computers. Many Internet service providers use caching to improve performance, this can result in data remaining in the cache when the user leaves their machine. This data could give hackers a way in to the company's backend systems.

Corporate intranets introduce new privacy concerns such as the capacity for data matching, e-mail monitoring and electronic surveillance. The 2001 AMA survey reported that 77.7% of US firms record and review employee communications and activities including phone calls, e-mail, internet connections, and computer files (AMA 2001).

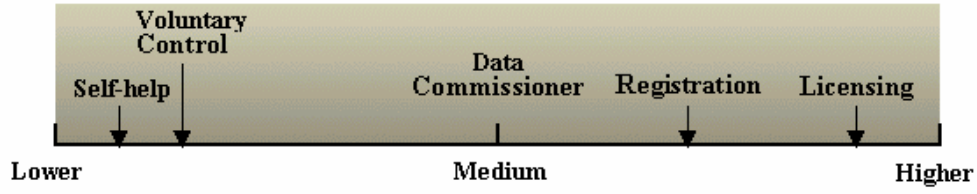

Figure 2. Level of Government Involvement in Corporate Privacy Management (Milberg, Burke et al. 1995) p. 66

The increasing importance of Internet commerce has led to increasing exploration of mobile and dynamic entities to combat the shortcomings of the traditional client server model. Application code can be dynamically relocated to other nodes in the system leading to greater scalability, and overcoming unreliable links. However, wireless devices form ad hoc networks – an adversary can compromise a single node and instruct all routing to go through the compromised node. Mobile users also wander through different cells and ad hoc networks – information on the users device can be stolen or altered without the users knowledge, and the device itself can be stolen which may well carry large amounts of personal data (Ghosh and Swaminatha 2001). The effectiveness of the Wired Equivalent Privacy (WEP) security protocol is still under debate. It is designed to provide a wireless LAN with the same level of security and privacy as a wired LAN, but still has major security flaws (Surveillance Camera Players 2001).

Privacy Policy

Many frameworks have been put forward as guidelines for privacy policy in the organisation (Henderson 1999) (Agranoff 1991) (Gaskell 2000) and some work has been done on identifying major internet privacy concerns among managers (Dhillon and Moores 2001). There are five fair information principles that form the basis for most privacy legislation (Federal Trade Commission 1998). Many self-regulatory bodies also use them. They are as follows:

- Notice and awareness,
- Choice and consent,
- Individual participation and access,
- Security information quality and integrity,
- Enforcement, accountability and recourse.

Privacy policies are often subdivided into those relating to data collection, accuracy and confidentiality (Agranoff 1991).

Table 1 Summarises the major findings of the security policy research identified above. The areas highlighted in grey will be referred to in the discussion.

The following section describes a content analysis of recent reports of privacy violations, in the concluding sections, these violations are set in the context of privacy policy and loopholes are identified.

METHODOLOGY

Privacy.org is a joint project of The Electronic Privacy Information Center (EPIC) (EPIC 2002) and Privacy International (Privacy International 2002). EPIC is a public interest research centre, which maintains an extensive list of privacy resources, including organizations, publications, conferences, and newsgroups, as well as a privacy archive of online documents and articles. The other partner in the project, Privacy International, focuses on issues of privacy specifically in the area of human rights. Together they provide a forum for daily news, information, and initiatives on privacy. Motivation for inclusion of news stories comes from the readers of privacy.org who are a self-selected group with an interest in privacy. Issues arising on privacy.org are considered worthy of review due to broad mandate and international focus of the organisations concerned.

The classification approach follows the recommended methodological approach for content analytic research of the world wide web described in (Weare and Lin 2000). The research question posed is "what are the key privacy issues of interest to the online security community". In order to validly and reliably classify messages first a sampling frame is identified, then the material within this frame is unitised. Finally a categorisation scheme is identified.

The choice of this sampling frame, described in detail below, is an example of using a "collector site" (Weare and Lin 2000). As asserted by Weare the use of this type of site is likely to be more comprehensive than using a search engine because it distils considerable experience of searching the web on the topic of privacy.

