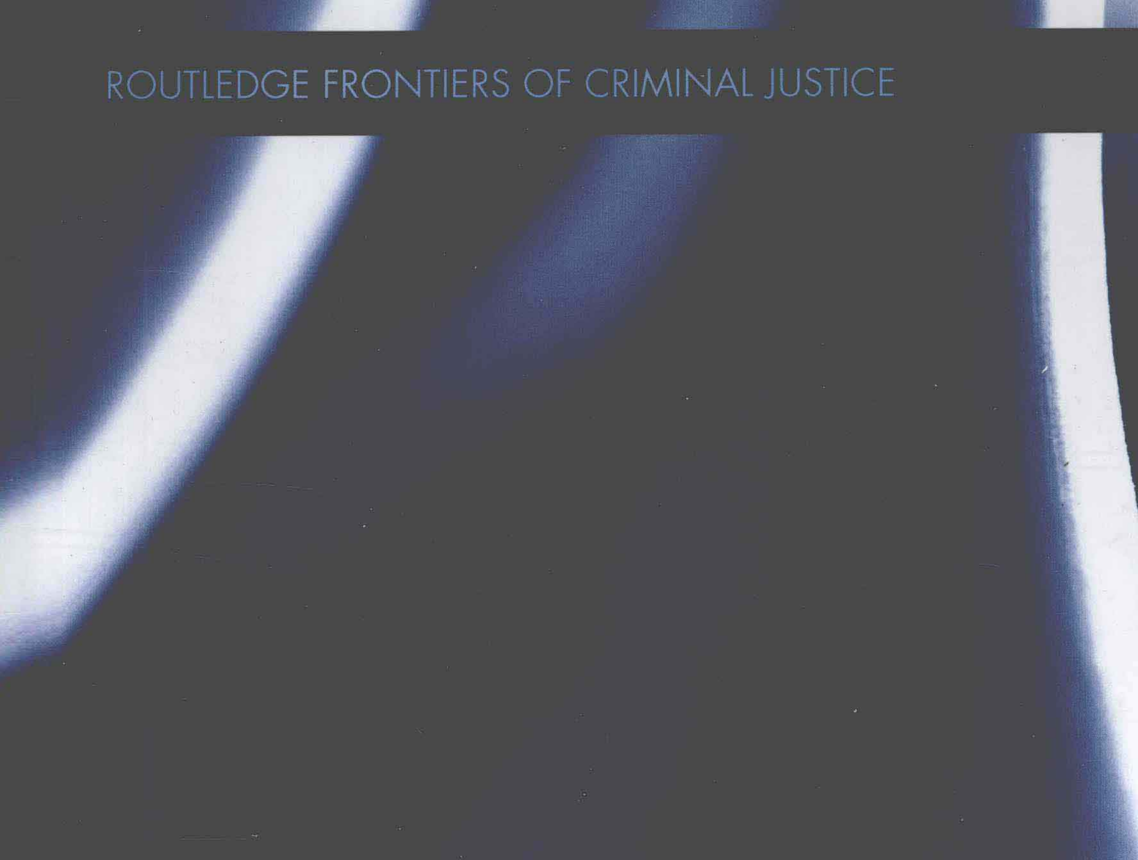
ROUTLEDGE FRONTIERS OF CRIMINAL JUSTICE



Technocrime, Policing and Surveillance

Edited by
Stéphane Leman-Langlois

ROUTLEDGE

Technocrime, Policing and Surveillance

Edited by Stéphane Leman-Langlois

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2013
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

Simultaneously published in the USA and Canada
by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Leman-Langlois, Stéphane, 1965–
Technocrime, policing and surveillance/Stéphane Leman-Langlois. – 1st ed.
p. cm. – (Routledge frontiers of criminal justice)
1. Computer crimes. 2. Computer security. 3. Electronic surveillance.
I. Title.
HV6773.L46 2012
363.25'968–dc23 2012004168

ISBN: 978-0-415-50025-8 (hbk)
ISBN: 978-0-203-10524-5 (ebk)

Typeset in Times New Roman
by Wearset Ltd, Boldon, Tyne and Wear

MIX
Paper from
responsible sources
FSC
www.fsc.org
FSC® C004839

Printed and bound in Great Britain by
TJ International Ltd, Padstow, Cornwall

Foreword

The term cybercrime is an intriguing and misleading neologism; like all new media-created words, it has contradictory and inconsistent referents. From *Ask.com* on cybercrime I quote:

> Computer crime, or super crime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Netcrime refers to criminal exploitation of the internet.

