HANDING OVER THE KEYS: CONTINGENCY, POWER AND RESISTANCE IN THE CONTEXT OF SECTION 3LA OF THE AUSTRALIAN CRIMES ACT 1914

NICKOLAS JOHN JAMES*

ABSTRACT

The Australian *Cybercrime Act 2001* (Cth) inserted a new section 3LA into the *Crimes Act 1914* (Cth). Section 3LA gives law enforcement officers the power to compel a person to reveal their private encryption keys, personal identification numbers or passwords, enabling the officers to access information held on a computer for the purpose of investigating and prosecuting a computer related offence. A failure to comply with the law enforcement officer's request is punishable by up to six months' imprisonment.

This paper is a Foucauldian analysis of the nature and impact of s 3LA. Two conclusions are reached. First, s 3LA is a technology of power that contributes to the disciplining of society in three ways: by manufacturing fear, by redirecting the flow of power between law enforcement agencies and private citizens, and by panoptic surveillance. Secondly, resistance to s 3LA was not only inevitable but contributed to its disciplinary effectiveness.

I INTRODUCTION

This paper uses the work and ideas of French theorist Michel Foucault to analyse a particular provision in the Australian *Cybercrime Act 2001*. Foucault would often take a widely accepted notion and consider it from a different angle; he would begin with something taken for granted as universal and inevitable and 'render it strange'.[1] In this paper, the key recovery provisions in the *Cybercrime Act* are rendered strange through their analysis as a technology of power.

The Australian *Cybercrime Act 2001* (Cth) commenced on 2 April 2002. The Act added a new part 10.7 to the *Criminal Code Act 1995* (Cth) and created seven new criminal offences: three serious computer offences[2] and four summary

* BCom LLB (Hons) LLM; Lecturer, T C Beirne School of Law, The University of Queensland.

[1] Keith Hoskin, 'Foucault under Examination: The Crypto-Educationalist Unmasked' in Stephen J Ball (ed), *Foucault and Education: Disciplines and Knowledge* (1990) 29.

[2] Unauthorised access, modification or impairment with intent to commit a serious offence, which carries a maximum penalty equal to the maximum penalty for the serious offence (s 477.1); unauthorised modification of data where the person is reckless as to whether the modification will impair data, which carries a maximum penalty of 10 years imprisonment (s 477.2); and unauthorised impairment of electronic communications, which carries a maximum penalty of 10 years imprisonment (s 477.3).

computer offences.[3] The Act also increased police investigative powers relating to search and seizure of electronically stored data by amendments to the *Crimes Act 1914* and the *Customs Act 1901*. Section 12 of the *Cybercrime Act* inserted a new s 3LA into the *Crimes Act 1914* (Cth):

> **3LA Person with knowledge of a computer or a computer system to assist access etc.**
>
> (1) The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:
>
> a. access data held in, or accessible from, a computer that is on warrant premises;
> b. copy the data to a data storage device;
> c. convert the data into documentary form.
>
> (2) The magistrate may grant the order if the magistrate is satisfied that:
>
> a. there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and
> b. the specified person is:
>
> i. reasonably suspected of having committed the offence stated in the relevant warrant; or
> ii. the owner or lessee of the computer; or
> iii. an employee of the owner or lessee of the computer; and
>
> c. the specified person has relevant knowledge of:
>
> i. the computer or a computer network of which the computer forms a part; or
> ii. measures applied to protect data held in, or accessible from, the computer.
>
> (3) A person commits an offence if the person fails to comply with the order.
> Penalty: 6 months imprisonment.

Under s 3LA, federal law enforcement agents can now obtain an 'assistance order'[4] requiring the owner or user of a computer to disclose their personal passwords and encryption keys provided the police have reasonable grounds to suspect that the computer either holds or can enable access to evidential material. The subject of the assistance order is not required to be a suspect, merely the owner or the user of a computer that is reasonably suspected of containing evidential material. A failure to provide the necessary assistance is punishable by up to six months imprisonment.

Realistically, the section is intended to be used only in the investigation of criminal activities. A reasonable magistrate would be unlikely to allow misuse of

[3] Unauthorised access to, or modification of, restricted data, with a maximum penalty of two years imprisonment (s 478.1); unauthorised impairment of data held on a computer disk, credit card or other storage device, with a maximum penalty of two years imprisonment (s 478.2); possession or control of data with intent to commit or facilitate a computer offence, with a maximum penalty of three years imprisonment (s 478.3); and producing, supplying or obtaining data with intent to commit or facilitate a computer offence, with a maximum penalty of three years imprisonment (s 478.4).

