Technology Determinism, the State and Telecom Surveillance

Peter Shields

INTRODUCTION
The importance of assessing the relationship between technology determinism and institutional power is a recurring theme in William Melody’s writings. Technology determinism is a perspective that views technical innovation as driving society. That is, the relationship between technology and society is regarded as linear and mono-directional. For instance, Melody (1973b) convincingly shows how technology determinism, functioning through the natural monopoly concept, supported a regulatory regime that insulated, preserved and extended the market power of AT&T, the dominant telecom carrier of the day in the United States. As he put it, ‘acceptance of the concept of technology determinism ... has had a devastating effect on the approach to regulation adopted by regulatory authorities... . It has narrowed the scope of analysis of public policy makers to encompass only changes within the established institutional structure’ (Melody 1973b: 170). Similarly, he demonstrated how the rampant technology determinism that infuses information society policy statements of national governments, international organisations and corporations, privileges regulatory strategies and resource commitments that would benefit major telecom supplier firms and countries (Melody 1996c).

Following Melody’s lead, this contribution assesses how the relationship between technology determinism and institutional power has played out in the domain of state telecom surveillance, a relatively neglected area of telecom policy studies. For a decade, concerns have been raised in the United States that the ‘telecom revolution’ and the emergence of the network economy are undercutting the state’s surveillance capabilities. Policy initiatives were launched in response to this ostensible crisis. These initiatives led to intense debate between law enforcement agencies and their allies, on the one side, and industry actors and civil liberty groups, on the other. The technology determinism, which is at the heart of this debate, has functioned to narrow the scope of policy analysis by obscuring the ways in which developments in criminal justice policy and associated changes in the state have conditioned policy initiatives. The law enforcement establishment has benefited most from this state of affairs.
Policy Initiatives in the United States
Since the early 1990s, law enforcement agencies have argued that the rapid deployment of fibre optic cable in telecom networks, the explosive expansion of mobile telephony and the Internet and the proliferation of strong private sector encryption technology are threatening to erode their long-standing capabilities of intercepting and monitoring electronic communications. Without appropriate regulatory responses, their argument runs, drug traffickers, terrorists and the like will be able to operate anonymously and with impunity in virtual havens with devastating effects for public safety.

Regulatory responses were not slow in coming in the United States. After several years of dogged lobbying by the Federal Bureau of Investigation (FBI), Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA, for the first time, ‘hardwires’ the surveillance interests of law enforcement agencies into the design of telecom networks and services; telecom carriers, both landline and wireless, must now engineer their networks and services in such a way that law enforcement agencies can continue to wiretap. The implementation of CALEA has not been smooth due to efforts by the FBI to use the legislation to significantly expand its surveillance capabilities. This includes, for example, its demand that cellular phone companies provide law enforcement with location-tracking information on demand.

On the encryption front, the Clinton Administration pressed for adoption of its Clipper Chip or key recovery initiative throughout the 1990s. The aim of the initiative was to guarantee law enforcement officials access to a set of ‘spare keys’ that could be used to unlock encrypted electronic messages when authorised to do so. The plan stalled in the face of intense opposition from industry actors and civil liberty groups.

With respect to the Internet, the FBI has disclosed that it has been using Carnivore, a surveillance system that is installed at the suspect’s Internet service provider to scan all-incoming and outgoing e-mails. While the system can be used to perform fine-tuned, court-approved targeted searches, reportedly it is also capable of sweeping searches, potentially enabling the agency to keep tabs on all network communications. Civil liberty groups opposed the deployment of Carnivore on the grounds that the FBI should not be trusted with what amounts to carte blanche authority when it conducts searches on the Internet.

There have also been efforts to internationalise some of these initiatives. For example, the FBI has pushed for the international adoption of CALEA. In the
early 1990s, the FBI held regular meetings with its counterpart agencies in European Union (EU) Member States with the goal of incorporating elements of CALEA into European law. Their collective efforts resulted in an EU Council of Ministers resolution, adopted in January 1995, that mirrored the FBI’s demands. Shortly afterwards, the EU Council agreed a Memorandum of Understanding, which extended the January agreement to non-EU countries that chose to sign. Nations interested in participating were told to contact the General Secretary of the EU Council or the Director of the FBI. And in response to pressure by the signatories, the International Telecommunication Union adopted a resolution in 1997 that called for priority to be given to the harmonisation of technical requirements to make law enforcement interception possible (see Statewatch 1997).

Paralleling these developments, the Clinton Administration engaged in a sustained diplomatic effort to persuade EU Member States, members of the G-8 and the OECD to adopt a global key recovery encryption system fashioned after its Clipper Chip proposal. The initiative was abandoned in 1998.