Cybercrimes are defined as:

> Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

Let us consider these attempts to pin down meaning. How can one circumscribe 'any crime that involves a computer or network'? Such a formulation begs the question of 'crime'. Furthermore, it is a unique sort of definition of crime in that it hinges on the means used to achieve it. Should burglary then be called 'screw-driver crime', 'lock-picking crime' or 'breaking-windows crime?' Now consider the matter of intention. 'Intention' has a noble history and again is dependent on the circularity of the definition – if one has been proven to have done something, it is defined as an intentional act. 'Physical *or* mental harm?' Surely that is a morass of complex speculation. 'Directly or indirectly' is again a quicksand of meaning.

Leman-Langlois argues very cogently in his introduction that the idea of 'cybercrime' is a clever, misleading term derived from media aesthetics – the result of the arts of producing profit-making unreality. As a media creation it lacks the fundamental elements of crime: motive, intention, opportunity and gain. And as the courts in their wisdom have specified, such actions are not only matters of freedom of speech in the United States, they impinge upon matters of reputation and character covered more by civil than by criminal law. Certainly, the interests that may be at issue are more likely to be questions of 'property', as such are asserted by the large internet corporations that control information, music, art and other social capital found in 'private spaces' on the internet. Perhaps also it is anomalous, like many modern delicts, in that it is a collective affront or incivility – a victimless matter that engages and worries many people. It has elements of a sensate, 'expressive' status-based violation. Why is it worrying? Its ambiguity, of course, is a reason for its popularity and wide-spread use. Its referential emptiness means it is easily filled with many contradictory notions.

As the chapters in this well-focused book demonstrate, 'cybercrime' is a mysterious unanticipated aspect of the most significant invention of the late twentieth century: it produces new forms of policing based on the flawed past 'case method' (Lemieux and Bales); it has world-wide consequences (Ribaux and Hicks); it is linked to the media in general fashion (Finn and McCahill, and Sheptycki), while the complex reflexivity that the technology and the crimes associated with it produce and amplify interest in it. Byrne and Pattavina – examining the uses of electronic tracking and auditing – show how the temptations of efficiency and technological solutions trump close evaluation of offender monitoring. Technology-based offender monitoring is yet another form of a longed for 'silver bullet'. A content analysis of the media (Finn and McCahill) does indeed raise questions about whether this is a single uni-dimensional thing, or an ensemble of contradictory meanings that are bundled haphazardly by the media. Since it is a kind of property crime via fraud, as Dupont observes, these are not entirely new forms of delicts.

As the introduction points out, cybercrime is troubling because of the quasi-labelling aspect of being seen as a 'crime': the representational aspect of the idea; its general and world-wide status as a problem; the false assertion of causation by technology and its interactive relationships to efforts to control such matters – 'technopolicing' and offender monitoring. It has been with us for quite some time, at least since the beginning of wide-spread use of credit cards (Dupont), and the 'threat' entailed is commercial and not entirely personal. It is analogous to white-collar crime, crime associated with trusted members of the middle classes.

One might ask, then, as does Sheptycki in this book, why is this bundle of affronts of interest to criminologists and sociologists? This media-driven interest in cybercrime does not appear to be the result of a 'moral panic' in the sense that a set of moral entrepreneurs have advanced the idea as a way to stir up public opinion and to encourage the passing of new laws. It is not clear who is to gain by such laws but it is clear, as Lemieux and Bales show, that the FBI and other federal agencies are clueless in respect to enforcing them in a creative and meaningful fashion. As Byrne and Pattavina show, the adaptation of both soft and hard technology to track ex-offenders runs ahead of a clear understanding of why this mode of control is adopted, for whom it is best suited and the consequences of its use. Huey and Nhan extend this analysis, contrasting televised versions of reality and actual DNA-based investigations. Perhaps fears amplified by experts and reified in new technologies are a central part of modern governance.

