

# **The Value of Privacy**

*a Law Week 2006 address by*

Paul Chadwick

Victorian Privacy Commissioner

State Library of Victoria

23 May 2006

## Privacy, the quietest of our freedoms

Privacy is the quietest of our freedoms. We need to listen for it with care. Privacy is easily drowned out in public policy debates.

It is confronting but accurate, in my experience, to say that privacy is best measured as it drains away. Privacy is most appreciated in its absence, not its presence.

Consider the following practical illustration. You take the privacy of your home for granted — until you discover that a neighbour has trained a camera on your bedroom window. After a burglary, feeling violated by the knowledge that a stranger has been through your love letters, your underwear drawer — it is then that you most appreciate the usually abstract notion of privacy. As the songwriter put it: You don't know what you got 'til it's gone.<sup>1</sup>

This feature of privacy creates a dilemma for privacy commissioners, who have a statutory function to promote understanding and awareness of privacy in our technological age. We have to make a choice. Should we be a permanent warning system, and wail away constantly about the multiple threats to privacy? It would not be difficult. The threats are everywhere, and generalised fear is easier to evoke than purposeful hope (as the tactics of politicians and the media on other topics frequently demonstrate).

Or should privacy commissioners choose the subtler option? This requires us to be imaginative in reaffirming the value of privacy in society; to make as vivid as we can the usefulness of the concept of privacy in everyday life, so that our listeners are persuaded that, yes, privacy does always need to be respected at the same time as we extract the benefits from new technologies that offer so much. In these past five years as Victoria's first privacy commissioner, I have consciously pursued this second approach, for three primary practical reasons.

---

<sup>1</sup> Joni Mitchell, *Big Yellow Taxi*. See also the testimony of another famous songwriter: 'After a while you learn that privacy is something you can sell, but you can't buy it back' (Bob Dylan, *Chronicles, Vol I* (2004, Simon and Schuster, New York) pp 117-18.

First, as we all know, if a siren wails constantly it ceases to have any warning effect at all. It becomes an irritating part of background noise, to be blocked out as we focus our concentration elsewhere. Second, I think we can see practical examples all around us of the value of privacy in everyday life. It is an accepted, traditional social value. It is not some novel radical cause straining to get itself accepted by a sufficient majority. It is ancient, and its long pedigree can serve a privacy commissioner well.

The radicals are those who, grasping at what may be transient factors created by the political or technological environment, would trade away too much of a value that has endured for good reason.

I have a third reason for choosing to lay emphasis on privacy as an everyday social convention, as a manifestation of common decency that happens now to be taking new legal forms. The third reason is related to the feature I mentioned at the outset of this talk: privacy is best appreciated in its absence. It is unwise to rely heavily on the technique of evoking fear of loss of privacy, because the point of the warning is usually understood only when it is too late for it to make any practical difference. By then, another part of privacy has gone. When this realisation dawns, it can produce a mixture of ennui and sullen acquiescence that is unhealthy in any polity.

I hope that by now you are wondering why I am laying out in such detail my approach to this aspect of my statutory role. It is to underline the significance of what will follow in the rest of this talk.

Today, I am deliberately changing the approach, fully aware of the risks of doing so.

This talk is intended to be taken as a warning. It is intended to create in you a certain sense of unease, of prudent wariness.

Do you want to live in a society such as the one that is likely to result from what I am about to describe? If not, start to think about what reasonable compromises, what balances, could avoid it.

The warning is in two parts –

- The aspect of privacy known as anonymity in a crowd is dying, draining away, and to fail to debate the implications puts in peril other aspects of freedom besides privacy.
- Unless we analyse critically the increasingly common phrase ‘nothing to hide, nothing to fear’ we recklessly ignore history’s lessons.

Before I explain, I must set out what is at stake. Why should you take notice of any warning if the cost of ignoring it is perceived by you to be inconsequential? I need to set out the purposes of privacy in all our lives. What follows is just a sketch made from a vast trove of works in a range of disciplines.

## **Purposes of privacy**

Basically, privacy serves three essential purposes for those who value human dignity and flourishing.

### ***Individuality***

Privacy is essential to our sense of self. We have a conversation with ourselves in our heads, then we speak and act among others. By being allowed privacy, we can create and restore our individual self.