In short, for a decade, United States law enforcement agencies have struggled at the national and international levels to maintain and, in some ways, to enhance their telecom surveillance capabilities. The struggle raises some important questions: are law enforcement agencies emerging as major players in the control arrangements that govern the design and evolution of telecom networks? If so, what are the implications for the communicative activity that takes place over these networks? The outcomes of the struggle, and therefore the answers to these questions, are far from certain. The modest goal here is to demonstrate that it would be a mistake to view this struggle as being driven solely by the rapid diffusion of telecom technologies.

**Loss of Control and Technology Determinism**

Much of the policy debate concerning CALEA, key recovery encryption, and Carnivore is premised on a jarringly simple logic: the problem is a given; only the means to its solution are in doubt. First, the problem. For law enforcement officials, as well as for many public policy makers and journalists, ‘loss of control’ has been the dominant narrative. The basic story line is that the telecom revolution has plunged state surveillance into crisis; recent and continuing advances in telecom have allowed organised crime to leap ahead in its contest with law enforcement. Without remedial action by industry and government, it is argued, these new technologies will bring about a *de facto* repeal of the existing telecom surveillance authority conferred upon law enforcement agencies. A
comment by former FBI Director, Louis Freeh, exemplifies much of the policy discourse:

... new and advanced telecommunications technologies ... have come on line and others will soon. They gravely impede or totally prevent court-approved surveillance... . Without an ability to wiretap, the country will be unable to protect itself against foreign threats, terrorism, espionage, violent crime, drug trafficking, kidnapping and other crimes. Indeed, we may be unable to intercept a terrorist before he sets off a bomb... . Unable to arrest traffickers smuggling in huge amounts of drugs that will cause widespread violent crime and death (Freeh 1994).

The focus in this discourse is on the loss of state control and its consequences, as well as on the technical change that has supposedly precipitated this loss. A solution to the problem is embedded in the story: the state must regain control. Since the problem is essentially a technological one, the solution must lie in the technical domain. CALEA, key-recovery encryption, and Carnivore, it is argued, will allow law enforcement to close the technology gap on criminals. As a result, state control over criminal activity will be re-established.

Many industry actors and civil liberty advocates have challenged the recent surveillance initiatives of law enforcement agencies. The challenges take at least three forms. Accepting the loss of control narrative, the first kind of challenge focuses on what are perceived to be the unacceptable costs of the initiatives. For example, it is often argued that the initiatives will obstruct or distort technological progress, impair the security of telecom systems, and reduce the competitiveness of American-owned hardware and software companies in foreign markets. Equally as often, it is argued that the initiatives inevitably will result in the erosion of civil liberties. The second kind of challenge begins to question the loss of control theme but stops short of providing an alternative narrative. For example, some critics have argued that there is little or no empirical evidence to support the claim that new technology routinely has hamstrung law enforcement’s ability to intercept and monitor electronic communications. The third challenge combines elements of the first and second. Accepting that the state’s loss of control claim may be valid with respect to telecom networks, some argue that this is more than offset by developments in thermal imaging, facial and behavioural recognition systems and DNA testing.

Most of the arguments outlined above contain grains of truth. However, the basic problem is that the general acceptance of the loss of control theme, and its
attendant technology determinism, has led to a fundamental misunderstanding of the state’s recent initiatives. Specifically, the stress on loss of control, and on the technical innovations that have supposedly resulted in this loss, greatly understates the degree to which the state has actually structured, conditioned and even enabled (often unintentionally) the kinds of organised criminal practices that state telecom surveillance is supposed to help control. That is, by characterising the state as purely reactive, the loss of control theme obscures the ways in which the state and other social forces have helped to create the very conditions that have generated calls for new electronic surveillance powers.

THE WAR ON DRUGS AND THE LOGIC OF ESCALATION

The claim, then, is that the loss of control narrative conceals more than it reveals about the forces that have propelled the recent telecom surveillance initiatives. The following provides a sketch of an alternative narrative that places the agencies of the government front and centre.

With the passing of the Soviet Union from the historical stage, concerns about organised crime joined with terrorism to dominate the domestic and international security agenda of the United States. This shift in priorities is reflected in the fact that law enforcement has been the fastest – and one of the only – areas of federal government expansion in the last decade or so. The state’s ongoing War on Drugs has been the key factor driving this expansion (Andreas 1999). Characterised by the language, strategies, and tools of military deterrence, the supply-side approach is premised on the notion that the best way to solve problems of drug abuse and addiction is to prohibit the supply of illicit drugs. It has been very evident that this approach has failed miserably; both the supply of drugs and levels of abuse and addiction remain high in the United States. Moreover, the collateral damage associated with the supply-side approach has been staggering (Bertram et al. 1996). In spite of this dismal record, the policy response to this failure has been to escalate the supply-side approach by getting tougher. The War on Drugs in the United States illustrates both the power and the limits of the state; even as the state fails to deter the illicit drug trade, there is no illicit drug trade without the state.

