Chapter 1

Introduction: technocrime

Technocrime does not exist. It is a figment of our imaginations. It is simply a convenient way to refer to a set of concepts, practices, frames and knowledges shaping the ways in which we understand matters having to do with the impact of technology on crime, criminals and our reactions to crime – and vice-versa: since crime, criminals and reactions also transform technology. Technocrime includes crimes against computers; crimes committed with computers; cybercrimes; and crimes involving credit cards, automated telling machines, communications apparatuses (such as satellite signal theft) or the violation of protection strategies (including alarm systems and CD/DVD copy protection schemes). Technocrime gives rise to technosecurity and technopolice, as sets of various activities explicitly designed to prevent or repress it (for a complete inventory, see Byrne and Rebovich 2007). These responses are openly justified by descriptions of 'new' technocrimes, with more lurid or horrifying behaviours calling for stricter laws, restrictions of due process rules and higher enforcement budgets. But it should not be assumed that technopolicing follows technocrimes. It may also simply be the logical extension of security and policing into the high-tech world.

Though private forms of technosecurity are clearly at the vanguard of high-tech crime protection, the state remains the leader in more exotic, generalized forms of applied, high-tech security (national security, military security) – though it relies on private industries for most of the tech provision, of course.

Much has already been written on new technologies, crime and security. Most of it leaves the sociologically inclined mind unsatisfied:

crime, like technology, comprises objects not easily observed or measured and it involves various practices. These are sociological objects: they are modified by culture and they modify culture. This books attempts to explore new avenues and to re-examine a number of trends in the literature about crime and technology:

- *Technology is a new way of doing crime*: the emerging high-tech toolset that criminals have at their disposal makes them more dangerous, to more people – crooks can con better with technology; paedophiles can lure their victims better; and anyone can harass, defame, threaten or blackmail better with technology. In other cases, technology makes criminals dangerous to new people in entirely new ways: previously unthinkable crimes have appeared, such as website defacing, circumventing copy protection schemes, the denial of service attacks and digital rape. Cybercrime and computer crime are the bane of the information society.

- *Technology is a new way of doing policing*: the policing tech toolbox has drawn much attention in professional publications, in official government reports, in the media and, to a lesser extent, in the scientific literature. New cybercops and netdetectives have been at the centre of news reports. Their cyberwatch and netvigilance outfits have not been thoroughly studied but certainly have grabbed media attention as the new professional, expert police elite, or at least one form of an advanced, future-oriented way of doing policing. New tools in the fight against crime have created controversy, such as the Taser and other so-called 'less than lethal' weapons. Others seem drawn from science-fiction movies: pulsed energy projectiles, infra sound, lasers, microwave and chemical riot-disruption weapons, as well as many others.

- *Technology is a new way of threatening national security*: cyberterrorists have been using advanced steganography and other advanced encryption tools to disseminate crucial information to their accomplices. They have plotted online in chatrooms and on Arabic language bulletin boards. Canadian Momin Khawadja sent UK bomb plotters emails telling them how he could build efficient detonators for them – fortunately, he was caught in the National Security Agency's top-secret SIGINT communication interception net. A 'cyber Pearl Harbour' is looming, with attackers targeting essential infrastructures in attempts to cripple economies. They will co-ordinate attacks on Supervisory control and data acquisition (SCADA) computer systems and on other targets selected to

produce cascading failures along our highly interconnected infrastructures.

- *Technology is a new way to* protect *national security*: massive database analysis, information sharing across state and private entities, real-time crime mapping, transaction surveillance, and more efficient communication between security and police entities, as well as *within* those agencies, will enhance our ability to fight crime, terrorism, subversion, industrial spying and other international threats. It will also help manage emergencies when prevention was insufficient or when natural, unpredictable events occur. Later, technology will help us prosecute, punish and watch those responsible.