At its most elemental, privacy permits and sustains individuality. Can you hear a note struck inside you by the words of one scholar [augmented to include us all]? –

The man [or woman] who is compelled to live every minute of his [or her] life among others, and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his [or her] individuality and human dignity. Such an individual merges with the mass. His [or her] opinions, being public, tend never to be different. His [or her]

aspirations, being known, tend always to be conventionally accepted ones. His [or her] feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man [or woman]. Such a being... is not an individual.<sup>2</sup>

### ***Intimacy***

Without privacy, there cannot be intimacy between individuals. We create intimacy partly by giving away some of our privacy freely to those we regard as close to us. They might be a partner in a relationship, a family member or a friend. The closeness of the relationship determines how much we say to them of our inner worries and hopes, or how much we relax and just “be ourselves” in their company. In this sense, privacy calibrates social relationships.

In the security of a trusting relationship, we often ‘think aloud’, putting on hold our sense of reserve. In relationships, privacy becomes shared, no longer associated only with solitude. But common to privacy in each of these settings — individuality and relationships — is the importance of control. We reveal and share of ourselves as we choose. The essence of feelings of indignity and humiliation resulting from breach of privacy is very often a feeling of loss of control.

### ***Liberty***

Privacy is also essential to liberty. Here, the value of privacy goes wider than individuals alone or in intimate relationships. Privacy is an instrumental freedom. Unless privacy is respected, particularly by governments, it can be difficult to exercise the various freedoms that have come to comprise liberty in our times. This is partly why a right to privacy is to be found in all the leading human rights instruments, including the *Charter of Human Rights and Responsibilities Bill 2006* currently before the Victorian Parliament.

---

<sup>2</sup> Edward Bloustein, cited in Thomas I Emerson’s *The System of Freedom of Expression*, at 546.

Freedom of belief or of conscience means little without privacy for prayer, contemplation, exchanges among believers, and formal worship.

Freedom of association, at a practical level, requires respect for privacy while those who wish to associate together support each other and plan actions to advance peacefully their common cause.

Privacy is a pre-condition to freedom of expression. Authors consult, compose, draft, rethink, re-draft — all *before* they publish. The basis of longstanding legal rules protecting the privacy of a person's papers and communications is the recognition that if you can deny a person this privacy you can deny them capacity to express themselves to others and to associate with others.

In practice, privacy in society cannot be absolute. Other values, including security, compete with liberty and its component parts, of which privacy is one. Compromises are made.

The legitimacy of the compromises depends partly on the integrity and transparency of the process through which the compromises are reached, partly on the legitimacy of the authority that decides the final shape of the compromise, and partly on the accountability of those who exercise new powers that curtail privacy.

Technology is making the work of settling and explaining those compromises more complex. Privacy issues arise in a great variety of settings. Let me give some examples:

**1 Identity verification** – If your government requires you, in effect, to have a smartcard, which bits of your personal information ought to be on it? Who will have access? What for? Australia's privacy laws developed out of the Australia Card proposal in the 1980s, which resulted in the compromise of a tax file number, strict limits on its uses, and data-matching legislation. Up-to-date privacy safeguards are even more necessary now because of changes since the Eighties, including –

- *new technologies* that make collecting, storing, sifting, matching, linking and sharing data easier and faster. For example, large collections of photos can be linked to surveillance camera networks and software to recognise and track individuals, (of which more later)
- *new powers* for information gathering given to government agencies by parliaments concerned about crime and terrorism
- *new information*, for example, data extracted from human DNA to determine or predict parentage, health and ethnicity. Data is now routinely generated about the users of many post-1980s goods and services that rely on digital technologies. In Australia, e-mail accounts, mobile phones and tollways are examples.

All this inevitably involves weighing benefits and risks, facilitating informed debate, crafting careful checks and balances, and encouraging periodic review.

Any government that wants to issue a unique identification number to most of the population and then to compile and link information about them using increasingly powerful technology bears a heavy onus to justify its case. To assist public understanding, I have issued a Smartcard Privacy Checklist of 20 questions that can reasonably be asked of any government.<sup>3</sup> Satisfactory answers would be a practical start to government's discharge of the onus.

**2 Anti-terrorism measures** – How does a liberal democracy manage risk and fear without transforming itself? How are we to avoid a society in which, as one scholar put it, 'all are safe but none is free'?<sup>4</sup>

---

<sup>3</sup> Issued 14 May 2006 and available at [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au), go to Publications, then Media Releases.