In traditional media such as newspapers, the content is essentially linear and the unit of analysis is the news article.

<table>
<tr><td colspan="3" rowspan="3">Enforcement, Accountability, Recourse</td><td colspan="5">Appoint Individual Responsible</td></tr>
<tr><td colspan="5">Education</td></tr>
<tr><td colspan="5">Damage Limitation</td></tr>
<tr><td colspan="2">DATA COLLECTION</td><td>Obtained in a lawful manner</td><td>DATA ACCURACY</td><td>Verify Sensitive Data</td><td colspan="4">DATA CONFIDENTIALITY</td></tr>
<tr><td>Notice and awareness</td><td colspan="2">Publish Policies</td><td colspan="2">Security, Information Quality and integrity</td><td>Keep up to date</td><td colspan="2">Secondary Use</td><td colspan="2">Unauthorised Access</td></tr>
<tr><td rowspan="4">Choice and Consent</td><td colspan="2" rowspan="3">Consent (implied or otherwise</td><td colspan="3">Participation and Access</td><td colspan="2">Data not disclosed for reasons other than that for which it was collected</td><td>Physical</td><td>Keep Logs</td></tr>
<tr><td colspan="3">Make available to individual</td><td>Verify</td><td rowspan="3">Third parties</td><td rowspan="3">Not given access</td><td>Technical</td><td>Traffic Profile Configuration Management</td></tr>
<tr><td colspan="3">Resolve Errors in favour of Individual</td><td>Backups of original installs</td><td>Admin</td><td>Designate Responsible Manager</td></tr>
<tr><td rowspan="3">Only collect data to meet business objectives</td><td>Adequate</td><td colspan="2" rowspan="3"></td><td rowspan="3">Permission obtained from original source</td><td>Procedures</td><td>Map Privacy sensitive data</td></tr>
<tr><td>Relevant</td><td colspan="3">Disclosures should be noted and records kept</td></tr>
<tr><td>Not excessive</td><td colspan="3"></td></tr>
</table>

Table 1. Guidelines for Self-Regulation (Adapted from (Agranoff 1991) and (Henderson 1999) and (Gaskell 2000))

Web-based approaches to the dissemination of information have a non-linear nature, which to some extent has obscured the boundaries of messages. However, news sites still adopt a standardised structure whereby there is a front page, and one web page devoted to each story, thus the unit of analysis in this case remains the news article.

In order to categorise web pages the frequency that an idea or subject appeared in a message is used, i.e. the most frequently cited topic became the means of classification.

The study focuses on a calendar year of stories from the archives of www.privacy.org from 1 January 2001 and 31 December 2001. In this time 468 stories were posted. For the purposes of this study, stories were restricted to those describing actual or threatened privacy violations, which reduced the sample to 282 stories when this was further restricted to those in the IT &T domain – excluding for example issues of the human rights implications of issuing identity cards or medical information being revealed by word of mouth and duplicate story subjects were removed. This resulted in a total of 72 usable reports. The reports were then classified according to the key violation(s) contained within them. Violation descriptors were drawn from previous research.

Privacy Abuse	Count
Unauthorised Secondary Use	17
Civil Liberties	15
Identity theft	11
Data matching/profiling	11
Unauthorised Plugins/Downloads	10
Computer Programming Error	3
Transborder flow	3
user error/data integrity	2
	72

Table 2. Classification of privacy abuse stories on www.privacy.org 1 January 2001 – 31 December 2001

RESULTS

Table 2 shows the results of the content analysis. There is some overlap with the top five privacy issues established by Dillon and Moores using a Delphi Survey (Dhillon and Moores 2001), which were as follows

- Companies should not sell personal information
- Adequate measures should be in place to prevent theft of personal information by a third party
- Eliminate the chance of losing personal files
- Maximise security to deter hackers from destroying data
- Eliminate spam

Figure 3 is a taxonomy derived from reviewing the stories within the sample frame.