- *Technology is a new way to encroach on civil liberties*: physical surveillance technologies include CCTV and an increasing number of innovations such as night vision, face recognition, gait recognition, computerized emotional state visual recognition, behavioural analysis and cross-system, camera-to-camera tracking. Physical surveillance also includes satellite imaging, city-wide sound analysis and location, mobile-phone radars, backscatter X-ray and many other technologies in development or already in use. To this must be added information surveillance or 'dataveillance' technologies, through biometrics, datamining and database interoperability. Linking those various forms of information and structuring them with social and psychological behavioural models will allow the creation of individual profiles more complete than the image individuals have of themselves.

- *Technology is a new way to protect civil liberties*: automated systems may see, hear and read everything, but they are devoid of ill-intentions, have no interest in publishing personal information, cannot benefit from blackmail, are free from political bias and do not care about our sexual preferences, personal quirks or the stupid mistakes we make. Automated systems are programmed to recognize threats to national and personal security only (of course, they are still programmed by humans).

The above contradictions should cause no surprise. Behind the new jargon of technology, mostly influenced by science fiction (for instance, the omnipresent 'cyber-' prefix inspired by Willam Gibson's 1984 *Neuromancer*), hide the same hesitation, controversy, conflicting politics and cultural constructs that have always been

integral to all attempts at defining crime and criminals and to devising our responses to them. In fact, much of technocrime shows that constructivist approaches are much more powerful ways to account for reality than conventional, more essentialist or naturalistic approaches. More than ever, crime is what 'we' make of it and is 'real in its consequences,' to paraphrase W.I. Thomas. Furthermore, as the chapters below show, this 'we' is more problematic than ever – most obviously when new laws criminalize mass behaviours. It is not surprising, therefore, that much of the analysis and nearly all the political discourse about technocrimes, consists of analogies with conventional crimes (filesharing is high-tech shoplifting).

Though much of the activity of the social sciences has also contributed to establish crime as a natural, objective, essential behaviour, the tech language offers an even stronger gloss of objective certainty. Contrary to the social disciplines, technology from the 'hard' or natural sciences takes human beings to space, allows remote-controlled surgery, helps us travel around the world, cures diseases, etc. Its less spectacular achievements are closely enmeshed in our daily activities: our work, entertainment, communications, learning, our very awareness of our world. When we are told there is such a thing as 'computer crime,' the concept seems closer to the natural laws that gave us computers than to the artificial laws that gave us crimes.

In many ways, technocrime also points to the critical flaws of late-modern society, the fragility of its technological structure, the unknown consequences of the deep demographic and social changes it has triggered and the general insecurity it has failed to alleviate. For others, technocrime encompasses an ordinary voyeuristic fascination with criminal behaviour, intriguing police drama and exciting technological gadgets. Either way, it makes good copy.

In reality, technocrime is a Gordian knot of political interests, economic interests, legal rules, technological developments, police, private security and forensics expertise, mass individual desires, geopolitical strategies and other forms of power we have yet to map. Some of the chapters in this volume, through their investigations of certain forms of 'crime' in the cyberworld, show how some of the most fundamental theoretical questions pop up in the most common activities of netizens. Is it possible to 'rape' an avatar? Can a virtual object actually be 'stolen'? (see chapter 6)? Or are we just pasting our common understandings of damage and tort on new, uncharted

regions of human behaviour and stretching language in order to describe things that it is clearly inadequate to describe?

Governing through technocrime

In a recent book, Simon (2007) described the increasing tendency of western societies to organize life with the help of systematic criminalization and police control. Wasteful, dangerous, risky, unhealthy, economically threatening and merely irritating behaviours are constituted into crimes or other forms of penal offences and watched, prevented, repressed and punished with the classical tools of the penal state. The mentally ill, the working poor, children, social assistance beneficiaries, immigrants, drivers and many others are being watched for potential criminal activity. Phenomena previously taken as social problems are now crime problems.