<sup>4</sup> Herbert L. Packer, *The Limits of the Criminal Sanction* (Stanford University Press, 1969) p 65. Materials specific to balancing liberty and security in the context of terrorism can be found in two submissions to the Victorian Parliament's Scrutiny of Acts and Regulations Committee on Victoria's *Terrorism (Community Protection)* legislation in 2003 and 2006, both at [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au), go to Submissions.

**3 Internet browsing** – Are your tracks in cyberspace private like, say, your library borrowing records?<sup>5</sup>

**4 Criminal justice** – How, if at all, should information be an instrument of punishment?<sup>6</sup> What are the implications of a judge’s implicit statement: “I sentence you to be Googled, forever.” Is vigilantism an inevitable consequence of open justice, powerful search engines and the worldwide web? Are the media legitimate participants in the corrections system?<sup>7</sup> Ought journalists, unconstrained as they are by due process, adopt the function of placing individuals in a ‘digital pillory’? Ought journalists systematically brand persons in cyberspace forever just as, in earlier times, a hot iron would brand forever a person’s body, marking him or her in a way that was impossible to expunge or live down?

**5 Genetic data** – The great achievement of sequencing the human genome means that we must learn to deal with an unfamiliar concept: shared bodily privacy. Your genetic data says much about you *and* your blood relatives. Who is to control it? Is there a right not to know the predictive information that your DNA or your relative’s DNA may contain?

**6 Mining data, and making inferences with consequences** – Although it may seem counter intuitive to many, part of the value of privacy is the role it plays in ensuring the circumstances necessary to the proper practice of journalism in a free society. The right to privacy appears in the basic human rights instruments alongside other rights that are also of critical significance to the practice of journalism. These rights mutually support one another.<sup>8</sup> Privacy rights are essential to the practice of journalism. As journalists go about their work of cultivating and protecting

---

<sup>5</sup> <http://www.smh.com.au/news/breaking/google-asked-to-hand-over-search-records/2>

<sup>6</sup> For a recent treatment from a philosophical perspective, see Martha Nussbaum, *Hiding from Humanity – disgust, shame and the law* (Princeton, 2004), in particular chapters 4-6.

<sup>7</sup> To avoid misunderstandings, I emphasise that the legitimate role of the media in the proper working of the open justice principle remains vital. It includes fair and accurate reporting of court proceedings and criticism, on facts fairly and accurately stated, of court decisions. It does not legitimately involve the augmentation by media of criminal sanctions imposed by courts after due process.

<sup>8</sup> This general point holds, notwithstanding the fact that in particular cases two rights may compete and a choice must be made. For details, see ‘Privacy and Media – subtle compatibility – five categories of fame’, Proceedings of the 26<sup>th</sup> International Conference on Privacy and Data Protection, Wroclaw, Poland, September 2004 (available at [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au), go to Speeches)

confidential sources; of charting and reporting new ideas and dissenting views that test our orthodoxies; and of chronicling the formation of new political movements and parties, or of machinations in existing ones — as they do all this, journalists rarely reflect on the background role of the right to privacy.

But readers of history as well as observers of contemporary events will attest that when freedom begins to wane, journalists are among the first to lose their privacy. More from history later. First, a current illustration.

You may have seen recent reports from the United States that the National Security Agency (NSA) has collected a vast amount of records from telecommunications companies about phone calls and e-mails made and received within the US by millions of Americans. This disclosure adds to reports in December 2005 that the NSA had eavesdropped, without judicial warrant, on international calls to and from the US. The latest reports suggest that the NSA has not listened to the content of all the calls, but instead has amassed an enormous amount of data showing which phone numbers called which other numbers, and the dates and times of the calls. Linking phone numbers to the individuals associated with those accounts is not difficult. By applying the power of computers and pattern recognition software to this data, it is possible to work out, or to infer, who has called whom, and when. Data mining e-mails produces potentially richer data. In response to these disclosures, journalists in the US have expressed concern that government mining of their records may disclose their confidential sources. Similar questions arise about the privacy of activities of Members of Congress and their staff, and those in civil society organisations who from time to time may oppose government policies or seek to have them changed.