Let us consider some other theoretical frameworks within which to consider technocrime. Technocrime does not fit easily to a 'cultural lag' explanation, in the sense that technology leads and responses to changes are reflected in shaping subsequent social relations. Modern life is trumped and surpassed by the phantasmorgic realities of television and their fetishising of 'crime' and 'policing'. We are all thoroughly mediated. We live in a media-led, virtual, multiple-reality created world in which crime is then embedded. It should be appreciated also that 'technology', the source of social change, is not a thing, not a mere means of making work easier, it is a cluster of techniques, material factors, uses and playful associations that arise in the course of doing work. It both causes change and is changed by social factors. It produces technological dramas and resistances that are both legal and illegal in character (Manning, 1992). Such an ensemble cannot be alone, a cause or consequence of conventionally defined crime. On the other hand, these fine chapters show that the social process of defining, acting towards, reacting to and redefining the social object, is the process by which it is constituted (especially Sheptycki's chapter). Conflict theory suggests something about the class-based nature of the crime and its victims. The difficulty here lies directly in the history of all such efforts to control a 'crime' that is essentially a direct consequence of that which is highly valued and an essential aspect of the economy. It is carried out, so far as we know, by intelligent, well-educated and middle-class people; it has blurred and barely discernible direct effects; it is complex and imaginative in nature and therefore very difficult to systematically and effectively police (see Ribaux and Hicks). We lack the necessary data to explore its incidence and prevalence. Labelling or deviance and reaction tells us, as Leman-Langlois notes in his introduction, that efforts to control technology via laws, enforcement agencies and 'technopolicing' produces the social object of interest, 'technocrime'. It thus possesses reality: created, labelled, given meaning and controlled by the actions directed towards it.

These well-written chapters convey something about the reflexivity of these matters of 'crime'. The present concern somehow captures the worries of our age: about 'others', 'illegal immigrants', collective and individual security; identity and the multiplicity of easily acquired and lost identities; familial and individual privacy; forms of terrorism or unanticipated surprise 'attacks' on what is valued; changes in the nature of status, class and 'property' and its definition; and the blurred line between the 'public' and the 'private' spheres. These are the parts that somehow interact in the domain that is 'technocrime'. Or perhaps it is a new form of risk-taking, play and leisure that can be carried out while simulating study at a Tim Horton's or a Starbucks. It resembles in this regard the reactions, personal and collective, that new drugs such as coffee, marijuana and LSD caused when they were first introduced. Reactions to the effects of ingesting these drugs caused people to act unpredictably, wildly and in frenzied modalities. The media of the day then attached interest to this behaviour and as it became stylised and recognisable, modes of social control were invented to control the outbreaks. The victims were demonised until the feelings and sensations became expected, enjoyable and conventionalised. As something of a mystery, such behaviour was both confused and confusing to audiences. It was dramatised as dangerous, yet it was part of the routine leisure activities of large numbers of people in the middle classes and could not easily be dismissed as hysteria or madness. The behaviour was then imitated, sought and diffused, and became part of being 'high', 'having a buzz on' and being addicted. Video games and simulations of crimes are addictive, ludic in nature and autotelic (self-rewarding) just as the behaviour of 'technocrime' is. They are woven into the nature of routine, everyday middle-class education and leisure. The very skills that are needed to commit these acts are taught daily in grade and high schools, community colleges and universities. This is, in part, why society is ambivalent about what, why and how one can regulate such behaviour. In this context, Dupont's chapter underscores a number of emerging truths highlighted also by Leman-Langlois. Dupont points out, as do others in this book, the structural aspects of such deviance and its systematic relationships to the consumerist debt-based economy of exchange and the status anxiety that arises from placing the self-as-card in jeopardy. Using 'plastic magic' is always something of a gamble with status.

As expert observers have long known, societies get the crimes they deserve, those that reflect their dreams, hopes, wishes and fears. Technology is a great mirror of our times. Technocrime is a wide screen on which people can project their deepest wishes and fears, the grey side of a mass consumerist society.

Peter K. Manning
Northeastern University

Reference

Manning, Peter K. (1992) 'Technological dramas and the police: statement and counter-statement in organizational anal\ sis', *Criminology*, 30 (3): 327–346.