[4] An assistance order differs from a search warrant in that a search warrant imposes no legal duty on the occupier of premises or on any other person to assist the law enforcement officer in their search.

the provision, and most citizens are unlikely to become the subject of any such assistance order. This paper, however, is not concerned with the direct impact of s 3LA upon cybercriminals and their associates, or the direct use of s 3LA in the investigation of cybercrimes. Rather, it is concerned with the wider disciplinary impact of the section, and criticism of and resistance to it. When adopting a Foucauldian theoretical framework, one views the law not as an apolitical rule made by parliament but as a technology of power available to be used by some within the community against others. In analysing s 3LA, two matters are considered: (1) its disciplinary nature and its panoptic surveillance of the community; and (2) the resistance to s 3LA, including the ways in which resistance contributes to its disciplinary effectiveness. Before considering these two issues, the social and historical conditions or contingencies that made the passage of s 3LA possible are identified.

II CONTINGENCY

A conventional approach to understanding the origin of section 3LA might be to pursue a causal line of inquiry. Such a causal approach might conclude that a need for more effective law enforcement in the area of cybercrime was required, and that this need outweighed any privacy concerns associated with the obligation to disclose passwords and private keys. The approach taken in this part of the paper, however, does not seek out the 'cause' of section 3LA. Instead the question it asks is: what combinations of circumstances in dispersed and seemingly unconnected fields of social activity combined in such a way as to give rise to this outcome? Section 3LA's passage was the consequence of a number of contingencies rather than the result of a particular cause.

Foucault referred to this type of work as uncovering the 'conditions of possibility'. Drawing up such a list of contingencies involves some historical investigation, but it does not require an exercise in causal logic and the artificial designation of some items on the list as primary and others as secondary. Nor does it require those contingencies on the list to be in some subordinate relation to an item not on the list considered the primary cause.[5] The contingencies described in this paper that contributed to the passage of s 3LA include international developments, pressure from police for more effective law enforcement powers, fears of Australian business regarding the rising costs of cybercrime, fears of the Australian community regarding cyberterrorism, and the growing impact and economic importance of the cyber-security industry.[6]

[5] Gavin Kendall and Gary Wickham, *Using Foucault's Methods* (1999) 6-7.

[6] These contingencies are listed, and the way in which each contributed to the passage of s 3LA is described, but it is not necessary to place the contingencies on a scale of ascending or descending importance. Nor is it necessary to suggest that all of these contingencies are evidence of some underlying contingency such as the advance of capitalism or the war on terror. Each contingency is in a contingent relationship with every other contingency. They may or may not relate in any way. If they do relate, no pattern or outside force dictates the form of their relationships with one another. See ibid 8-9.

The first contingency contributing to the passage of the *Cybercrime Act* and of s 3LA was the European Union's *Convention on Cybercrime* and its adoption by the Committee of Ministers in November 2001. The Convention required countries to pass laws on cybercrime and to agree to promote mutual assistance in enforcing laws and conducting investigations. More specifically, the Convention required that countries enact laws guaranteeing that users provide access to all files on a system under penalty of gaol, including encryption keys. Article 19 specifically provided that '[e]ach party ... ensure introduced measures allow for the search and seizure of stored computer data'.[7] The Convention was initially open to the 52 members of the Council of Europe and to countries that were involved in its development, including the US, Canada, Japan and South Africa. At the G-8 meeting in Paris in July 2000, the French Government recommended opening the Convention to all countries.[8] The Australian government indicated during its Second Reading Speech in July 2001 that the Cybercrime Bill was based on the Council of Europe's *Convention on Cybercrime*.

Another contingency was the perceived inadequacy of the law in Australia relating to search and seizure of electronic evidence. One of the most problematic characteristics of electronic evidence from the point of view of law enforcement agencies is its ability to be encrypted. Australian law only regulates the exportation of encryption technology; there is no direct restriction upon the use of encryption within Australia.[9] The Australian Attorney-General's Department commissioned its *Review of Policy Relating to Encryption Technologies* (The Walsh Report) and initially planned publication in 1997.[10] Gerard Walsh was instructed to investigate the nature and use of encryption technology within Australia and to form an opinion as to whether legislative or other actions were required in the interests of national security and law enforcement. His Report acknowledged the wide availability of strong encryption: 'Strong encryption, which cannot be defeated by law enforcement and national security agencies, is already available commercially or in the public domain'.[11] The Report described the conflict between the availability of encryption and the requirements of law enforcement agencies:

---

[7] David Banisar, 'The World of Surveillance Part I: Building Surveillance into Communications' (2000) *Privacy Law and Policy Reporter* 34.

[8] Ibid.

[9] The exportation of encryption technology is covered by the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* ('The Wassenaar Arrangement'), a multilateral agreement intended to restrict the proliferation of products with potential military applications. Encryption is explicitly included in the section regarding 'dual-use goods and technologies', products that have a genuine use in the civilian realm, whilst remaining potentially dangerous if used in war. The Wassenaar Arrangement has been adopted into Australian law by way of the *Customs Act 1901* and the *Customs (Prohibited Exports) Regulations*. Nick Ellsmore, *Cryptology: Law Enforcement & National Security vs. Privacy, Security & the Future of Commerce* (1999) <http://cryptome.org/crypto97-ne.zip> at 5 June 2003.