ANALYSIS

The following section reviews the major issues identified, in order, and some solutions put forward. These are drawn together in the final section where the representational gap between policy and reality is elucidated some suggestions for narrowing that gap are put forward.

Unauthorised Secondary Use

Data that was used for secondary purposes without authority was comprised of first, name and address information, and second browsing data. Concerning name and address data unauthorised use was reported in the following categories.

a) Internal: where a company uses information it gathered for one purpose, for a different purpose

b) External: where the organisation simply on-sells the data for commercial gain (Bowman 2001) (O'Harrow 2001)

In the most high profile external cases were those that involved children, since they contravened the US children's online privacy protection act (EPIC 1999).

Two further issues arose in the analysis of the stories. The issue of opt out, and what companies should do with their data in the event of bankruptcy.

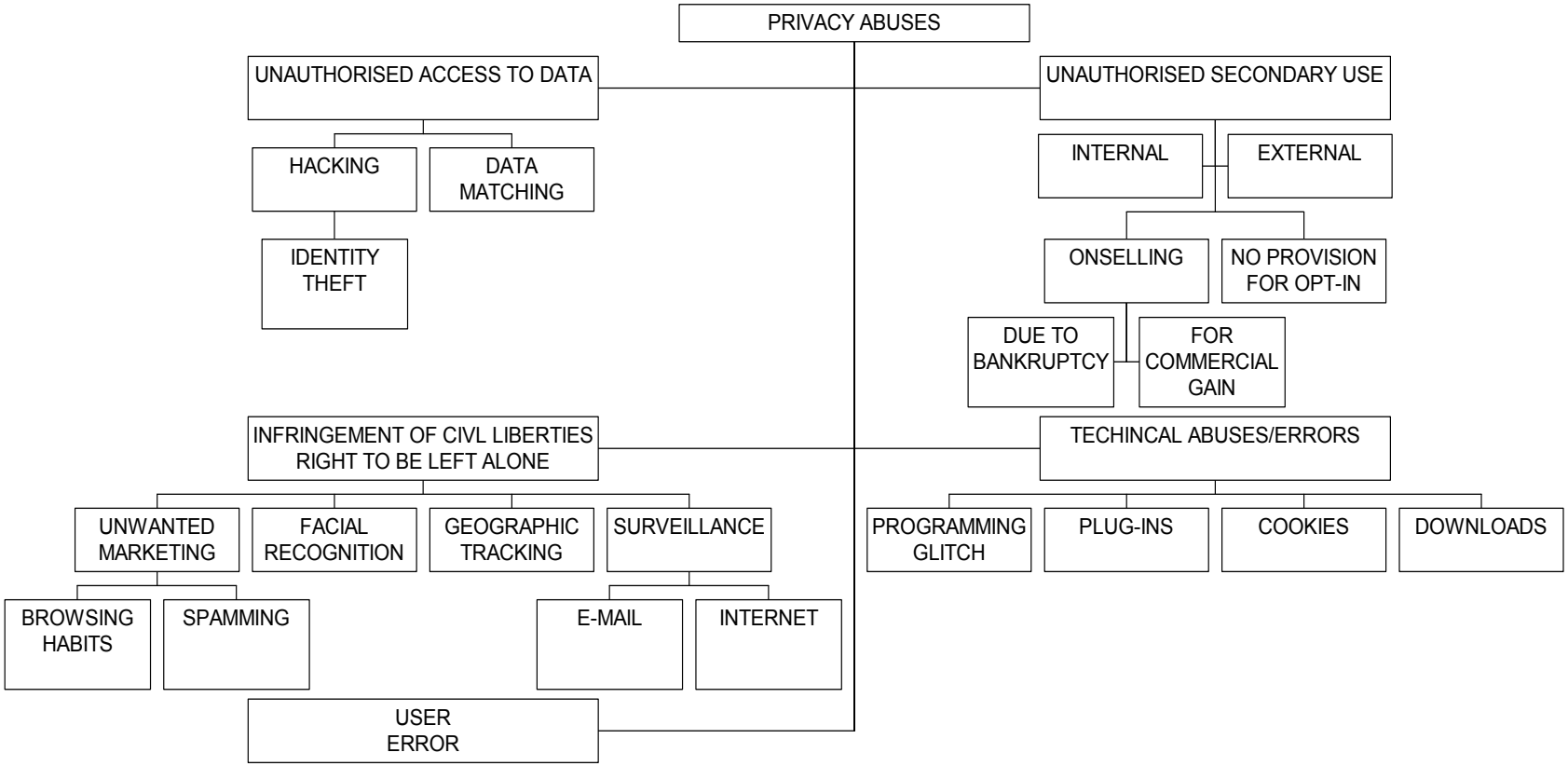

Figure 3. Taxonomy of publicised privacy abuses

(i) Opt out

In the news stories selected a recurring theme was the absence of Opt-in. Customers generally have their personal information included in marketing strategies, unless they specifically request that this does not happen. A prominent case was the Macy's wedding registry has a default opt-out system where customer's wedding details are passed onto other Macy Partners including name, birth date and credit card number unless the customer expressly opts out. This puts the burden of assuring personal privacy on the customer. Privacy advocate groups suggest that default opt-in would be a better approach.

(ii) Bankruptcy

Clearly from the analysis carried out here companies continue to sell information. There were a number of cases where companies had on sold personal information such as names addresses and telephone numbers. Reasons for this were bankruptcy (Federal Trade Commission 2001) (Wolverton 2001) both companies decided to on-sell their customer information to rival/takeover companies in order to recoup losses. Privacy policies should be explicit about the destiny of personal information in the event of bankruptcy.

Concerning of data on browsing habits a web filtering company created reports on online habits, which it sold to marketeers. In a similar approach a telephone companies have monitored clients phone using habits to market other products to them (McCullach 2001). The first case received attention again because it concerned children. In the second case the practice continued. A third case is built in copyright protection for CDs that means they cannot be listened to on a computer. The rationale