State response to such problems takes two broad forms: first, the penal system is used to individualize responsibility for crimes. 'Justice' will make those responsible pay for their actions. The previous failure of mega-social programmes to eradicate a variety of target problems (poverty, addictions, etc.) also helps funnel resources towards individualized conceptions of the problems. While crime was previously taken to be a symptom of social problems, it is not rare today to hear the exact opposite discourse, where poverty, social disorganization and citizens' retreat from public spaces in their neighbourhoods are the symptoms of a deeper crime problem (especially since Wilson and Kelling's famous 1982 paper). Secondly, since crime problems are conceived of as constant, background *risks* for all citizens, which must be *managed* through behaviour modification, situational prevention and target-hardening, much of the actual work needed can be left to individual citizens (and their private agents, should they choose – and if they can afford it – to entrust professionals with their security).

Much of technocrime operates in the same way. For instance, cybercrime is being used to justify and to encourage the monitoring of online activities and to create new responsibilities for various actors: parents watching (over) their children, employees watching other employees, employees watching their employers, employers watching their employees, spouses watching (out for) each other, Internet Service providers (ISPs) watching their customers and retaining data about their activities online, etc. The cyberworld, much like the real world, is fraught with ill-intentioned individuals who

are adept at disappearing into the massive quantity of activities and people online. Therefore, all must be watched.

More than in any other type of late-modern policing, technopolicing involves multiple entities, and conventional, state-centred police organizations are but one actor in the overall production of technosecurity. The actual breadth, depth or intensity of corporate policing online will never be known, but indications are that it is quite extensive. Traditional police organizations routinely ask corporations to produce near-complete investigations and evidence packages before they take over and proceed to submit the case to prosecuting attorneys. This is in part because the police have little resources, both in terms of tech-savvy investigators and analysts and in terms of the technology itself. Corporations and especially those most at risk of cyber-victimization, have, on the contrary, the required know-how, technology and, of course, a much more immediate, pressing motivation. However, it would be a mistake to conclude that actual, concrete surveillance and control of our activities are rampant. Because of dysfunctional technologies, incompetent users, low priority or simply the extremely high number of targets, technosecurity remains (for now) more talk than consequence.

In fact, one interesting aspect of technopolicing is how it is functionally split from traditional, conservative and far more common policing. In the case of conventional crime analysis, civilian expert analysts are typically at the bottom of the police respect/influence ladder. They do not have on-the-street crime experience and are not trained crime investigators; they have not proven themselves in the field; and they are thought of as 'outsiders' which, in police culture, means untrustworthy. This attitude is only worsened for analysts who focus on weird, complex or non-physical crimes.

However, a 'technopolice brigade' also exists: officers and admini-strators whose actions and influence pull the other way – the more the tech, the better the policing. The most spectacular success story for technopolice enthusiasts is the adoption of the 'Compstat' ethos and technologies, introduced by Bill Bratton in New York in the 1990s, but slowly making its presence felt throughout the world (with various degrees of success; I witnessed a 'Compstat' session in Philadelphia in 2005 where crime mapping was at best a form of visual support for an otherwise rather ordinary police briefing). British 'Intelligence-led policing' (ILP) is also tech-heavy. Compstat relies in part on crime mapping software (MapInfo) and on the experts needed to make it work. However, crime mapping was introduced primarily as a management tool and is only beginning to be used to

devise responses to crime. For now, such responses are limited to the conventional forms of increased (visible and invisible) presence and crackdowns. The *reasons* why crimes occur are deemed immaterial to police work. Paradoxically, then, the new technology has allowed the police to revert to ancient tactics.

Technology certainly permeates policing in one area: in North America and elsewhere, *weapons* technologies and often military technologies, are increasingly adopted by civilian police forces and by private security services. Many authors (but especially Kraska 1999) have already described how the militarization of policing is mainly driven by the increasing adoption of military weapons and the tactics and strategies they impose. Current controversy about the misuse of electrical pulse weapons, commercialized mostly by Taser International, shows how police safety is currently perceived as depending on the correct technological tools (which would include powerful firearms, bulletproof vests, CS/mace/pepper spray-cans, etc.) – in other words, despite declining crime rates, public policing is increasingly seen as an antagonistic, violent, high-danger occupation.