Let us leave to one side the issue of whether it would be lawful, without judicial warrant, for the phone companies to provide the data of millions of Americans to the US Government's technologically sophisticated spy agency. We will also pass over the issue of whether it would be lawful for the NSA to collect and process that data as

reported. Court proceedings have been instituted into those matters and we must await the results.<sup>9</sup>

Let us also leave to one side the obvious question whether Australian telecommunications companies and government agencies engage in similar activity, with or without judicial oversight. We may reasonably expect that local journalists will eventually ask these questions and report to the public the answers given by the relevant accountable persons. Depending on the answers, legal processes may ensue here too.

Leave all that aside. Turn your thoughts instead to the implications for privacy of such practices if they were to become widespread. We leave vast amounts of data behind us as we use many of today's technologies: ATMs; credit cards; loyalty programs run by airlines, retailers and many others; new types of ticketing; GPS-equipped vehicles; consumer items with RFID chips embedded in them; and our mobile phones. In the near future, it would seem, a government-issued smartcard, with its substantial supporting databases, will add to the amount of data collected and/or processed about most Australians.

Who is to have access to the various datasets listed above? How are they to be authorised to sift it for the facts — or inferences — that the data may seem to reveal about how we live our lives? Will we know it happens? Who will test the accuracy? Can we see the data about us, and the conclusions about us that may be drawn from the data? May we appeal the consequences of the decisions made on the basis of those conclusions?

These are some of the questions for a future in which we attempt to balance liberty, efficiency and security. They are not questions solely about the quantity of our privacy. They are questions about the quality of our freedom.

---

<sup>9</sup> The legal documents from the incomplete proceedings in the District Court, Northern District of California (No. C-06-0672-JCS) are available at [www.eff.org](http://www.eff.org)

If privacy is to be preserved for Australian society in practice as well as in theory, in fact as well as in spin, then these kinds of questions will need to be precisely formulated in plain language and pressed with persistence on the proper authorities in the many diverse contexts in which they arise. Responses will need to be openly debated. The inevitable compromises will need to be passed into laws of adequate detail through due process by authorities that are legitimate. Those who administer the compromises will have to be able to be held accountable under law in the open. Those who do the oversight (including, in their small way, privacy commissioners) will also have to be overseen by parliaments and media. In holding power to account, disclosure is always the final safeguard.

## **Cameras that communicate and think – the end of anonymity in a crowd**

In his 1969 Boyer Lectures<sup>10</sup>, Sir Zelman Cowen summarised what the claim to privacy protected. You will recognise some of the elements from my earlier summary of the purposes of privacy. Sir Zelman said privacy protects –

- an individual's solitude,
- intimacy in relationships of the individual's own choosing,
- reserve, the shutting off from unwanted intrusion,
- anonymity, the ability to be lost, without identification, in a crowd.

I believe that, almost 40 years on, the last of these — anonymity in a crowd — is dying. It is draining away quickest in crowded places in urban and suburban areas, but the trickle has begun in most places.

Our gradual loss of this aspect of our privacy is the result of several factors, which are developing at speed. The consequences for privacy and, more broadly, for other aspects of liberty, are very significant, depending on the way our society handles this trend.

---

<sup>10</sup> 'The Private Man' (1969, Australian Broadcasting Commission)

The factors are –

- *Proliferation of surveillance cameras*, which are becoming cheaper, smaller and better at watching and remembering;
- *Networking of surveillance cameras*, so that these more numerous and more sophisticated individual cameras can be co-ordinated;
- *‘Cameras that think’* — that is, the linking of these networks of cameras to software that processes what the cameras see and provides additional information. Examples include:

- Facial recognition technology, with which the faces of the people on camera in real time — say, in the crowd at the football or in a train carriage — are compared with still photos held in a database in order to try to identify persons of interest.

- Automated Number Plate Recognition (ANPR) technology, with which the registration numbers of cars that pass the cameras are ‘read’ at high speed and reported back for matching against the data of the roads authorities to check whether the persons associated with the vehicles — say, the registered owner or licensed driver - are of interest. Perhaps, if they have outstanding fines, police on patrol further up the road will be contacted to intercept the vehicle.

