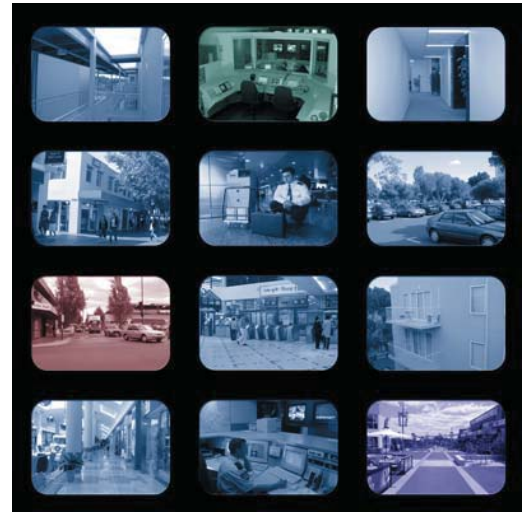


COVER STORY

Cover Story - Balancing Privacy, Security and Technology.

Faced with high levels of surveillance and an increasing need to identify ourselves as part of everyday transactions, we could be forgiven for thinking that it has become almost impossible to maintain our privacy. The rise in the use of surveillance technologies is generally justified by the need to maintain a safe society. Federal privacy commissioner Malcolm Crompton looks at the question of whether we can have a society that is safe and open, and still respects privacy.



Balancing Privacy, Security & Technology

Malcolm Crompton



The numbers of video cameras in any large city, the move to using credit cards for all purchases and the capacity and speed of databases can lead to the feeling that we are being watched and identified too often by too many people.

The reality is that we are being watched and have always been watched. The difference between now and 50 years ago is that these days, our details and/or images end up on databases or video libraries in the hands of people we probably do not know.

Faced with high levels of surveillance and an increasing need to identify ourselves as part of everyday transactions, we could be forgiven for thinking that it has become almost impossible to maintain our privacy.

The rise in the use of surveillance technologies is generally justified by the need to maintain a safe society. This change in our society raises the question of whether we can have a society that is safe and open, and still respects privacy.

One of the greatest concerns regarding the rise of the 'surveillance society' is that we are being increasingly identified as we come under greater surveillance. Surveillance does not have to be used in this way but it seems that many developers have given little attention to the impact of the technologies they implement on privacy.

Identity and new technologies

New technologies do not necessarily destroy privacy. They can be either privacy enhancing technologies (PETs) or privacy intrusive technologies (PITs), depending on how they are designed and the uses to which they are put.

Technologies have the potential to be more privacy invasive where they are used by organization to obtain large amounts of information about individuals which that organization may not need, or that the individual may not know about. Take for example, credit card companies. In the process of compiling your monthly account, a credit card company acquires information about where you have shopped, what you have purchased, how much you paid and when you bought it. This can distort the balance between individual privacy and other social needs.

There are a number of technological developments which are relevant to the debate about the rise of the surveillance society and the push to identify people more often.

These technologies include:

- biometrics
- tracking and monitoring technologies
- data mining
- electronic transactions
- encryption and digital signatures

Technological developments often indirectly impact on the identification of individuals.

“Transactions that were once anonymous are now becoming increasingly identifiable as more information can be gathered, collated and linked to an individual.”

However, in many cases, this increased capacity to identify people is simply an artifact of another process. For example, most people do not realize that a mobile phone can also be a persistent and accurate location tracking device.

Numerous biometric technologies using fingerprints, hand geometry, face recognition, voice recognition, iris and retinal scanning, keystroke recognition and DNA are currently in development. These digitized measures of biological data have the potential to create powerful authentication and identification tools. However, systems designed to generate a unique biometric identifier for use in a whole range of different contexts can raise significant privacy risks. Alternatively, they can be designed to operate in a privacy protecting manner.

Tracking and monitoring technologies cover a wide variety of systems ranging from increasingly sensitive video and audio surveillance tools, through to tracking the movement of mobile phones in real space and online interactions in virtual space. These have the potential to reduce the scope for anonymity as more individuals are increasingly under the gaze of others.