Robots are mission-oriented, autonomous systems and, as such, police robots remain in the realm of science fiction. However, current remote-operated observation and intervention platforms, though always mistakenly referred to as 'robots,' do open the way to even more spectacular technologies, like the eventual operation of 'real' robots. These are already available on the private market: small devices making random surveillance rounds in empty buildings, swapping their own battery when needed, notifying human watchers when suspicious occurrences are detected; and some can be equipped with weapons. It is difficult, at this time, to imagine how policing, security and crime will be modified by the probably inevitable adoption of such technology – but it is certainly a fascinating exercise.

Strangely, as is apparent in Peter Manning's chapter (Chapter 11), technopolicing, by and large, *does not work*: 1) it does not reduce crime, it does not make citizens less afraid of crime, it does not make cops happier with their work; 2) it also does not work for purely technical reasons; 3) and, finally, it does not work because it does not match the conception police have of their mission. Of course, one might argue that the situation is not unlike that of conventional policing: though crime will never be eradicated by policing and actual policing effects on crime are not often measurable, the complete *absence* of policing could conceivably result in an explosion of criminality. In other words, without technopolicing, the technocrime problem might

be *worse*. Whether or not one is sceptical about such pronouncements, they are certainly far too vague to provide any form of interesting conclusion about the nature, effects and interactions of technopolicing with technocrime. Be that as it may, regardless of the actual impact of technopolice on our reality, its vertiginous amplification and spiralling costs certainly make it an interesting social and political phenomenon.

Structure of the book

This book covers many aspects of the technocrime question, though many, many more remain untouched. Chapters vary not only in their subject matter but also in their theoretical and empirical density. Chapter 2, by David Brin, accomplished science-fiction author, is an extension of his controversial opus, *The Transparent Society* (1998). Brin offers a thought experiment: what if the technology of surveillance could become sufficiently democratized to offer viable counter-surveillance? There is an abundance of evidence showing that watching those in authority renders them more accountable. The news is full of politicians captured by mobile-phone cameras after hit-and-run incidents, of videos of police officers beating suspects (the most famous case remains that of Rodney King in Los Angeles) or tazering them to death, of military public-relations personnel adjusting Wikipedia entries to reflect a better image of operations abroad, etc. Brin concludes that counter-watching, or what Mann (Mann *et al.* 2003) calls 'sousveillance', is not a techno-fantasy or a gadget obsession – one might add that it may never work very well – but is the only means by which we will maintain a modicum of ruling-class and institutional accountability in the future.

In Chapter 3, Stéphane Leman-Langlois reports on an ongoing study of ordinary people's perception of police CCTV. The author ran some group interviews in an area of downtown Montreal (Canada) and asked residents, shop owners and employees whether cameras had an effect on them: did they feel safer; did they think their privacy was threatened? As it turns out, cameras were almost universally deemed to be irrelevant to all aspects of every participant's day-to-day life. In fact, when asked about their security, residents living in direct view of the well publicized cameras almost never actually mentioned them. Their insecurity was caused by social indifference, by the felt absence of either community or police help in times of need. It was also caused, predictably, by visible signs of disorder,

such as discarded needles and graffiti. Finally, it was also caused by random, unpredictable behaviours taking place in their own buildings or anywhere on the street, regardless of the presence of cameras. The obvious conclusion is that CCTV is disconnected from the reality of the street and that an increased police reliance on CCTV is perceived as a progressive disconnection of the police from the reality of city life: to these respondents, 'policing through the lens' (Leman-Langlois 2003) is policing the irrelevant.