Contributors

Brian Bales is Intelligence Officer at the National Security Agency (NSA) Threat Operations Center. He completed his master's degree at The George Washington University in 2010.

James M. Byrne is Professor in the Department of Criminal Justice at the University of Massachusetts, Lowell. He has been teaching at the University of Massachusetts since 1984. James Byrne received his undergraduate degree in Sociology (Summa cum Laude) from the University of Massachusetts, Amherst, and his Masters and Doctoral degrees in Criminal Justice from Rutgers University. He is the author of several books, monographs, journal articles and research reports on a wide range of criminal and juvenile justice policy and programme evaluation issues. James Byrne's research interests include institutional culture, intermediate sanctions, offender reentry, violent crime and the effectiveness of various forms of offender treatment and control.

Benoît Dupont is Professor of Criminology at the Université de Montréal and Director of the International Centre for Comparative Criminology. He is also the holder of the Canada Research Chair in Security, Identity and Technology. His areas of interest include the governance of security – especially the functioning of security networks – the impact of new technologies on policing and the impact of mass surveillance on privacy. He recently co-edited a book with Jennifer Wood entitled *Democracy, Society and the Governance of Security* (Cambridge University Press, 2006).

Rachel L. Finn is an Associate Partner at Trilateral Research & Consulting, LLP, London, UK.

Tacha Hicks received her MSc and PhD, both in Forensic Science, from the University of Lausanne. She has co-authored a book on glass interpretation, acted as a section editor of an encyclopaedia of forensic science and published articles on the topic of evidence evaluation. After working for three years at the Forensic Science Service as a forensic researcher, she returned to Lausanne and completed a post-doctorate work on the use of DNA profiles and DNA database for investigation. She is currently teaching, with her colleagues from Lausanne, full online courses on statistics and evaluation of forensic evidence.

Laura Huey is Assistant Professor of Sociology at the University of Western Ontario. She is the author of several articles on issues related to policing, victimisation, forensics, and surveillance and counter-surveillance. Her book, *Negotiating Demands: The Politics of Skid Row Policing in Edinburgh, San Francisco and Vancouver* (University of Toronto Press, 2007), represents an intersection of several of her theoretical and research interests.

Stéphane Leman-Langlois holds the Canada Research Chair on Surveillance and the Social Construction of Risk and is Professor of Criminology at the Laval University School of Social Work.

Frédéric Lemieux is Professor and Programme Director of the Bachelor's in Police Science and Master's in Security and Safety Leadership at The George Washington University. He is also a member of the GW's Cyber Security Policy and Research Institute's Advisory Board. He has published several books and articles on intelligence-led policing as well as international police cooperation.

Michael McCahill is Lecturer in Criminology at the University of Hull, UK.

Johnny Nhan is Assistant Professor of Criminal Justice at Texas Christian University. His research focuses on different areas of cybercrime, including policing, piracy and legal issues. He is particularly interested in examining different forms of crime control in the internet environment.

April Pattavina PhD is Associate Professor in the Department of Criminal Justice and Criminology at the University of Massachusetts, Lowell. She has over 20 years experience conducting research in the corrections and policing fields. Currently, she is working on a project with the Center for Advancing Correctional Excellence at George Mason University to develop a data-driven computer simulation model to apply evidence-based practices to reentry planning initiatives. She has extensive expertise in working with correctional and policing data sources to promote better information collection efforts and quantitative research. Her publication record includes an edited book, *Information Technology and the Criminal Justice System*, and articles on topics such as information sharing across criminal justice agencies, new directions for electronic monitoring technology and offender classification systems.

Olivier Ribaux is Professor in Policing and Security, Crime/Criminal Intelligence Analysis and Forensic Intelligence, and Director of the Master of Law in Legal Issues, Crime and Security of New Technologies at the University of Lausanne, Switzerland. He has specialised in the fields of criminal intelligence analysis, financial crime analysis and forensic intelligence for the police and magistrates, and in the context of other training programmes, mainly in Switzerland and France. He also contributes to many working groups in the areas of security and intelligence. His latest book is *Les traces de souliers*, (PPUR, 2008), co-authored with Alexandre Girod and Christophe Champod.