Data mining involves the use of generic algorithms to optimise searching and combine information on different databases and generate new information in the process, including identification of de-identified information.

One of the impacts of new technologies has been a loss of anonymity in many transactions which are now conducted electronically. Many of our electronic transactions, as currently designed, leave digital trails.

Transactions that were once anonymous are

now becoming increasingly identifiable as more information can be gathered, collated and linked to an individual. Despite this tendency, loss of anonymity is not inevitable. The technology exists to conduct anonymous or near anonymous electronic transactions and much work is going into develop these alternatives.

Cryptographic tools and asymmetric encryption systems such as public key

technology allow for more security in electronic transactions.

Public Key Infrastructure is a system designed to enable the widespread and open use of public key certificates. It can be used to deliver a number of goals:

- Authentication of the identity of a subscriber in online transactions can be achieved by the subscriber ‘signing’ an electronic communication with their private key.
- The integrity of the message can be checked. Where a subscriber signs an electronic document a message digest or hash of the message is produced. If the hash value remains the same after the message has been received then the message has not been altered in transit.
- Non-repudiation can be achieved. Where an electronic message is signed with a digital signature, the fact that it was signed with a

particular key cannot be repudiated or denied. In practice, this amounts to strong evidence that the message was signed by the rightful owner of the private key.

- Confidentiality of messages can be assured. A message encrypted with a subscriber’s public key can only be decrypted with that same subscriber’s private key.

Three of these elements, authentication, integrity, and confidentiality, are particularly pertinent to privacy protection.

Technologies relevant to identification could potentially be privacy enhancing technologies (PETs) or privacy intrusive technologies (PITs). Whether a technology is a PIT or a PET depends not only on how it operates, but also on how it is structured. One key factor is whether or not it involves the collection of unnecessary information, including a greater degree of identifying content than required for the system to function.

An individual’s identity need not be disclosed for all transactions. For example, when we pay for goods with cash, we often leave no identifying details. One way to protect privacy is to introduce an ‘identity protector’ and use encryption and digital pseudonyms to separate an individual’s true identity from the details of one’s transactions and communications. This would result in a significant reduction in the collection of identifiable information and therefore enhance the protection of privacy.

Systems that involve the use of a single identifier for each individual which is linked to a single set of demographic and identifying



In many major cities, trained surveillance operators monitor crowds with a view to reducing crime.

information that is used in a wide range of situations have the strong potential to be privacy invasive. This was the basis of the infamous 'Australia Card' proposal in the late 1980's.

More recently, in 2001 the Malaysian government began issuing a multi-application ID card. The card has an embedded microchip and is used as a national identity card, driver's license, passport and electronic purse. Plans for additional applications include using it to withdraw cash from automated teller machines and storing health and immigration information. The cards have been criticised by consumer associations concerned that they make individual's personal and confidential information too vulnerable. The extensive linking of information has the capacity to significantly intrude on a citizen's privacy. The extent to which it does would depend on how it operates in practice, and what protections exist technologically and in law against misuse and abuse.

Another PIT is the use of fingerprint scanning technology to purchase groceries. A system called SecureTouch-n-pay developed by Biometric Access Corporation has reportedly been introduced into Kroger convenience stores in the USA. To enroll in the systems, customers must show a Kroger representative their driver's license and a credit card and have their fingerprints recorded. Customers then present their fingerprint and a PIN (typically their phone number) in place of a card payment at the check-out to validate their payment. This system appears to require a disproportionate level of identification for such a simple, and potentially anonymous, transaction as purchasing groceries.

A technology on the drawing board that also carries the risk of tracking individuals through their grocery purchases is the replacement of bar codes with microchips and radio transmitters. This has significant potential to improve distribution mechanisms for goods and to speed up grocery check-outs. It also carries a privacy risk that goods could be tracked from the manufacturer all the way to the individual consumer's home. In the development and design of new technologies, considerations need to be given not just to the intended uses of a product, but also potential unintended consequences that may adversely affect an individual's privacy. The intended effects in this case may greatly improve distribution networks and enable enhanced stocktaking. The unintended effects could involve tracking

individual consumers and collection of information on individual purchases if linked to identifiable payment options.