[10] The Walsh Report was subsequently withheld by the Federal Government and only released to the public by way of a Freedom of Information application by Electronic Frontiers Australia.

[11] Gerard Walsh, *Review of Policy Relating to Encryption Technologies* (1997), <http://www.efa.org.au/Issues/Crypto/Walsh/walsh1.htm> at 5 June 2003. This section was censored from the original release.

> [S]trong cryptography, imminently available to the mass market, will offer significant enhancement of data security and personal and corporate privacy, but also provide a powerful shield behind which criminals and others may operate.[12]

One of the recommendations contained in the Walsh Report was that the *Crimes Act 1914* be amended as follows:

> [T]he authority be created for the Commissioner of the AFP to require persons to answer questions, notwithstanding the principle of non self-incrimination, concerning passwords or codes relating to material seized in the course of investigation of serious criminal offences and found to be encrypted or to produce materials relating to the cryptographic processes employed.[13]

The Australian Centre for Policing Research also highlighted the need for procedural law reform in its scoping paper, *The Virtual Horizon: Meeting the Law-Enforcement Challenges*.[14] According to the paper, one of the most important aspects of cyberspace regulation from the point of view of cyber-policing was the obligation of system owners to assist investigations, including the provision of assistance in order to get around encryption.[15] The paper identified the challenges to law enforcers required to investigate computer related offences as including:[16]

> Acquiring appropriate powers — In order to effectively and efficiently investigate crime in a lawful and ethical way, police will require a full range of powers and authorities to undertake activities which are reasonably required to intercept, search for, and obtain electronic and other evidence, and to apprehend and deliver offenders to be dealt with according to law.
>
> Decoding encryption — Offenders can securely maintain the business and other records needed to operate criminal enterprises. While remaining secure from outside perusal, the data will remain easily accessible to criminals. At the same time, police face considerable problems in decoding any encryption and recovering the information.[17]

The paper concluded that existing state and federal laws regarding the use of search warrants were inadequate to address many of the issues arising in relation to cybercrime,[18] and that 'reform of relevant search and seizure laws may be the most urgent need'.[19]

Passage of the *Cybercrime Act* was also facilitated by the rising cost of cybercrime to the Australian business community and the consequent loss of faith by that community in the law's efficacy. Since 1997, four Australian Computer

---

[12] Ibid.

[13] Ibid.

[14] Australian Centre for Policing Research, *The Virtual Horizon: Meeting the Law Enforcement Challenges - Developing an Australasian Law Enforcement Strategy for Dealing with Electronic Crime* (2000).

[15] Ibid xxvii.

[16] Ibid.

[17] Ibid 25.

[18] Ibid 98.

[19] Ibid 101.

Crime and Security Surveys have been conducted and published.[20] Three conclusions relevant to the passage of the *Cybercrime Act* can be drawn from the findings in all four surveys. Incidents of cybercriminal attacks on Australian business organisations have been steadily increasing.[21] The costs of cybercrime, including both the damage to or loss of valuable information and the costs of implementing protective measures, have also been increasing.[22] There is also a continuing perception within the Australian business community that the criminal law is inadequate to address cybercrime.[23] The findings point to a desire within the community for a more effective legal regime, a desire that inevitably manifests as pressure upon legislatures to grant police the necessary investigative and enforcement powers.

Cybercrime threatens e-commerce's viability. It threatens to undermine the tentative trust placed by business and consumers in the use of computers and the Internet for conducting transactions. In addition to being an attempt to reduce the costs of cybercrime, the *Cybercrime Act* was also contingent upon a desire to create within Australian businesses a sense that electronic commerce is taken seriously by government, that attempts are being made to protect it, and that electronic commerce is a feasible and positive development for Australian industry.[24]

Similarly, the passage of the Act was contingent upon a perceived need to address both the social threat of cybercrime and the fears of the wider Australian community regarding cyberterrorism. *The Virtual Horizon* paper described cybercrime's potential social threat as follows:

> The social costs for victims of crime such as child exploitation and cyberstalking and for their families are also significant. The repercussions of such incidents may be medical problems such as depression or other mental health issues, unemployment, truancy, broken families and a general deterioration in the individual's quality of life and community well-being.[25]

---

[20] The first Australian Computer Crime and Security Survey was produced in 1997 by the Office of Strategic Crime Assessments and Victoria Police. The second survey was produced in 1999 by Deloitte Touche Tohmatsu and Victoria Police. The third survey was produced in 2002 by NSW Police, Deloitte Touche Tohmatsu and AusCERT. In May 2003, the fourth survey was released. The survey was produced by the Australian Federal Police, Queensland Police, South Australia Police, Western Australia Police and AusCERT. AusCERT, *2003 Australian Computer Crime and Security Survey* (2003).