Benoît Gagnon, in chapter 4, tackles a number of new buzzwords in the media and the specialized literature: 'cybercrime' and 'cyberwar'. Comparing US and Chinese government cyberspace presence, he concludes that both are moving towards a militarization of their approach. This implies and, in fact, rests on, an increasingly nationalized view of what takes place on the web: both powers present cyberspace as territorial, 'national' space where government sovereignty can be asserted. In both cases there is also an obvious intensification of government presence in cyberspace, especially through military institutions. As a part of the national infrastructure – in fact, an important, underlying part, since it allows most of the other elements to be connected together – any form of 'misuse' or 'misbehaviour' on the web can be perceived as a threat to national 'cybersecurity'. Though of course the precise manner in which national security is conceived of differs profoundly between China and the USA, the result is the same: a rapidly increasing desire to control cyberspace.

Chapter 5 gives a fascinating glimpse into the structuring of part of what has been called the 'surveillant assemblage:' how the police, the justice system and private enterprises network and organize to control online activities identified as dangerous, immoral or damaging. As described by Johnny Nhan and Laura Huey, the assemblage is fraught with problems of various kinds: unreconcilable legal requirements, inter- and intra-agency rivalries and epistemological differences regarding the nature of crime, public police intervention and public morality – not to mention the simple lack of resources allocated agencies tasked with fighting cybercrime.

Chapter 6 attempts to chart entirely new territory: crime and punishment in virtual societies. The example presented by Jennifer Whitson and Aaron Doyle is the computer realm of Linden Lab's *Second Life*. Still mostly considered to be games or simple hobbies by much of social science, online worlds are in fact nothing less than massive social experiments where many of the fundamental objects of sociology and criminology, such as rules, deviance and human

agency, are reconfigured in real time. Group and individual dynamics are observable and accessible, social relations are restructured, new forms of deviance are identified, prevention and repression activities take shape. Politics, financial interests and legal pressures both in-world and out-world (the 'real world') influence this continuously richer reality, as courts, the police and the media begin to pay attention to what is happening. Though the future of 'second lives' of every type is difficult to predict with any degree of accuracy, one can reliably predict substantial growth and probably the progressive enmeshment of virtual lives with aspects of the real world. It remains to be seen whether this entanglement will make the virtual more concrete, or if it will reveal what we take as concrete as constructed, artificial and virtual.

In Chapter 7, Stéphane Leman-Langlois considers the development of the concept and discourse of 'privacy' online and in virtual worlds. It is the author's contention that privacy is being progressively redefined by our online activities, where much of our enjoyment of various cyberworlds – from the simple search field and results on Amazon.com to more complete realities, such as Second Life – is dependent on our willingness and ability to share information about ourselves with various known and unknown entities. One can better understand this change by thinking of privacy as a new form of currency, exchangeable for various goods, services, information, entertainment and what amounts to simple comfort in existing and acting online. If this assessment is correct, identity and privacy will lose any reference to a private inner sanctum, a sphere of intimacy to be kept secret or shared only with immediately present, trusted persons. A 'right to privacy,' therefore, will move closer to a right to property, where personal information is withheld only until a benefit is offered in exchange. This has several interesting implications for surveillance and control online, of course. One of the more obvious is that, since information flows are far from equivalent – some are personal and 'worth' something only when combined and aggregated while others from multinational corporations depend on profitability – all breaches of privacy/information property rules are unlikely to be policed equally.

In Chapter 8, Frédéric Lemieux describes how various criminal intelligence outfits have adopted complex IT systems in order to gather, store, manage, analyse and communicate information about crimes and criminals. This is technopolicing at its purest: all those involved believe in the power of technology and information to control crime. New bureaucratic policing management styles,

themselves heavily tipped towards the centrality of information (we are, after all, in the 'information society'), have adopted policing styles sharing the same traits. Intelligence-led policing (ILP) is the prototype of such styles and, of course, was only thinkable when adequate computing power permitted the efficient and timely production of immediately, concretely usable ('tactical') information. Though information management was always at the centre of police (or other) investigations and to a lesser degree helpful in determining general, abstract, organizational missions and medium and long-term priorities, the idea that *all* police work, including patrol, should be 'intelligence led,' is rather new. It has also caused a minor revolution in such organizations through the introduction of expert analysts and their high-tech tools. However and predictably, the *actual* crime reduction effects of that revolution remain difficult to detect.