- Behaviour prediction technology, which, according to its purveyors, is software that compares the behaviour of the persons under the eye of the cameras with pre-programmed behaviors that are thought to lead to adverse consequences, such as vandalism or other anti-social behavior. If it ‘foresees’ trouble, the system may alert the human operator. Naturally, such a system relies on judgments about what appearances and behaviors to pre-program. This raises the distinct prospect, not just of computer error, of wasted operator effort and of inconvenienced or humiliated members of the public. It also allows for discriminatory programming that targets particular types of person.

These three developments – facial recognition, numberplate recognition and behaviour prediction — have been introduced, or tested, or mooted here in Australia. They tend to be more developed in the United Kingdom, where surveillance cameras are numerous. So it may be useful to consider a recent UK development which, to my knowledge, has not yet been proposed for Australia. It involves a dramatic extension of the concept we know in Australia as Neighbourhood Watch. In Shoreditch, England, members of the community have been encouraged to take up an offer that appears to involve the provision of an enhanced TV service, one channel of which would be a live feed from the network of surveillance cameras in the local area. The public is encouraged to watch the channel and report anything they regard as suspicious. As one commentator observed, this is a paradise for ‘curtain twitchers’. Were such a development to become established in Australia, it would mark a significant step towards a surveillance society, and we would have to learn to balance any claimed benefits with the kinds of corrosive effects on civil society that can be discerned in the studies of communities in which spying and informing have been encouraged in the past.<sup>11</sup>

One other factor should be noted. The technologies of surveillance are naturally a growing area of the ‘information economy’. Significant investments have been made in devising and marketing these products, and in installing and maintaining them. Governments are natural customers. Not only are they responsible for public safety, but they are also able to control the statutes that govern use of the surveillance technologies. This market force should not be neglected. Generally speaking, government bureaucracies make good customers because they tend to place large orders and to operate with comparatively weak accountability to ‘shareholders’.

The Council of Australian Governments (COAG) consists of the Prime Minister, the Premiers and the Chief Ministers of the Territories. COAG is in the process of

---

<sup>11</sup> For the relatively recent example of East Germany prior to 1989, see Anna Funder’s *Stasiland* (Text Publishing, 2002), in particular chapter 6 for a summary of the extent of community informer networks and, in passing, an illustration of the potential of state-issued identity papers to be a focus for the setting of limits, both by the state on the citizenry and by citizens, through resistance, on the state.

developing a national framework for Closed Circuit TV (CCTV), that is, surveillance cameras.<sup>12</sup> COAG's relevant communiqué from September 2005 states in part –

*COAG agreed that each jurisdiction would undertake and share across governments a review of the functionality, location, coverage and operability of mass passenger transport sector CCTV systems. This will be a first step towards a broader consideration of the use of CCTV in support of counter-terrorism arrangements. COAG also agreed to a national risk-based approach to enhancing the use of CCTV for counter-terrorism purposes, including the development of a National Code of Practice for CCTV systems for the mass passenger transport sector. The Code will set a policy framework, objectives, protocols and minimum requirements for the use of CCTV systems to enhance counter-terrorism arrangements so that future investment is based on appropriate risk analysis. It will also contain agreed requirements for fixed and mobile CCTV systems, and national guidelines for the collection, storage, access, use, privacy, disclosure, protection and retention of CCTV information. The Code will allow each jurisdiction to determine its own CCTV requirements having regard to the use of CCTV for local counter-terrorism purposes....COAG agreed to identify necessary legislative measures to ensure consistent implementation of the Code, and to work cooperatively in research, development, trial and evaluation of new CCTV technologies.*

It will be apparent from the factors I have listed above and from COAG's statement that the governments of Australia are collectively preparing to improve, through the use of increasingly powerful technologies, their surveillance of the public. The stated purpose is to counter terrorism. Experience suggests that surveillance for other purposes will soon follow, a process known as 'function creep'.

It is the function of a privacy commissioner to monitor, assess, advise and make public statements on matters affecting privacy. I believe that it is my duty to warn

---

<sup>12</sup> Communiqué, Special COAG Meeting on Counter-Terrorism, 27 September 2005. Concurrently, COAG is preparing a National Identity Security Strategy, aspects of which are likely in due course to be relevant both to the smartcard and the CCTV framework.

now that a significant part of what has been understood to comprise privacy is likely to wither as a result of a mixture of: swiftly improving surveillance technologies; marketing to governments already made receptive by current security and ‘identity management’ issues; limited media scrutiny; and lack of informed public awareness. The intended and unintended consequences will be difficult to handle unless scrutiny, awareness and debate improve quickly.