[21] Ibid. The 2003 survey found, inter alia, that 42% of the respondent organisations experienced one or more computer attacks in the previous 12 months which harmed the confidentiality, integrity or availability of network data or systems.

[22] Ibid. The 2003 survey found that the total losses incurred by the respondent organisations for 2003 was approximately $12 million, compared to approximately $6 million in 2002.

[23] Ibid. The 2003 survey found that of those respondent organisations which experienced harmful attacks, 68% did not report the incident to law enforcement authorities. Of those respondent organisations that did not report incidents to law enforcement authorities, 52% did not do so because of a perception that it would be difficult or impossible to catch the perpetrators.

[24] Robert Chalmers recently suggested this when he wrote that: 'The Act does make some substantive improvements. However no doubt it is also intended to fulfil something of a similar symbolic role in painting cyberspace as a more regulated and safer place to inhabit'. Robert Chalmers, 'Regulating the Net in Australia: Firing Blanks or Silver Bullets?' (2002) 9 *E Law (Murdoch University Electronic Journal of Law)* 1-30.

[25] Australian Centre for Policing Research, above n 14, 20.

The notion that this threat warrants increased police powers is apparent in the statement by the Federal Minister for Justice and Customs following the passage of the *Cybercrime Act*:

> Previously if a terrorist attack had been carried out on Australia's national information infrastructure police did not have the power to compel suspects to assist in an investigation of complex computer systems protected by passwords or encryption ... The new investigation powers contained in the Act will give police the power to ... compel a computer owner to assist police with their inquiries.[26]

Peter Coroneos, chief executive of the Internet Industry Association, also linked the *Cybercrime Act* to the 'war on terror':

> The world changed after September 11. We believe that in the wake of the attacks it's appropriate to push ahead with cooperative arrangements industry was developing with national security agencies' to help track down criminal and terrorist activities on the Internet. [Australia's] *Cybercrime Act* was almost prophetic, in that our thinking was already turning to these kinds of issues. It's only a matter of time before terrorists realise, if they haven't already, that it's safer and more convenient to conduct disruptive activities from a remote location over the Internet than it is driving planes into buildings.[27]

Politicians and business leaders continue to emphasise the threat of cyber-terrorism. During an address at the AusCERT Asia-Pacific IT Security Conference in May 2003, Queensland Minister Paul Lucas made the following comments:

> People will never forget the appalling violence of terrorist events such as 11 Septemberand the Bali bombing. Cyber-terrorism is a real threat, as it has huge potential to wreak havoc in databases and computer networks around the world with politically-motivated cyber-terrorism compounding the problem of computer hackers.[28]

The legislature was certainly aware of the threats referred to in these statements when the *Cybercrime Act* and section 3LA were passed. While it is not suggested that such statements generated the community's fears, they did highlight that fear in a way that facilitated the passage of the *Cybercrime Act* and its acceptance by the community.

Australia's burgeoning cyber-security industry also facilitated the Act's passage. The livelihoods of an increasing number of organisations and individuals depend upon the escalating war on cybercrime. Recently, the public sector has seen the creation of new and specialised organisations and taskforces to tackle cybercrime and address its consequences. Federal agencies such as the National Office for the Information Economy, the Department of Defence, the Defence Signals

---

[26] Rachel Lebihan, 'Aust Cybercrime Bill Rides on US Attack Fear' (2001) *ZD Net Australia - News and Technology*, <http://www.zdnet.com.au/news/security/0,2000061744,20260812,00.htm> at 5 June 2003.
[27] James Elder, 'Cyber Terrorism' (2002) *E.Law Practice.*
[28] Findlaw Australia, *Cybercrime Experts* (2003)
<http://www.findlaw.com.au/news/default.asp?task=read&id=14741&site=LE> at 5 June 2003.

Directorate, the Australian Federal Police and the Department of the Treasury have resources and staff devoted to the problem of cybercrime. At the state level, various police forces have set up specialist units to deal with cybercrime, including the Police Child Exploitation Internet Unit in NSW and the Computer Crime Investigation Squad in Victoria.[29] Within the private sector, there are 190 'e-security' firms in Queensland.[30] Profit seeking ventures and bureaucratic entities often become self-perpetuating structures that normalise those knowledges and beliefs, which sustain their existence and advance their causes. Again, while it is not suggested that these organisations exaggerate the threat of cybercrime and cyberterrorism, they do have a stake in maintenance of the perception of that threat.