behind this is the fear that users will employ software to encode them as MP3s and distribute them on the Internet. As a remedy some companies require users to register with a website before listening to the CD on a computer. This information can then be used to market similar music to these individuals. This last case is clearly a conflict between protecting copyright and misusing consumer's personal information. There is a blurred line between this last class of secondary usage, and the next classification "civil liberties". It is not uncommon for a law-enforcement or other agency to hold information about a person, or their whereabouts for no particular reason, which is widely seen as an infringement of civil liberties. Some examples follow.

Civil Liberties

Devices with Spatial Tracking ability

The advent of devices that report user location, such as cell phones that track user location via Global Positioning Systems GPS, affords commercial profilers and the government more opportunities to monitor behaviour. Two interesting cases in the period under review were the "Enhanced 911" service, which alerts police to the location of a mobile phone when the user dials 911 (Pelofsky 2001), and Acme Rent-A-Car, a company in Connecticut, which installed GPS in its fleet of rental cars. The rental car company monitored the vehicle's speed, and automatically imposed fines. This was the subject of a court case where one of ACMEs clients sued them for charging him $450 for speeding three times whilst using one of their cars (Lemos 2001). It has been suggested that an opt-in approach should also be used to allow users of mobile devices choice about whether they are tracked or not. Another technical solution has been proposed; the use of disposable mobile phones, these are similar in concept to disposable cameras, and would not reveal the identity of the user. The notion of building in intelligent agents that negotiate a privacy arrangement between parties before a deal is done has also been suggested (Forder and Quirk 2001) this requires an international standard on privacy exchange such as P3P (P3P 2001).

Surveillance

The Privacy Foundation (PF) reports in a recent study that one-third of employers are continuously monitoring employees' e-mail usage. In the same class as this, is a branch of video surveillance that includes facial recognition. Again civil libertarians resent this invasion; there is a group who raise public awareness of this issue by staging plays or other performances for surveillance cameras (Surveillance Camera Players 2001). Even in the wake of events of September 11th, this

group remains opposed to video surveillance (Surveillance Camera Players 2001), although there is evidence of some softening in the general community (Schneider 2001).