Of course, some privacy intrusive technologies are specifically designed that way, for example Spyware products. An example is iSpyNow, a computer monitoring product that allows for remote monitoring of another user. It logs all websites visited, logs both sides of chat conversations, captures information on every window the individual interacts with, tracks

A technology on the drawing board that also carries the risk of tracking individuals through their grocery purchases is the replacement of bar codes with microchips and radio transmitters.

every application executed, captures text and images sent to a clipboard and tracks all keystrokes. It is installed by sending it as an email attachment to the user to be monitored and is designed to be undetectable.

In contrast, PETs have the potential to bring enhanced trust by bringing individual permission and control into the equation. Information technology companies are currently investing considerable resources in developing new technologies which aim to provide the necessary functionality while protecting privacy.

Technological means to protect privacy can involve restricting access to personal information or the development of systems that provide the necessary functioning without needing to reveal personal information. For example, the cryptographic encoding of communications using public key infrastructure and digital signatures, or systems that simply do not generate unnecessary personal information in the first place, illustrate how technological design can enhance privacy. Software tools that specify, and even automatically apply, the privacy preferences of individuals illustrate another kind of technological privacy protection.

One new technology which claims to be a PET is idemix developed by IBM. Idemix stands for 'identity mixer'. This enhanced public key technology tool claims to provide authentication functionality without revealing an individual's identity. In the idemix system, organisations only know users by their

pseudonyms. The user can have a different pseudonym for each organisation and these different pseudonyms cannot be linked. A key part of idemix is a 'pseudonym authority' which users can access easily and which grants users 'pseudonym credentials'. The system comes with other important controls, including prevention of re-use of information and self-destruction of the data on misuse.

This system and others like it allow for 'pseudonymity' rather than anonymity. In many cases total anonymity may not be appropriate. If the identification of the individual is necessary and appropriately authorised, for example in an investigation of fraud, the pseudonym authority can uncover the individual user's identity.

Biometric encryption is another new technology with the potential to enhance privacy protection. However, biometrics also have the potential to erode privacy, depending on how it is implemented. One privacy enhancing implementation of biometric encryption uses a person's biometric such as a finger print pattern or iris scan and uses it as part of an encryption algorithm to encrypt a PIN number. The finger print pattern is not stored and the PIN number cannot be decoded without your live finger print pattern. Only the individual with a particular biometric can gain access to an account or computer system. With this system, the biometric cannot be used as a universal identifier as it is used to encrypt a different number or alphanumeric for each application. There is not one single link as each encryption is different and cannot be matched.

The availability of such technologies alone is not sufficient to ensure that system designers choose PETs over PITs. The technology for digital cash and other anonymous and pseudo-anonymous online payment systems has been available for some years, but has not been widely implemented. While there may be other factors to account for this, one factor may be that existing online credit card payment systems also provide the vendor a rich source of personal information about the purchaser. Market pressures are an important factor to address in promoting the development of adequate privacy protection in the context of new technologies.

The Market and identity

There are a range of competing commercial pressures relevant to identification and privacy and new technologies. These include

- Levels of identification needed for commercial

transactions

- The trend towards market customisation and customer profiling
- The marketing benefit of privacy protective customer management
- Pricing mechanisms

There is some commercial pressure to increase capacity of organisations to collect information about individuals. However, in most commercial transactions the identity of an individual consumer is actually less important than other assertions the individual may make.

“Software tools that specify, and even automatically apply, the privacy preferences of individuals illustrate another kind of technological privacy protection.”

In most commercial transactions the customer's claim to provide a consideration of a particular value is more important than their identity. This may involve counting the cash offered for payment, or checking the receipt of the item returned for refund or exchange.

In other cases, the important assertion a person may make about themselves is that they have a particular attribute, for example the individual is a licensed builder and therefore entitled to the trade discount. Here again, it is not the individual's identity as such, but rather the fact that they have the required attribute which is at issue.