The final contingency contributing to the passage of the *Cybercrime Act* and s 3LA considered in this paper is the existence of the Echelon system. In 1947, the governments of the United States, the United Kingdom, Canada, Australia and New Zealand allegedly signed a National Security pact known as the Quadripartite Agreement. Under the terms of the agreement, the five nations divided the planet into five spheres of influence; each country was assigned particular signals intelligence targets.[31] Echelon was set up for intelligence gathering and has since developed into a network of intercept stations around the world. Its primary purpose is to intercept private and commercial communications.[32] This is conjecture, but it is likely that the availability and use of strong encryption by Australian businesses and individuals is an impediment to Echelon's operation and effectiveness. Section 3LA is a mechanism that undermines the effectiveness of encryption and thus facilitates compliance by the Australian government with its obligations under the agreement.

III POWER

Section 3LA is a tool which facilitates attempts by law enforcement agents to extract access codes forcibly from computer owners and operators using the threat of imprisonment. It is what Foucault referred to as a 'technology of power'. As a technology of power, s 3LA is used not only against those who are suspected of having committed a cybercrime. It has an impact upon the regulation of the entire community; it is one element in a complex disciplinary structure. As Foucault explains, modern society is a disciplinary society. Citizens are subjected to and monitored by a complex disciplinary framework that both enables and controls

---

[29] Patrick Quirk and Jay Forder, *Electronic Commerce and the Law* (2nd ed, 2003).

[30] Findlaw Australia, above n 28.

[31] The existence of this agreement has never been confirmed by the member nations, but in May 2001, the European Parliament's Temporary Committee on the Echelon Interception System issued a report concluding that '... the existence of a global system for intercepting communications . . . is no longer in doubt'. European Parliament, *Temporary Committee on the Echelon Interception System, Report on the Existence of a Global System for the Interception of Private and Commercial Communications (Echelon Interception System) (2001/2098(Ini))* (2001) <http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf> at 5 June 2003.

[32] Electronic Privacy Information Centre, *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments* (2002) 50-51.

the ways they think and the ways they behave. It seeks to ensure that most citizens remain 'docile bodies':[33] that they think acceptable thoughts, that they do acceptable things and that they do not stray too far from 'normal'. Law is one disciplinary mechanism that orders their thoughts and actions. There are of course other disciplinary mechanisms, some of which are more influential and more powerful than law: the media, schooling and education, religion, peer pressure. Foucault viewed law as a mechanism that is confined mainly to legitimising the disciplinary technologies and normalising practices established by other mechanisms.[34]

> I do not mean to say that law fades into the background or that institutions of justice tend to disappear, but rather that the law operates more and more as a norm, and the judicial institution is increasingly incorporated into a continuum of apparatuses (medical, administrative, and so on) whose functions are for the most part regulatory.[35]

A law's most widespread impact is a consequence not of its direct enforcement against the suspected criminal, but a consequence of its existence as a normalising standard of behaviour with which all must comply. A Foucauldian analysis of s 3LA as a technology of power is therefore directed not towards the State and its objectives, but towards the operation of the law in 'dispersed and localised sites':[36]

> The analysis ... should not concern itself with the regulated and legitimate forms of power in their central locations ... On the contrary, it should be concerned with power at its extremities ... with those points where it becomes capillary ... one should try to locate power at the extreme points of its exercise, where it is always less legal in character.[37]

Who is it that exercises this power? Law is typically portrayed as a technology used and exercised by the State, an invisible monolithic authority that occasionally manifests as legal agents. Foucauldian analysis undermines this portrayal. There is a government, but government is not in complete control of the community. Many other institutions exercise power: autonomous government agencies, private corporations and powerful individuals. This is consistent with Foucault's insistence that power is not something possessed only by the State.

---

[33] Paul Rabinow (ed), *The Foucault Reader* (1984) 179-88.

[34] Alan Hunt and Gary Wickham, *Foucault and the Law: Towards a Sociology of Law as Governance* (1994) 57.

[35] Michel Foucault, *The Will to Knowledge: The History of Sexuality 1* (1998) 144. See also Michel Foucault, 'Truth and Power' in James D Faubion (ed), *Power: Essential Works of Foucault 1954-1984 Volume 3* (2002) 63. Foucault comments:

> To pose the problem in terms of the state means to continue posing it in terms of sovereign and sovereignty, that is to say, in terms of law. If one describes all these phenomena of power as dependent on the state apparatus, this means grasping them as essentially repressive: the army as a power of death, police and justice as punitive instances, etc. I don't want to say that the state isn't important; what I want to say is that relations of power, and hence the analysis that must be made of them, necessarily extend beyond the limits of the state. In two senses: first of all, because the state, for all the omnipotence of its apparatuses, is far from being able to occupy the whole field of actual power relations, and further because the state can only operate on the basis of other, already existing power relations.

[36] Hunt and Wickham, above n 34, 55-6.

[37] Foucault, above n 35, 96.