Identity theft

Theft of personal information was also one of the key issues identified by Dhillon and Moores (2001b). It should be noted that even without an internet of computerised information systems this can occur, a skilled fraudster can gain the appropriate information by stealing a wallet or intercepting mail to set up accounts, loans etc, in the victims name and begin running up debts. Online applications for credit cards make the process more anonymous and various online data sources could ease the task of such impersonation, for example one story within the sample frame reported that "birth records of more than 24 million Californians have been sold by the state and posted on the Internet, offering easy access to critical information needed to create fake identities. By logging onto a genealogy Web site, people can gain access to such personal data as someone's place of birth and mother's maiden name, which can then potentially be used to access bank records and other sensitive material" (San Jose Mercury News 2001).

Data matching/profiling

Stories relating to data matching were the fourth most common. Prominent examples were the state of Michigan gathering Social Security Numbers (SSN) when people applied for driving licenses with the purpose of tracking down people who are not making child support payments (Cain 2001).

Hotmail, a free e-mail service, has posted users' e-mail addresses, cities, and states to Infospace, an Internet white pages directory. The combination of Hotmail user information with the Infospace directory creates privacy risks, as the Infospace already directory contains individuals' addresses and phone numbers. Users of the Hotmail service must "opt-out" of this information sharing (Hopper 2001).

New York City voter registration records, that include voters' home addresses and party affiliations, are now online. In order to find if someone is registered to vote, and get their name and address all you need is a surname and date of birth, date of birth can be looked up using anybirthday.com (Privacy Foundation 2001).

It was evident from the above stories that where outrageous breeches occurred, legal bodies in the states concerned would set about remedying them. However, generally it seems the onus is still on the individuals to protect themselves.

Unauthorised Plug-ins/Downloads

Some software and devices are sold with plug-ins to carry out monitoring of browsing/watching activities. A popular software games distributor Egames included "Spyware" which downloaded a program to users machine and monitored browsing activity (Bonisteel 2001).

The Privacy Foundation has discovered that the TiVo personal video recorder collects information about users' TV viewing habits, and communicates the information back to the company's headquarters (Martin 2001).

As a technical rebuttal to this type of privacy abuse the Privacy Foundation has developed freeware that can detect web bugs. Web bugs are imperceptible graphics on web pages or embedded in e-mail that are designed to collect user data. The program, Bugnosis, is a plug-in to the Microsoft Internet Explorer web browser (Privacy Foundation 2001).

Computer Programming Error

A printing error by an American Express processing centre resulted in clients receiving other persons' account statements. Some clients received statements that included the Social Security Numbers, birth dates, and fund balances of co-workers and strangers. Andrew Shen, of EPIC, commented that: "More and more, the cause of privacy breaches isn't malicious intent but a programming mistake." (Cha 2001). The representational gap between existing privacy policy and these types of error is simply that staff training and education is not being conducted effectively, in this case testing of the system must have been inadequate.

Transborder flow

A few cases arose in the sampling frame that questioned the efficacy of the safe harbour agreement in protecting personal data. In particular a UK resident is planning to ask the Federal Trade Commission (FTC) to investigate whether the Microsoft Passport system violates the EU-US safe harbour agreement (Krebs 2001).

User Error

Richard Smith, the Chief Technology Officer of the Privacy Foundation, requested and received his own profile from ChoicePoint. ChoicePoint sells profiles to private investigators, attorneys, and federal law enforcement agencies. A review of the profile led Smith to conclude that it contained more misinformation than truthful information. And, Smith learned, he cannot opt-out from the ChoicePoint's collection of personal data (Scheeres 2001).

Eli Lilly, a major drug manufacturer, accidentally disclosed the e-mail addresses of hundreds of patients using Prozac, an antidepressant (O'Harrow 2001).

Clearly remedies for this exist in privacy policies. The first case relates to verifying sensitive data, and the second to user training. More careful implementation of business rules could assist in minimising the entry of incorrect data.