Consumer identity will be relevant to some commercial transactions where the consumer is undertaking to provide a guarantee or perform a function specific to that person, such as collect a credit card. For the majority of cases identity is actually not required.

However, there are commercial pressures to collect identifying information to enable closely targeted marketing and customer profiling. Customer profiling can improve the personalisation of customer services and increase marketing efficiency and significantly reduce advertising costs. This can involve some confusion of purpose. Consumer research indicates that most users prefer to give out only information needed for a transaction.

Identified information is often collected in the form of loyalty schemes and competition entries. The stated need for identity information may

refer to distribution of prizes, but the company's intended purpose is often to use the identified information for marketing purposes. This kind of mismatch between consumer and business expectations can lead to a breach of customer trust. On the other hand, customer relations management undertaken openly, with the agreement of the customer and under the customers control can, and has, markedly increased levels of trust between the customer and the vendor.

Retaining the consumer's trust is a key element in business to customer relations and

an important market consideration. The importance of privacy to levels of consumer trust in electronic commerce has been one of the drivers to the development of the P3P technology which allows computer readable privacy policies. Some industry players have adopted privacy protection as a critical business practice in response to the levels of public concern about privacy.

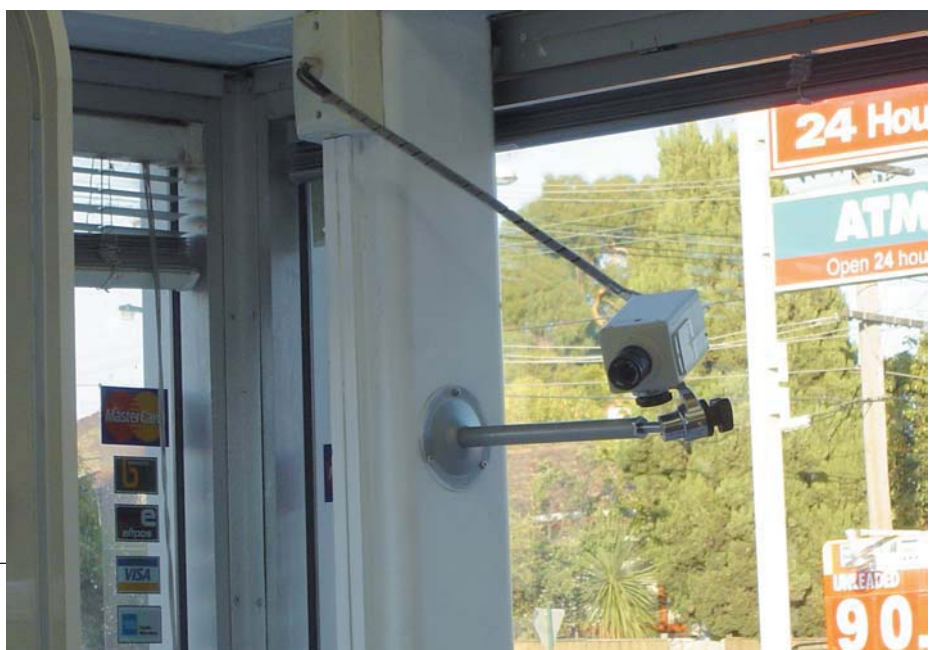
Market pressures include not only consumer demand and preferences, but also pricing mechanisms. Pricing mechanisms can also be an effective influence on the role of the market in respect to privacy. One example is the prevalence of spam in email platforms compared to mobile

phone text messaging ('SMS'). The cost of sending huge volumes of unsolicited email marketing messages is very low. As a result, email spam is a significant problem worldwide.

In contrast, the level of SMS spam is relatively low in Australia. This could largely be attributed to the pricing mechanism. In this country, mobile phone text messaging was established on a pay-to-send basis. According, it is not commercially viable to send the same volume of SMS advertising messages as in some other countries. In contrast, SMS spam is a significant problem in Japan which has a network architecture that allows spammers to use IP based services to send out bulk text messages that cost little or nothing. Under this system the customer pays for all the data they receive, including spam.