James Sheptycki is Professor of Criminology at York University, Toronto, Canada. He has published widely on criminological topics including domestic violence, drugs and crime, organised crime, money laundering, serial killers, transnational policing and comparative criminology. His recent work, *Crafting Transnational Policing*, with Andrew Goldsmith, concerns transnational policing and the notion of a 'constabulary ethic' (Hart Publishing, 2007).

Contents

1 Introduction

Stéphane Leman-Langlois

In April 2011 the Federal Bureau of Investigation (FBI) and the US Marshals Service announced it had disabled a vast botnet called Coreflood, which spanned multiple countries. At its peak, Coreflood sent eight million 'pings' to its control servers *per day*. When the FBI was done with it three days later, the few remaining zombies called home fewer than 100,000 times per day. In computer security terms this was an unprecedented success.

Although dramatic, the success of Operation Adeona, as it was called, did not result in the typical parade of handcuffed miscreants being brought to justice. The investigation did not involve the collection of evidence, the interviews, the undercover agents, the crackdowns, the wires, the surveillance, the informers or the forensic analysis typical of the classic, media-friendly police operation. It pitted FBI hackers and lawyers against unknown operators in unknown places. Once command servers were identified the FBI obtained warrants allowing them to seize five machines and 15 domain names and to replace them with their own in order to send thousands of 'exit' commands to Coreflood zombies checking in.

Though still infected, those host computers then stopped attempting to connect to the network to deliver information and accept new commands. Because the botnet software remained installed on the machines, it restarted every time the computers were rebooted, which meant the FBI had to maintain its fake servers until every machine was disinfected.

But even the seizure and server swap was virtual: no hardware was bagged, tagged and dumped into a police van. The entities owning the hacked servers were simply ordered to quietly redirect all traffic headed to their domains to FBI-controlled domains.

Estonia, the United States' new partner in international cybersecurity, also seized an undisclosed number of Coreflood servers in the same way. After having suffered paralysing attacks on its government servers in 2007, Estonia has become a world power in cybersecurity and cyberwar. It also trains NATO's cyberwarriors at its Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

As for the zombies, their owners were sent a 'notice of infected computer' by the FBI, recommending that they install proper antivirus software, update their operating systems or use a new version of Microsoft's 'malicious software removal tool' in order to disinfect their machines and to prevent re-infection. They were also assured that the FBI did not collect information or use their computer in any way – which, of course, having become Coreflood's new botmasters, they could easily have done. Alternatively, users could give the FBI permission to remotely uninstall Coreflood from their computer once they accepted the risk that this operation could cause damage to their system (the botnet's malware package attaches itself to key parts of the Windows operating system). Interestingly, this risk was heightened by the fact that a large proportion of Coreflood's zombies were 'mission critical' components of institutional networks typical of large corporations, government organisations and hospitals, etc.

The US Department of Homeland Security (DHS) Immigration and Customs Enforcement agency has used roughly the same approach when dealing with copyright infringement. To date, close to 100 websites have been partly disabled when their domain names were seized and browsers were redirected towards a threatening law enforcement message instead of the file-sharing sites they were looking for. Though semi-experienced users can work around this strategy and still reach the sites, for the masses this amounts to a denial of service, officially executed under court warrant.

In typical low-crime municipalities, multiple administrative units have adopted videosurveillance as their main security strategy. Cameras are used to monitor and direct traffic, to watch political demonstrations near government buildings, to monitor drivers, ticket booth employees and commuters in buses, subways, trains and cars, on/off ramps, stations, stops and platforms. Such surveillance has many objectives, but the regulation of behaviour, or the control of conduct deemed inappropriate, deviant, irritant, antisocial or simply out of step with the desired image of the site being surveilled are always among them. While scientists, ethicists, lawyers, politicians, community groups and privacy watchdogs have had their eyes on police videosurveillance – that operated by, or to the benefit of classic, public police organisations – it is the 'non-police' systems that have multiplied in the last few years (Leman-Langlois, 2011). This negative definition exposes the embryonic nature of research on this topic. Though these systems are not private, they are not quite public either, since many private and semi-private (such as corporations owned and/or operated by governments) actors are involved. They are also quite definitely not *public*, in the sense that they are buried in infrastructure budgets and rarely spoken of in democratic institutions. Yet these systems are clearly *policing* technologies: they are used to impose order, preserve the peace, control behaviour, sort out deviants and other undesirables and organise private, mass private, public and hybrid spaces (real and virtual) according to their desired purposes.