If Australia is to continue towards becoming a surveillance society, but wants to remain a democratic society in which certain basic freedoms including privacy weigh meaningfully in the balance, then it is essential that the process on which all governments, through COAG, are embarked be the subject of informed consultation, open debate, due process in law-making and independent oversight of the balances duly enacted.

Failure adequately to honour one or more of these democratic safeguards — openness, due process, independent oversight — has been one of the striking characteristics of several governments’ actions taken under the heading ‘counter-terrorism’ since 11 September 2001. For example, the suddenness, secrecy and inadequate process that accompanied the round of anti-terrorism legislation that emerged from the COAG meeting of 27 September 2005 was, considering what was at stake, the single most serious failure of the deliberative democratic process in Australia<sup>13</sup> that I have witnessed in almost 30 years of reporting on and participating in public affairs.

It is imperative that we do better as Australia addresses the extent to which we are to empower and equip government bureaucracies and their contracted service providers to use the new technologies of surveillance.

---

<sup>13</sup> The inadequacies included: lack of notice; narrow consultation within government; failure to provide details for public debate among relevant specialists in law and academia as well as community organisations (until the Chief Minister of the ACT breached protocol and unilaterally made draft legislation public); truncated parliamentary processes; official enquiries that enquired and reported *after*, not before, parliament made major legislative change directly relevant to the subject-matter of the enquiries. The subject matter involved fundamental re-balancing of liberty and security in favor of security (preventative detention without charge, control orders, limited rights to representation and other safeguards, sedition offences, widened information demand powers). In such matters, due process is essential to the legitimacy of the resulting law. Failure to honor deliberative democratic processes comes at a cost in confidence and trust.

There is a phrase in increasingly common use to comfort or to silence those who have concerns about the growing capacity of governments to conduct surveillance and to gather personal information about the citizenry. That phrase is: ‘nothing to hide, nothing to fear’. Let us now take a serious look at it.

## **Nothing to hide? Nothing to fear?**

The implication of the phrase ‘nothing to hide, nothing to fear’ is that only the guilty, with shameful secrets, object to having details of their lives known to the authorities. The implication is that they fear the legitimate consequences of disclosure of what they have done because what they have done must have been unlawful or improper. The implication is that to express concerns about loss of privacy is implicitly to admit to having guilty secrets. This can be a potent disincentive to the workings of participatory democratic processes precisely when those processes need to be working well.

Here are three reasons to be wary of the phrase ‘nothing to hide, nothing to fear’ every time you hear or read it –

- the onus is misplaced;
- government bureaucracies are always potentially dangerous and it is prudent always to limit their potential to do harm, in part by limiting the information that they may collect about individuals and by limiting what they may do with the information that they may properly collect;
- as times change, it may be a cause for genuine fear that certain information about a person will become known, even though in earlier times there was no reason for the person to have kept it hidden.

History contains many illustrations. I will offer three, each of them using a composite character based on historical fact. I will also ask you to imagine a future in which a characteristic that is not nowadays something to hide could become a characteristic that you may fear to have disclosed.

Why do I say that the onus is misplaced? Because the citizen is not under any onus to explain why he or she does not want to disclose aspects of his or her life to government. Government bears the onus of explaining that it has a legitimate reason to know particular details. ‘Nothing to hide, nothing to fear’, directed at each member of the public, should be turned around and directed at government as: ‘No legitimate reason to know, no legitimate reason to ask’.

Why do I say that all government bureaucracies are potentially dangerous? Because they are hierarchies that limit the understanding of each ‘cog in the machine’ about what the machine does, and this helps to separate each cog from his or her sense of individual responsibility for the results of the machine’s operations. The separation of individuals from their individual ethical responses works in both directions. At the top, those who give directions may claim a lack of understanding of all that flows from those directions when they are put into action by persons at each subsequent level all the way to the bottom. Persons lower down the hierarchy, where consequences are apparent, may claim a lack of understanding of what is assumed to have justified the giving of the directions, whatever the consequences.