The dynamics of the supply-side approach have played out in the domain of state telecom surveillance. As the state stepped up its War on Drugs, the ability to wiretap was portrayed as a key supply-side tool. As former FBI Director, Louis Freeh put it: ‘Court-ordered wiretapping is the single most effective investigative technique used by law enforcement to combat illegal drugs’ (Freh 1995). Law enforcement’s fixation with the anti-drug offensive is reflected in official wiretap
data. Since 1990, the majority of reported wiretaps have involved drug-related investigations, ranging from 60% of all applications in 1990 to 75% in 2000 (Administrative Office of the United States Court 2001). This is in the context of a sharp increase in the overall number of reported wiretaps. Leading law enforcement officials offer these statistics, and other body count numbers—number of drug traffickers captured, amount of drugs seized and destroyed, and so on—as evidence of their success, even as the drug supply flows unabated.

Many of the technologies associated with the telecom revolution have presented businesses in the illicit economy with opportunities for greater efficiencies. For example, drug traffickers have used cell phones, pagers and encryption-enabled phones to better coordinate supply and distribution activities as well as to more efficiently evade law enforcement (Constantine 1997). It can be argued that law enforcement’s more intensive use of wiretapping as a supply-side tool provided drug traffickers with an incentive to rely on telecom technologies that are widely publicised as being difficult to tap.

The policy debates on CALEA, key-recovery encryption, and Carnivore depict these developments as a major loss of state control. Assuming the moral correctness of the supply-side approach, the problem is viewed as a technological one; advances in telecom are enabling drug traffickers and other criminals to circumvent the law. CALEA, key-recovery encryption and Carnivore are portrayed as defensive responses that will help restore control. This is misleading. It glosses over the fact that the state’s failed supply-side approach to the illicit drug trade has created the conditions that have led to the calls for these surveillance initiatives. It is the very existence and enforcement of supply-side controls that have made it necessary for many drug traffickers to try to circumvent them by using new telecom technologies. It is this dynamic, not technical innovation per se, that has called forth the surveillance initiatives.

CALEA was enacted and Carnivore has been deployed, while the key-recovery encryption initiative floundered. CALEA and Carnivore, themselves partly products of supply-side escalation, can be viewed as visible signs of the state’s resolve that may well create the conditions for further escalation. For example, in the late 1980s and early 1990s, drug-trafficking organisations used cellular phones, in part, because they could evade law enforcement telecom surveillance more efficiently. As law enforcers met this challenge, with advances in interception technology and the passage of CALEA, the more sophisticated drug traffickers began to use cloned cellular phones to conduct their business. By the time investigators identify a violator who is using a cloned phone and follow the
traditional path of gaining court-authorised permission for a tap, the violator has moved on to the next cloned phone, thus staying one step ahead of law enforcement (Bocchicio 1997). Drug traffickers who respond to law enforcement supply-side techniques with more sophisticated methods provide a rationale for better supply-side tools. Law enforcement officials can thus simultaneously praise their progress (the passage of CALEA) and point to the emergence of a formidable new enforcement problem – cloning of cell phones – which in turn is used to justify further regulatory measures. Escalation, in other words, feeds upon itself.

**Conclusion**

Following Melody’s example, I have shown that technology determinism narrows the scope of policy analysis to encompass only those changes within the established institutional structure. In the debates over telecom surveillance initiatives, technology determinism, functioning through the loss of control narrative, has served to deflect critical attention from the failed supply-side approach to the problem of the illicit drug trade. This has benefited those institutional interests that have gained most from this approach – the law enforcement establishment.

The alternative narrative may add a fresh policy-relevant perspective to the debates on recent state telecom surveillance initiatives. For example, the loss of control narrative suggests that some erosion of civil liberties may be a necessary cost as the state battles to regain control so that it can once again protect public safety with confidence. The alternative narrative suggests that it may be more accurate to view any erosion of civil liberties that may occur as yet another instance of collateral damage resulting from the War on Drugs. The narrative also suggests that a fundamental re-evaluation of drug policy in the United States would have important implications for the state’s telecom surveillance policy.

The attacks on the World Trade Center and the Pentagon in September 2001 have greatly intensified the debates over the state’s telecom surveillance powers. Congress has passed the USA-Patriot Act of 2001, which significantly enhances law enforcement’s wiretapping capabilities. It also removes or reduces judicial oversight from a number of wiretap procedures. The debates on this legislation and other legislative proposals are taking a familiar shape: law enforcement agencies and policy makers are stressing a loss-of-control theme as the justification for more telecom surveillance powers. Questions about the role of the state and other social factors in shaping the ‘new’ threat are being pushed into the shadows amid the struggle to regain control. The loss of civil liberties is being viewed by many as a necessary sacrifice in this struggle.