Power is possessed by all, is exercised by all, and permeates society.[38] There is no invisible ultimate authority: there are only people, competing and cooperating and trying to help and trying to control. Power is present in all forms of social relations, it is 'at work' in every situation. Power is, in a sense, everywhere.

Section 3LA is a technology which facilitates the exercise of power not only by law enforcement agents. Cyber-security experts use it to justify their fees, journalists as fodder for stories, and academics as a topic for papers. The combined result of these and many other such attempts at control is the creation of a disciplinary society, a society that is constantly seeking to regulate itself. Law is a technology that operates as justification for the application of physical force by one person (the State-sanctioned law enforcement officer) against another (the alleged criminal). However, it is law as a justification for the application of surveillance, and as a disciplinary mechanism that are the more important and more common applications of law as a norm.

Section 3LA is a technology of power that contributes to the disciplining of society and to the production of docile bodies in three important ways: by manufacturing fear, by redirecting the flow of power, and by panoptic surveillance.

Section 3LA manufactures fear in two forms: fear of the criminal other and fear of the police. Becoming aware of the existence of s 3LA, citizens simultaneously identify themselves as innocent subjects to be protected and as criminal subjects to be punished. As innocent subjects to be protected, s 3LA reinforces the impression that they are threatened by the actions of cybercriminals and cyberterrorists, and encourages them to rely increasingly upon the protection offered by law enforcement agencies. As criminal subjects to be punished, while they may not have in fact breached the law, many will still fear that they have done *something* wrong and will attract the gaze of law enforcement agencies. Section 3LA disciplines by encouraging citizens to both rely upon and fear police.

By undermining the effectiveness of data encryption, s 3LA redirects the flow of power away from business and private citizens towards law enforcement agencies. Encryption is one of the means by which citizens can resist and oppose cybercrime without the assistance of law enforcement agencies, by protecting their own data.[39] Encryption has the potential to empower the law-abiding individual as well as the criminal. Section 3LA undermines this empowerment and shifts power away from citizens by weakening the effectiveness of encryption and compelling citizens instead to place greater reliance on law enforcement agencies.

---

[38] This does not mean that power is distributed equally or democratically; Foucault recognised that dominance does exist, and insisted that it should be pointed out whenever it does occur.

[39] See generally Dorothy Denning, *Information Warfare and Security* (1999).

The third and most important way in which s 3LA contributes to the disciplining of society is through panoptic surveillance. Surveillance is a technique of power that does not necessarily rely on force. It coerces by means of observation.[40] The metaphor for modern surveillance Foucault uses in *Discipline and Punish* is Bentham's panopticon. The panopticon is a prison constructed in the shape of a wheel around the hub of an observing warden who at any moment *might* have the prisoner under observation. Unsure of when authority is watching, the prisoners strive to conform their behaviour to its presumed desires.[41] Modern society is panoptic because citizens are constantly watched and monitored by institutions of the State. In turn, citizens monitor and watch each other. Every movement might be seen, every transaction might be recorded. There is no need for an all-seeing State: because they feel watched, citizens internalise authority and regulate their own behaviour. Panoptic power achieves what judicial power cannot: the transformation of most citizens into self-regulating, self-disciplining and self-monitoring docile bodies.[42]

Data encryption was one of the ways by which citizens could hide from what they imagined to be an all-seeing eye, and create a space within which they could work and play away from the judgmental gaze of authority. Section 3LA has subverted that freedom by compelling citizens to hand over the keys upon demand. It is panoptic in the sense that citizens are disciplined to conform by the awareness that at any moment law enforcement agents could compel them to hand over their keys and allow agents access to information contained within their computers. Actual action by agents is not even required: surveillance and discipline make citizens wardens who willingly regulate their own behaviour.

---

[40] See especially Michel Foucault, 'The Means of Correct Training' in Paul Rabinow (ed), *The Foucault Reader* (1984) 189. Foucault comments at 192-3:

> Hierarchised, continuous, and functional surveillance may not be one of the great technical 'inventions' of the eighteenth century, but its insidious extension owed its importance to the mechanisms of power that it brought with it. By means of such surveillance, disciplinary power became an 'integrated' system, linked from the inside to the economy and to the aims of the mechanism in which it was practised. It was also organised as a multiple, automatic, and anonymous power; for although surveillance rests on individuals, its functioning is that of a network of relations from top to bottom, but also to a certain extent from bottom to top and laterally; this network 'holds' the whole together and traverses it in its entirety with effects of power that derive from one another; supervisors, perpetually supervised. The power in the hierarchised surveillance of the disciplines is not possessed as a thing, or transferred as a property; it functions like a piece of machinery. And, although it is true that its pyramidal structure gives it a 'head', it is the apparatus as a whole that produces 'power' and it distributes individuals in this permanent and continuous field. This enables the disciplinary power to be both absolutely indiscrete, since it is everywhere and always alert, since by its very principle it leaves no zone of shade and constantly supervises the very individuals who are entrusted with the task of supervising; and absolutely 'discrete', for it functions permanently and largely in silence. Discipline makes possible the operation of a relational power that sustains itself by its own mechanism and which, for the spectacle of public events, substitutes the uninterrupted play of calculated gazes. Thanks to the techniques of surveillance, the 'physics' of power, the hold over the body, operates according to the laws of optics and mechanics, according to a whole play of spaces, lines, screens, beams, degrees, and without recourse, in principle at least, to excess, force or violence. It is a power that seems all the less 'corporal' in that it is more subtly 'physical'.