I stress that the word ‘potentially’ qualifies ‘dangerous’. I do not mean simply the extreme dangers to life, liberty and property that the worst historical examples demonstrate. The more information governments collect about individuals, and the more the information is shared among authorities who are unfamiliar with the circumstances of its collection, the greater the likelihood of inaccuracy, misunderstanding, mistaken inferences and bad decision-making. The decisions of bureaucracies may have serious consequences for individuals. We have developed safeguards against this risk — parliamentary scrutiny, statutory regulators, judicial review, a free press and protection for whistleblowers are five such safeguards. But the safeguards do not always work promptly or properly. We are fools if we think we will ever eradicate the risk that bureaucracies can do damage to the lives of individuals, damage that can take considerable time for a bureaucracy to understand, acknowledge and remedy.

How can the disclosure to government of a characteristic that need not be hidden - because it is neither unlawful nor shameful - nevertheless be a cause for fear? It is time for three of history's examples.

### ***Germany, 1932-1945***

It is 1932 in Germany<sup>14</sup> and a prominent lawyer, now a judge, has no reason to hide his ethnicity or his faith. He is a practising Jew, renowned and respected by the community in which he and his family have lived and worked for generations as law-abiding, tax-paying, loyal citizens. His brother had died for Germany in the First World War. In January 1933, Adolf Hitler's Nazis come to power. Now our judge has plenty to fear, yet still nothing to hide in the sense that there is nothing shameful or contrary to law or improper about being a Jew. By April, the government has organised a boycott of Jewish businesses, doctors and lawyers. Laws change, and soon our judge is barred from his own court, then from practising law at all. He gets some of the children out of the country, but he feels obliged to stay; his home is Germany and the local Jewish community relies on him for advice, now more than ever. He and his family are required to stitch a yellow star to their clothes to brand themselves in public as being Jews. By 1941, with its detailed records about the population, government bureaucracy has identified and deported to camps in Poland the judge and every member of his extended family all over Nazi-occupied Europe. It tattoos them with a unique identification number. By 1945 it has murdered them all.

### ***Cambodia, 1974-1979***

In 1974, a medical doctor in Cambodia finds her skills in high demand. Her husband, an engineer, is also busy. Their three children are doing well at school. The family has no reason to hide their qualifications. On the contrary, their educational achievements are the basis of their income and the respect they enjoy in their community.

---

<sup>14</sup> Composite based on the literature of the Holocaust and my conversations with families, in Germany and Australia, whose members lived through the period. For an acutely observed, contemporaneous account of the 'legal' and bureaucratic methods of Nazism by a non-Jewish German dissenting lawyer, see Sebastian Haffner's *Defying Hitler* (Weidenfeld and Nicolson, first published 2002).

In 1975, Pol Pot takes power<sup>15</sup> and begins a communist revolution in Cambodian society which sees the city of Phnom Penh almost emptied of its population, who are put to work in agriculture in the countryside. Famine ensues. Many thousands die.

In these changed times, fear now leads our doctor and her family to hide the fact of their educations. They fail. The eldest son dies, malnourished, in forced labor. Our doctor and her husband die under torture after being arrested, without evidence, but because they have been mentioned in the ‘confessions’ extracted by torture from three other people. We know something of the fate of about 20,000 people like the doctor and her husband because someone in the bureaucracy kept records of the activities of the interrogation centre in the Phnom Penh suburb of Tuol Sleng.

### ***Australia, 1945-1951***

It is Australia in 1945, and the whole family is overjoyed that Pete is home at last. He has been overseas since 1937, when he joined the international brigade of volunteers who unsuccessfully attempted to help the Spanish Republican Government prevent the establishment of a fascist dictatorship under General Franco. Pete got out just in time. When he reached England in 1939, he and his commo mates were just in time to join up for the war against the fascists in Germany and Italy. His letters home were full of his hopes for the post-war world. The family shares his optimism. After all, the allies of Britain and Australia in the great victory over fascism included communist Russia. The whole family looks to Pete for political guidance. Family members repeat what he says to anyone who asks. There is nothing to hide.

By 1950 times have changed.<sup>16</sup> Pete and all communists are part of something called the Red Menace. He gets sacked for his political beliefs. The boss, who had fought

---

<sup>15</sup> Composite from the literature on Cambodia in the relevant period and my own brief experience during the rebuilding of the professions of journalism and law there in 1995 following the UN mission. For a fine general history, see David Chandler *A History of Cambodia* (Silkworm Books, 2<sup>nd</sup> ed. 1993).