The impact of technology and science on the conduct of investigations, recent media attention notwithstanding, has rarely been analysed. Jean-Paul Brodeur, in Chapter 9, remedies this situation with a study of a police force's use of forensics and other technologies to solve homicides. In order to construct an empirically based theory of the criminal investigation process, Brodeur first deconstructs the typical assumptions and definitions commonly associated with investigation and finds that they are mostly tautological, founded in semantics rather than empirical observation. In reality, 'solving cases' involves many individuals who are not police investigators and investigators do far more than investigate. The high tech of scientific investigation, so dear to Hollywood writers, mostly comes in when every other way to solve the case has failed – only to fail equally, though far more expensively.

Chapter 10 describes a society where citizenship is a matter not of legal and national belonging, with rights and responsibilities, but of a quantity of benefits one qualifies for. David Lyon explains how, for political, economic and bureaucratic reasons, individuals are increasingly asked to demonstrate that they actually qualify for those benefits – the spectres of freeloaders and crooks are routinely mobilized in public discourse to account for the inefficiencies of state and private bureaucracies. Sorting out the freeloaders (those who benefit without deserving, such as immigrants) and the crooks (those who actively find ways to abuse the system) has become a major focal point of state bureaucracies and technocrats have enthusiastically embraced every new scheme marketed with the promise of sorting the deserving citizens from the others. National ID card systems, radio frequency idntification (RFID) chips, new, exotic types of biometrics

and various yet-to-be-released panaceas are adopted everywhere without serious concern for various questions relating to their actual performance or their total, global costs (including indirect costs to consumers, travellers, etc.). Their social and political costs and, more abstractly, their cultural costs – for instance, how they reconfigure our understanding of citizenship – are, of course, usually not even conceived of or, if they are, they are deemed entirely secondary to efficiency matters.

The final chapter, by Peter K. Manning, offers what may appear, at first, as an opposite picture of that given by Lyon. Manning shows that, in reality, policing through surveillance remains focused on traditional, if not outdated, conceptions of police work. Surveillance on a higher plane, such as described by Lyon and elsewhere in this book, remains impossible in practice. The practical full realization of surveillance on a grand scale may actually never be possible, limited by failing technologies, petty power struggles, disinterest, information incompatibility, legal hurdles and many more such obstacles. The chapter ends with a description of what the police actually do, which illustrates artfully the unbridgeable gap between surveillance and late-modern policing. That said, the question may not be whether or not 'total information awareness' is possible; rather, technology now makes it believable. The goal may seem actually attainable by a critical mass of key politicians, bureaucrats, police officers. And this belief may be changing how *all* policing is being done through, for instance, new models, such as ILP.

Together, the chapters from Lyon and Manning show us the future as a dysfunctional utopia: dreams of total surveillance structuring a progressively more fragmented control.

References

Brin, D. (1998) *The Transparent Society*. New York, NY: Perseus Books.

Byrne, J. and Rebovich, D. (eds) 2007) *The New Technology of Crime, Law and Social Control*, Monsey, NY: Criminal Justice Press.

Gibson, W. (1984) *Neuromancer.* New York, NY: Ace Books.

Kraska, P. (1999) 'Militarizing criminal justice: exploring the possibilities', *Journal of Political and Military Sociology*, 27: 205–15.

Leman-Langlois, S. (2003), 'The myopic panopticon: the social consequences of policing through the lens,' *Policing and Society*, 13: 43–58.

Mann, S., Nolan, J. and Wellman, B. (2003) 'Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments,' *Surveillance and Society*, 1: 331–55.

Simon, J. (2007) *Governing through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. Oxford: Oxford University Press.

Wilson, J. and Kelling, G. (1982) 'Broken windows: the police and neighbourhood safety,' *The Atlantic Monthly*, March: 28–39.