DISCUSSION

Table 1 shows the main tenets of self-regulation in terms of collection, accuracy and confidentiality, subdivided according to the FTC guidelines (Federal Trade Commission 1998). The content analysis of recent news stories suggests that a number of these areas are not given the attention they deserve. These areas are highlighted in grey in Table 1.

The area for greatest concern is secondary use. In countries on the right hand side of the scale in

Figure **2**, this activity is illegal. Where it is not, the recommendation is that disclosures should be noted and records kept. Even this basic form of privacy protection is lacking in many organisations. It is likely that this record keeping is not occurring because there is insufficient incentive to do so, yet stories of unauthorised secondary use are still making headlines.

Another major issue foreshadowed at the start of this paper is the fact that only a third of businesses implement privacy policies. The stories reviewed focused particularly on bankruptcy and what happened to data in cases where a firm goes bust. Are a person's details a tradeable commodity? And at the very least should policies with respect to data, in the event of bankruptcy be published?

In the area of data collection concerning choice and consent, specifically it is arguable whether implied consent is good enough to protect an individual's privacy. Many privacy advocates suggest that consumers should have to opt-in to be included on mailing lists etc. This has negative implications for businesses, in particular those that rely heavily on marketing. From the consumer's point of view receiving mailings only in a stated area of interest could be construed as better service than bulk mailing.

In the area of participation and access, individuals have the right to access information about them and to know what data is collected. This right fringes on the discussion of civil liberties, and it is hard to reconcile with the actual or perceived need for surveillance, which by its nature cannot be made public. Information stored about an individual could be done so in the name of national security in which case it may not be prudent to allow them to access it. Other cases where this might occur could be for the consumer's own protection. In the past this has been the case for example with medical records. However, if we assume all information held about an individual *should* be available to that individual, how are they to go about finding the source. This is a problem with spam where very often it is hard to discover the source of the information, this detection and enforcement of this right, is the function of activists such as the "death to spam" group (Rimmer 2002).

In the area of enforcement, accountability and recourse, which spans the

other areas, stories analysed revealed a de-facto lack of accountability in testing and enforcement. Theoretically this is overcome by vesting responsibility within a firm on one individual. This is not occurring possibly due to a high turnover of staff. It may also be due to the flat managerial structures of modern businesses which tend to take away absolute power from individuals. The effects of lapses in training, enforcement and testing are potentially disastrous, if only from a public relations point of view. If an inadequately tested product goes to market, and confidential customer details are inadvertently revealed it is likely to produce a crisis of confidence among consumers.

Limitations

Some key issues identified by other researchers are absent in this work; in particular the threat of unauthorised access in terms of hacking received little attention. Hacking is often carried out as an end in itself (Spafford 1995). It is beyond the scope of this paper to describe all the motivations and outcomes of hacking. This has been covered in detail in (Parker 2001). However, one of the frequently encountered issues on privacy.org is identity theft. This is very often a by-product of hacking for example where the hacker seeks to harvest credit card details from a commercial site. Another area that could have been expected to receive more attention was mobile e-commerce. Whilst some issues peripheral to mobile e-commerce, such as geographical surveillance and marketing emerged. The security of mobile e-commerce and data theft by this means did not receive much attention in the sample of stories analysed. Both these omissions in the data could be explained by the emphasis on privacy and in particular the human rights focus which is inherited through association with Privacy International.

Conclusion

If a company is to self-regulate effectively aspects of policy relating to the above issues should be taken seriously. Secondary use has emerged as a key issue, supporting previous research in the area. In countries or states where there are no regulations specifically banning such activities there is little motivation to do so. The onus is on the individual to protect their rights, and as explained in the section on regulation, in countries where there is scant privacy regulation the data collected from individuals is likely to be correspondingly poor. Whilst implied consent is clearly a controversial area for privacy advocates, it is clear that a balance needs to be found between the ability to do business, specifically marketing, and the necessity to allow clients freedom not to participate. Surveillance has taken centre stage with the world on heightened alert to terrorism. It would be interesting to know whether this has had the effect of lowering expectations of participation and access with respect to personal data. Finally, the emergence of flat organisational structures, in which there is greater access to data and information at all levels of the enterprise, challenges the recommendation of many privacy researchers that responsibility for privacy policy and information liability be vested in one individual. This paper has reviewed a subset of news stories within a defined sampling frame. With reference to research on privacy policies, deficiencies between what is recommended as policy and areas in which abuse of privacy occurs has revealed particular shortcomings and areas on which more work needs to be done by enterprises seeking to do business in the global community.