<sup>16</sup> Composite from the literature and from recollections by Melbourne families of the era. For treatments of the impact in the United States of having beliefs that were thought to be sympathetic towards communism in the 1950s, see, for instance Ellen Shenker *The Age of McCarthyism: a brief history with documents* (Bedford-St Martins, 2<sup>nd</sup> ed, 2002), Corliss Lamont, *Freedom Is As Freedom Does: civil liberties in America* (Continuum, NY, first published 1956, 4<sup>th</sup> ed. 1990). The recent film *Good Night and Good Luck* examines the era from the perspective of some media practitioners.

in the same battalion with Pete, says he is personally sorry. In 1951, the Government proposes a *Communist Party Dissolution Bill* to allow it to ban the party and to 'declare' people to be communists, that is, to brand them as the enemy within. The High Court says the legislation is unconstitutional. The Government puts the proposal to a referendum. If it succeeds, Pete's lifelong political beliefs, which are a big part of his identity, could put him outside the law. The family is relieved when, in September, the referendum proposal fails. Pete gradually learns more about the purges under Stalin and talks to some of his immigrant mates from Eastern Bloc countries. He loses any illusions about the old ally Russia. But he sticks to his youthful hopes that communist ideas might change the world for the better. The family becomes much more discreet about Pete's beliefs.

I think these three historical illustrations give the lie to the phrase 'nothing to hide, nothing to fear' where government information-gathering powers are concerned. But perhaps my examples seem too remote in time or place, or too extreme in consequences, for you to accept my general point that the phrase 'nothing to hide, nothing to fear' should be subjected to wary scepticism here in contemporary Australia.<sup>17</sup>

Turn with me, then, away from the past for an imagined look into the future.

Among today's audience there are surely some people who smoke cigarettes. I wouldn't encourage you, but it is your choice. It is not unlawful. Attitudes and laws related to smoking have certainly changed significantly over the past 25 years or so, but you have nothing to hide. If you are asked whether you are a smoker or non-smoker, you probably answer that you are a smoker, and doubtless this information is sometimes recorded in order to establish your preferences for, say, seating arrangements.

---

<sup>17</sup> Views will naturally differ, but consider three further illustrations, two from a time and one from a place less remote. Ethnicity and religion formed the basis of official mass killings in Rwanda and the Balkans as recently as the 1990s. Some official policies of Australian governments in past eras had very serious adverse effects on many indigenous people. In these three examples, at certain times, a person had something to fear if it came to notice that they were, respectively, Tutsi (Rwanda), Muslim (Kosovo), below a certain age and part indigenous part non-indigenous (Australia). Before and after those times, these characteristics were not something to hide.

Now imagine, say, 15 years from now you are watching a television program. Say it explains that evidence (discovered in 2011) shows that the harms caused by passive smoking are more serious than previously believed. Fresh laws are being proposed. New government advertising campaigns are to be broadcast on the screens that, 15 years from now, are a basic feature of every public space and most private ones.

The next day on the way to work you see one of the ads, and in that ad is footage of a much younger you, puffing on a cigarette in the street outside an office building. It is from an archive of surveillance camera footage of office workers taken during one of your lunch breaks. I wonder if you should be anxious that in 2021 the caption on the screen beneath your image may read:

‘Aggressive Smokers, May 2006’

I stress, this illustration is hypothetical and deliberately far-fetched. My point is not to predict that what is imagined will happen to you or others, and of course I hope it will not. I seek merely to spur you to reflect on how information about you that seems innocuous at a given point in time may have different implications at another time, implications that might reasonably make a person anxious.

## **Conclusion**

I said at the outset today that, in sounding a warning, I was changing an approach I have generally followed for five years as a privacy commissioner with a function to improve public understanding of the value of privacy.

I am aware of the risks of issuing warnings. But I am convinced that it is necessary at this time to take risks to generate the kind of productive unease that causes democratic cultures to question more persistently those who want the power that a re-balancing of liberty and security will confer.

Technologies will steadily improve. Over the months and years to come, as governments suggest that responses to various public issues require more surveillance of the public and more personal information from the public, ask more questions.

Insist on proportionality. Verify that promised safeguards are enshrined in law and can be enforced.

Trust, but cautiously.

Keep an eye on your governments.

I thank the Victoria Law Foundation for the invitation again to give an address during the annual Law Week. I thank you for your attention.