With these few apparently disparate stories a few characteristics of technocrime – and technopolicing – emerge. First, though this seems paradoxical, the notion of 'crime' has to be understood in an extra-legal frame of reference. Though stealing money from credit card accounts is likely to be recognised as a crime by almost every code, running a botnet or swapping music files have variable, and constantly evolving, legal standings. Furthermore, technocrimes are often not as tangible as stealing a GPS through the broken window of a car. Tangible actions and effects are not required for technocrimes to exist. In short, what is interesting about the stories of 'crime' referred to above is not their criminal nature but their criminal representation.

Of course, many criminologists prefer to define their object with the help of criminal or penal codes, but this is not productive for our purposes. Nowadays few people think that 'possessing' marijuana should be a punishable offence – or in fact, according to public opinion surveys, that it is even *immoral*. Conversely, surveys also show that a majority of us think that those deemed responsible for the recent economic collapse – mostly executives from major financial institutions – should be thrown in jail. Through pension fund payment adjustments made necessary by the 'subprime' debacle, most working citizens stand to lose hundreds, if not thousands of dollars of yearly income. Yet anyone caught stealing one-tenth of this amount from my wallet or by skimming my debit card is guaranteed a trip through the criminal justice system. In short, for those interested in the sociology of crime, deviance and their responses, penal laws are not a scientific tool, a theory or a definition of crime: they are themselves objects of study, one stream of variables among many others.

What are the rationales at work in new laws, regulations, allocated enforcement budgets, privatisation or nationalisation of security, etc.? What were the social, political and legal processes behind the identification of new problems and new solutions? Who is responsible for that change? Who benefits? Who loses? Who gives tacit, silent consent? Who reacts in the public domain? As for the crimes they are meant to identify, define and punish, they in fact share few, if any, characteristics. Consequently, what unites the crimes in the 'technocrime' category has little to do with their nature but that they are presented, defined, studied and reacted to as reprehensible, harmful, immoral, risky, dangerous, etc.

What about the criminals? Warez hackers meet in bulletin boards and IRC chatrooms; they do not know each other and come from a variety of international jurisdictions where the copying, breaking, unlocking and redistribution of copyrighted material does not have the same legal status. They are aware that what they do is often (but not always) disliked by the copyright owners, but the extents to which they are breaking a law, the nature of that law or its legitimacy are not uniform, static elements in their own conceptualisation of their behaviour. Facebook revolutionaries in Egypt, on the contrary, knew exactly that what they were doing was illegal and harshly punishable – so did the Chinese bloggers criticising the Politburo or whistleblowers sending documents to Wikileaks in the expanding ultra-secret world of the global war on terrorism. What these actors have in common – besides their use of new technologies – is that governments, sometimes on their own, sometimes with prompting from powerful constituents, have criminalised them. In short, technocrime is behaviour presented and treated as worthy of the responses typically accorded to crime: seizures, arrests, warranted (and warrantless) surveillance, prison, fines, community work, etc., whether we agree with this criminalisation or not.

In fact, since we are defining crime in an extra-legal way, we can also consider the distinction between criminal or penal sanctions and civil remedies to be far less relevant than they might be to a jurist. If jurisdictions allow civil remedies for music file swapping to run into millions of dollars, they are effectively erasing the distinction, since the severity of the compensation is far more punitive than what criminal courts might impose to equivalent – or in fact far more serious – criminal offences.