References

Agranoff, "Controlling the threat to personal privacy:corporate policies must be created." *Journal of Information Systems Management*, 1991, 8, pp. 48-52.

AMA, *2001 AMA Survey Workplace Monitoring and Surveillance*, New York, American Management Association, 2001, 2.

Anon, "Australia: We're Adequate!" *Privacy Journal*, 2001, 4.

Bonisteel, S., “Michigan reaches privacy pact with e-games over spyware,” NewsBytes, 2001, available at http://www.newsbytes.com, last accessed 02/02/02.

Bowman, “Who is at heart of congressional hearings,” 2001, available at http://news.com.com, last accessed 14/02/02.

Cain, C., “Suit Claims Invasion of Privacy,” detnews.com, 2001, available at http://www.detnews.com, last accessed 02/02/02.

Cha, A., “Retirement Plan Error Discloses Personal Data,” 2001, available at http://www.washingtonpost.com, last accessed 16/02/02.

Computer Economics, “Information Systems and E-Business Spending,” Carlsbad CA 92008, *Computer Economics*, 2001.

Davidson, S. J. and D. M. Bryant, "The right of privacy: International discord and the interface with intellectual property law," *Computer and Internet Lawyer*, 2001,18:11, pp. 1-13.

Dhillon, G. and T. Moores, "Internet Privacy: Interpreting Key Issues," *Information Resources Management Journal*, 2001, 14:4, pp. 33-37.

Dhillon, G. and S. Moores, "Computer crimes: theorizing about the enemy within." *Computers & Security*, 2001b, 20:8, pp. 715-723.

EPIC, “Child online protection act,” 1999, available at http://epic.org/free_speech/house_cda.htm

EPIC, “Electronic Privacy Information Center,” 2002, available at http://www.epic.org/, EPIC, last accessed 29/01/02.

EU. “EU Directive on Personal Data Protection Enters into Effect,” 1998, available at http://www.eurunion.org/, last accessed 21/5/01.

Federal Trade Commission, “Privacy Online: A report to congress,” 1998, available at http://www.ftc.gov/reports/privacy3/toc.htm, last accessed 16/02/02.

Federal Trade Commission, “FTC Announces Settlement With Bankrupt Website,” 2001.

Toysmart.com, “Regarding Alleged Privacy Policy Violations,” available at http://www.ftc.gov, last accessed 02/02/02.

Fonseca, B., "Blanket Insecurity." *Computerworld*, 2000, 24:4, p. 8.

Forder, J. and P. Quirk, *Electronic Commerce and the Law*, Brisbane, Wiley, 2001.

Gaskell, G., “Simplifying the onerous task of writing security policies,” 1st Australian Information Security Management Workshop, School of Computing & Mathematics, Deakin University, 2000.

Ghosh, A. K. and T. M. Swaminatha, "Software security and privacy risks in mobile e-commerce." *Communications of the ACM*, 2001,44:2, pp. 51-57.

Henderson, "Personal Information privacy: implications for MIS managers," *Information and Management*, 1999, 36, pp. 213-220.

Hopper, I., “Technology: Hotmail's subscriber information shared with public Internet directory,” 2001, available at http://archive.nandotimes.com/technology/story/, last accessed 02/02/2002.

Krebs, B., “UK Resident to name microsoft in FTC privacy complaint,” *newsytes,* 2001, available at http://www.newsbytes.com/news/, last accessed 16/02/02.

Leizerov, S., "Finding Privacy Abroad," *Intelligent Enterprise*, October2001, pp. 52-53.