Market pressures can promote both privacy enhancement and privacy intrusion. It will not be sufficient to leave privacy protection to the market, as there are too many areas where the privacy impact of different choices is not transparent. In many cases, consumers are unaware of the impact some industry practices have on their privacy and so cannot influence company behaviour through the marketplace.

The lack of information individuals may have about business information handling practices is a classic case of market failure. Laws are needed to enable individuals to make privacy choices where the market alone may not. Effective privacy protection also relies on the role of law to address broad public policy considerations.



The use of CCTV in shopping centres, service stations and office complexes means that the average person now has their image captured over 300 times per day.

Finding a new balance

Privacy laws are necessary to provide an incentive for technological developments to enhance privacy. In a democratic society, the law is required to establish the public policy objectives that the market alone will not provide. Equally the opposite applies. Law that ignores the realities of marketplace and technological development will have little impact.

A debate is needed to challenge the public and private sector organisations that wish to collect more, not less, identifiable information. The benefits of collecting less identified information need to be understood and organisations will come to realise that identifiable information is not always necessary for their activities, especially if market forces in the form of consumer responses tell them this.

Greater public awareness is needed about the benefits that can be had through the use of anonymous technologies. The assumption that you can have privacy for yourself and deny, or fail to protect, the privacy of others needs to be contested.

Finding a new balance will require organisations to carefully examine when an individual's identity is really required for the operation of various processes within an information system. In the design of any new information system, the collection and retention of identifiable personal information should be minimised. Information systems should be transparent and provide individuals with the ability to control the disclosure of their personal information. Individuals must be able to decide for themselves whether or not their identity is to be revealed or maintained in an information system. Effort should be made to promote greater public awareness of privacy-enhancing technologies. The use of privacy technologies by public and private sector organisations should be also encouraged.

The law alone cannot ensure the right balance. Privacy laws need to be in the form of general principles, as information handling is highly contextual. This can create a significant margin for interpretation and implementation. Privacy laws are also necessarily confined to each jurisdiction, while new technological developments are leading to trans-border information processing and an increase in international flows of personal information.

Moreover, a law in itself cannot ensure the existence of technological capacity necessary to enable privacy protections.

Law has the potential to both promote or to stifle technological creativity. The law is most at risk of stifling technological solutions when it attempts to mandate some technological approaches in favour of others. The interaction of the market and technological developments is likely to be needed to provide for technological tools that can protect privacy. If we can get the balance right there is enormous potential to harness the power of the market and technological developments to ensure that privacy rights are protected into the future.

The law must be flexible enough to recognise and promote privacy enhancing technologies and market initiatives, while still ensuring that adequate privacy protections are in place.

“The law alone cannot ensure the right balance.”

Conclusion

Every human born needs privacy. To grow and develop, individuals must have some opportunity to escape being under the gaze. Our freedom will be restricted in a society that does not allow individuals to make some choices between anonymity and responsible participation in society.

Technological changes have tended to

distort the right balance between privacy protections and other interests. However, new developments in information technology need not be privacy intrusive. When designed and used appropriately they can be privacy enhancing.

Technologies with one unique identifier, used in a whole range of contexts, which link all that information, create significant privacy risks. Identity authentication systems that do not require the authenticating body to hold large amounts of information about an individual, where the individual knowingly exercises a choice to enroll in the system, pose less risk.

In finding an appropriate balance between privacy and accountability, it is necessary to distinguish between circumstances where identification is required and those where some other form of authorisation is needed. An important key in developing PETs will be determining when knowledge of a person's identity is necessary and when it is not, and then building systems that can separate the two.

The challenge is to ensure that privacy is designed into new technologies. Privacy is fundamental to human dignity. We can and must find a way to protect privacy rights in the new technological environment. New technologies greatly enhance the availability and accessibility of information and the possibilities for communication. New technologies could also enable new ways to have privacy, freedom and choice. The challenge is to make that happen. ■

The deployment of CCTV surveillance public areas has given rise to heated debate regarding the boundaries between privacy and security.