Besides the coercive responses of governments and corporate stakeholders, the objective nature and universally undesirable quality of technocrimes are also consistently hammered into our culture by various powerful actors, especially by the mainstream, concentrated media and the usual parade of experts they call on to furnish their simplistic, biased portrayals of reality. Much scientific research is also conducted on unexamined notions of cybercrime, cyberwar, cyberfraud, cyberharassment, cyberpiracy, cyberloitering and the like. These authoritative sources continually reinforce the already dominant discourse about crime and technology. Symantec's latest high-gloss animated presentation of cybercrime (Symantec, 2011) is a prime example. The report, which starts with claims that some $388 billion are lost through cybercrime each year, only becomes interesting on its last slide: there the reader learns the definition of cybercrime, which includes mere irritants such as using someone's unsecured WiFi network or merely *receiving* phishing emails (whether or not some actual financial fraud later takes place). It also has two broad categories of 'other' cybercrimes, as defined by respondents. The $388 billion figure is immediately suspect, especially when the writers of the report emphasise its range by comparing it to the total *value* of the worldwide drug trade. Such an empty yet politically biased comparison may inspire a few to find out how the figure was calculated. In fact Symantec simply multiplied the *average* loss suffered by victims who incurred financial losses by the total number of victims – most of whom suffered no loss at all. But even that was deemed insufficient, adding up to a mere $114 billion. To this, the Symantec marketers chose to add a fictitious figure representing the 'guesstimated' costs of recovering from a cybercrime, once again averaged and re-multiplied by the total number of victims. As expected, the media reported, and repeated *ad infinitum*, the monstrous figure uncritically.

As for the rest of us, we cannot of course write our own laws nor, usually, enforce the existing ones. Yet, the way we have reacted to the new risk of technocrime is remarkably similar to our responses to traditional crime risks. We fear for our children's safety on Facebook, we demand or at least accept new laws purporting to enhance our safety and we adopt personal protective strategies, including new technologies of security and surveillance. Symantec's report mentioned above also has multiple links to new Symantec anti-cyber-risk consumer products.

Second, the study of technocrime does not rest upon the construction of a shopping list of objects that could be defined as 'technologically aided behaviours deemed reprehensible', which might include individuals stealing credit card details, corporations selling or leaking private information or governments creating massive – and massively leaky – citizen databases. The usefulness of the concept lays in its focus on the social representations of the nexus of new technologies and new forms of misbehaviour. Studying a technocrime means attempting to identify the factors that make it appear as such in policy texts, in public discourse and in the general culture, etc. Therefore it makes no sense, for instance, to ask whether technocrime is dangerous or not. In reality, technologically assisted crimes have a very uneven success rate, either from the point of view of their return on investment (the work involved versus the benefits reaped) or from that of their ability to escape arrest and condemnation. In short, technologically minded criminals are not mainly the unstoppable, invulnerable supervillains they are often portrayed to be – especially when file-sharing 'pirates' are thrown into the mix. In fact, in most cases they are rather inane. For instance, most hard drives seized during criminal investigations are not encrypted, a rather basic countermeasure. Hackers cannot help but brag about their latest attack. Bot herders get into fights with other bot herders and dedicate some of their resources to disabling one another. Yet technocrimes draw continuous attention because they lie at the centre of some of the most important cultural symbols of our time: technology and its dangers, information as a third type of economic output (with the classic goods and services), risk, safety and justice as control and punishment (Garland, 2001).

Third, technocrime cannot be dissociated from its purported responses, which for simplicity we will subsume under the heading of 'technopolicing'. Technopolicing rests upon the two separate beliefs that (1) new technologies can fight crime more efficiently, faster or with enhanced results; and (2) the world of crime has been transformed and requires entirely new forms of policing. The second argument is well illustrated by the FBI strategy outlined above, which shows the level of sophistication *some* crime-fighting has reached. These cybercops are now acting on a plane of reality so removed from our own that most of the details of the cases are never even suggested in the ordinary mainstream media. In a recent interview for a leading Canadian news outlet I was asked whether a good antivirus was the solution against LulzSec collective-type attacks. If computer security is such an opaque black box it is not surprising that technopolicing can be simplistically presented as the only solution to new crimes, whether technologically assisted or not.

As for the first argument, it can be heard in almost every aspect of modern life. From the first 'sabotages' and the Luddites movement, the adoption of new technologies were already perceived, by their adopters as well as their opponents, as a more efficient way to produce goods and services. In security, policing and elsewhere, technologies are still mobilised to replace decreasing traditional capabilities, such as cutbacks in the workforce. Sometimes they are introduced as ways to do more – faster and more safely. When it is used to control technology-aided behaviours, technopolicing may involve locking 'codes', as Lessig (2006) would put it: modifying technologies in order to make rule-breaking impossible, or, failing that, to make it impossible for rule-breakers to hide their identity. Circumvention is often possible but until it is, breaking rules