Lemos, R. “Rental-car firm exceeding the privacy limit?” *CNET*, 2001, available at http://news.com.com/, last accessed 14/02/02.

Martin, D., “TiVo's Data Collection and Privacy Practices, Privacy Foundation,” 2001, available at http://www.privacyfoundation.org/privacywatch/, last accessed 16/02/02.

McCullach, D., “Prepaid Phones and Privacy too,” 2001, http://www.wired.com/news/politics/

Milberg, S., S. Burke, et al., "Values, personal information, privacy and regulatory approaches," *Communications of the ACM*, 1995, 38:12, pp. 65-74.

Milberg, S. J., H. J. Smith, et al., "Information privacy: Corporate management and national regulation," *Organization Science*, 2000, 11:1, pp. 35-57.

O'Harrow, R., “Eli Lilly has privacy lapse,” *Washington Post*, 2001, available at http://www.washingtonpost.com/ last accessed 21/01/2002.

O'Harrow, R., “Marketers May Face Student-Data Curbs Marketers May Face Student-Data Curbs,” *NewsBytes*, 2001, http://www.newsbytes.com/news/, last accessed 14/2/02.

P3P, “Platform for Privacy Preferences,” 2001, available at http://www.w3.org.

Parker, D. B., "A consistent definition of information security," *Communications of the ACM*, 2001, 44:6, pp. 12-13.

Pelofsky, J., “Privacy-US Wireless Firms Choose Opt-in to Protect Privacy,” Reuters, 2001, available at http://www.washtech.com/news/regulation/

Privacy Foundation, “Bugnosis: Web Bug Detector,” 2001, available at www.bugnosis.org, last accessed 12/02/2002

Privacy Foundation, “Connecting the Dots Between Public Records Databases,” 2001, available at http://www.privacyfoundation.org/commentary/

Privacy International, “Privacy International,” 2002, available at http://www.privacyinternational.org, last accessed 29/01/02.

Rimmer, S., “Death to Spam,” *Alchemy Mindworks*, 2002, available at http://www.mindworkshop.com, last accessed 12/11/02.

San Jose Mercury News, “State Sells Birth Data to Web Site, Raising Fears,”, 2001, available at http://nl4.newsbank.com/, last accessed 14/02/02.

Scheeres, J., “What the (Don't) know about you,” 2001, available at http://www.wired.com/news/privacy/, last accessed 16/02/02.

Schneider, M., “More amusement parks looking into surveillance technology since Sept. 11,” *Associated Press*, 2001, available at http://www.uniontrib.com/, last accessed 14/02/2002.

Spafford, E. H., “Are computer hacker break-ins ethical ?” *Computers, Ethics & Social Values*, D. G. Johnson and H. Nissenbaum, Prentice Hall, 1995, pp. 125-135.

Surveillance Camera Players, “Acting Out: They like to be watched,” 2001.

“Meet the surveillance camera players coming to a video monitor near you,” available at http://www.notbored.org/the-scp.html, last accessed 14/02/2002.

Surveillance Camera Players, “Nothing has changed, therefore everything must change,” 2001, available at http://www.notbored.org/change.html, last accessed 14/02/2002.

Thibodeau, P., "Europe's Privacy Laws may become a global standard," *Computerworld*, 2001, 77.

US Department of commerce, “Welcome to the safe harbor,” 1998, available at http://www.export.gov/safeharbor/, last accessed January 30th, 2002.

Weare, C. and W. Y. Lin, "Content analysis of the World Wide Web - Opportunities and challenges," *Social Science Computer Review*, 2000, 18:3, pp. 272-292.

Wolverton, T., “Egghead sale could crack on privacy issues,” 2001, available at http://news.com.com/, last accessed 14/02/02.

AUTHOR

Dr Sophie Cockcroft is a Lecturer in Information Systems and E-commerce at the UQ Business School. Before joining UQ she taught at the University of Otago in New Zealand and City University in Hong Kong. Her research interests include system development, data quality, security and privacy.