[41] James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors* (1997) <http://www.law.duke.edu/boylesite/fouc1.html> at 4 June 2003.

[42] Mark Winokur, *The Ambiguous Panopticon: Foucault and the Codes of Cyberspace* (2003) <www.ctheory.net/text_file?pick=371> at 5 June 2003.

IV RESISTANCE

In physics, the application of force is met with resistance in the form of friction. In legal discourse, the application of legal power is inevitably met with resistance through criticism and by disobedience. Foucault insisted that resistance forms *whenever* power is exercised: 'there are no relations of power without resistances; the latter are the more real and effective because they are formed right at the point where relations of power are exercised'.[43] Resistance is not external to the exercise of power. Resistance is a technical component of power, part of its operation.[44] It is useful to think of the analogy of the machine: movement within the machine is the result of power, and resistance — friction — is an unavoidable aspect of that process.

The passage of the *Cybercrime Act 2001* and s 3LA was far from unopposed. Criticism of the provision appeared in statements made by civil liberties groups, business leaders and academics. The main criticisms were that it was poorly worded; that it gave almost unlimited investigative powers to the police; that it assumed a much greater threat from cybercrime and from cyberterrorism than actually existed; that it was contrary to the right to silence; and that it undermined the right to privacy. In its submission prior to the passage of the Cybercrime Bill, civil liberties group Electronic Frontiers Australia (EFA) pointed out that s 3LA had the potential to lead to imprisonment of a person who had innocently forgotten the password to their computer:

> There may sometimes be legitimate reasons why a private key or plain text could not be handed over to a law enforcement agency, and it would be difficult for the subject of an assistance order to provide proof that they did not possess or have access to a key or plain text. The prospect of users of encryption being jailed despite having genuinely lost their private keys is a major and quite legitimate concern.[45]

Robert Chalmers suggested that 'it may be that in the rush to push through amendments the new laws were not as well considered or crafted as they might have been'.[46] Phillip Argy, national vice-president of the Australian Computer Society, was of the view that 'the Act went a little too far, in that it erred on the side of giving too much power'.[47]

Section 3LA provides that a search warrant may be issued demanding cooperation if 'there are reasonable grounds for suspecting that evidential material is held in,

---

[43] Michel Foucault, 'Power and Strategies' in Colin Gordon (ed), *Michel Foucault Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (1981) 142.
[44] Kendall and Wickham, above n 5, 50-1.
[45] Electronic Frontiers Australia, *Submission - Inquiry into the Provisions of the Cybercrime Bill 2001* (2001) <http://www.efa.org.au/Publish/cybercrime.html> at 13 March 2003.
[46] Chalmers, above n 24.
[47] Elder, above n 27.

or *is accessible from*, the computer'. Given the nature of the Internet, evidential data stored anywhere in the world may be accessible from a particular computer:

> Essentially, what they've done is say if they have reason to believe that there's a bit of information in a computer, they can get warrants to search that computer and any computer on any network to which the first computer is connected. ... So if it's the Internet, that's pretty broad. We accept that you can't have these enforcement authorities having to go back to a judge every five minutes to incrementally expand the warrant, so we're prepared to live with some sort of sensible balance, but they've used a sledgehammer to crack a nut.[48]

EFA spokesperson Greg Taylor accused the Australian government of 'using the fear generated by the US tragedy to push through changes to the law ... The Australian Labor Party seem to have caved in on the Bill, making reference to the acts of terrorism on the US and the changing climate of cyberterrorism'.[49] Taylor argued that there is no reason why cyberterrorism should be related to the 11 Septemberterrorist attacks, other than unsubstantiated claims the terrorists may have used email communication or encryption techniques to disguise information distributed over the Internet.[50] In another statement to the press, EFA described the legislation as 'an overbroad knee-jerk reaction to recent well-publicised virus attacks'.[51]

In its submission EFA directly criticised s 3LA as contrary to the common law principle of the right to silence:

> The law enforcement provisions may also have the effect of over-riding the common law privilege against self-incrimination. This situation could arise where a person was compelled to reveal a password or encryption key as a requirement of an assistance order. The right to silence is a long-standing right in most jurisdictions and it is unacceptable that it should be potentially over-ridden in the Bill without strong justification or even acknowledgement.[52]

The EFA submission also argued that s 3LA breaches the 1997 OECD cryptography guidelines that Australia has adopted and which specifically recognise the fundamental right of privacy in relation to encrypted data:

> Article 5. The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national

---

[48] Ibid.

[49] Lebihan, above n 26.

[50] Ibid.

[51] Craig Liddell, *Cybercrime Bill Condemned by Industry Groups* (2001), <http://australia.internet.com/r/article/jsp/sid/10790/page/0> at 13 March 2003.

[52] Electronic Frontiers Australia, above n 45. While Australia does not have a Constitutional guarantee of the right to silence, such a right is recognised in all Australian jurisdictions and all common law countries. The Australian right to silence has been clearly stated by the High Court in *Petty v The Queen* (1991) 173 CLR 95, 99:

> A person who believes on reasonable grounds that he or she is suspected of having been a party to an offence is entitled to remain silent when questioned or asked to supply information by any person in authority about the occurrence of an offence, the identity of participants and the roles which they played ... An incident of that right of silence is that no adverse inference can be drawn against an accused person by reason of his or her failure to answer such questions or to provide such information.

See also Gerard Walsh, 'The Right to Silence: A Sanctuary for Sophisticated Offenders, or Central to the Presumption of Innocence?' (1999) April *Law Society Journal* 40, 40.

> cryptography policies and in the implementation and use of cryptographic methods.[53]

Revealing a private key or a password has potentially drastic consequences for a person's cyberprivacy: it can compromise the integrity of the person's digital signature. EFA also noted that the person on whom the assistance order is served is not necessarily assumed to be guilty of an offence.

Resistance to s 3LA took the form of commentary and criticism by business and government leaders within the media, and by legal experts in works of academic scholarship. This criticism was often argued passionately, presented clearly, and grounded in established principles of justice and privacy. Nevertheless the Act was passed and section 3LA remains as law. Why was resistance to s 3LA apparently ineffective? One answer is that the institutions favouring the provision were at the time able to accumulate and exercise more power than those who opposed it. However, it is also possible that resistance to and criticism of s 3LA contributed to its success. This could have occurred in three ways.

First, within a legal system that portrays itself as participatory and democratic — such as that within Australia — criticism of the law is encouraged and forms part of the ongoing process of law reform. Criticism by some within the community relieves the majority from the obligation to participate in resistance. Most do not need to voice opposition to s 3LA because they assume that others will do so on their behalf.

Secondly, criticism of s 3LA was and is one of the mechanisms by which awareness of the provision's panoptic impact circulates throughout the community. While 'ignorance of the law is no excuse', in order to be effective for behavioural regulation, laws must be known. Legal institutions rely upon media commentary and academic scholarship to propagate knowledge of the law: propagation is effected whether commentary is positive, neutral or negative.

Thirdly, discourse is both a form of knowledge and an exercise of power. Discourse determines what can be said and what cannot be said. Even when legal discourse permits criticism of a law, it still controls the form of that criticism. Criticism of s 3LA on the grounds that it undermines the principle of privacy is permitted criticism. This is demonstrated by comparing the following statements. The first statement is by EFA:

> Clearly there is tension between privacy rights and legitimate law enforcement needs. An approach needs to be found that balances these issues. [54]

The second is by the Australian Centre for Policing Research:

---

[53] Electronic Frontiers Australia, above n 45.
[54] Ibid.

> [There is a] need to achieve an appropriate balance between the requirements of policing and fundamental human rights, such as the right to privacy and freedom of speech.[55]

Those who favoured s 3LA and those who opposed s 3LA said essentially the same thing: the same legal discourse and the same discursive rules limited statements by both. Whether one favours security or privacy, one is still bound to play by the rules of legal discourse. Even if criticism of the law does lead to change in the law, change is likely to be no more than cosmetic. The authority and the disciplinary power of the state and of the various agents and institutions that take advantage of the law remain unchallenged. The critics of a provision like section 3LA ultimately form an important part of the disciplinary structure that ensures laws are willingly accepted by the community.

V CONCLUSION

Section 3LA is unlikely to be used directly against the majority of Australian computer owners and users. Nonetheless, s 3LA's power-effects are only partially manifested in the form of direct regulation. It is more likely to achieve its objectives through panoptic surveillance and normalisation, and in that respect the provision's power-effects will be much more widespread. The police may never arrive at the doorstep with an assistance order compelling most citizens to disclose their passwords, *but they could if they wanted to*. As this knowledge gradually circulates throughout the community, citizens will willingly and obediently reduce the space within which they feel free to live, to play, to act and to create away from authority's scrutiny and judgment.

[55] Australian Centre for Policing Research, above n 14.