Theoretical Criminology

Vol. 13(2): 155–176; 1362–4806
DOI: 10.1177/1362480609102877

Identity theft vulnerability

Neoliberal governance through crime construction

TORIN MONAHAN
Vanderbilt University, USA

Abstract

Under the rubric of neoliberalism, the governance of populations occurs through new technologies and techniques of social control. Contemporary neoliberal discourses of crime control, in particular, normalize conditions of individual insecurity and responsibility while diverting attention away from root causes of social problems. The phenomenon of identity theft offers a generative case study for theorizing the ramifications of neoliberalism as a mode of crime control. The field is marked by the production of consumer-citizen subjects, who embrace self-discipline to mitigate crime threats; the transformation of mundane criminal acts into national security threats; the development of flexible accumulation skills, on the part of identity thieves, to compensate for the decline in state support for social reproduction; and the maintenance of insecure information infrastructures, which simultaneously increase the profitability of industry and vulnerability of the public.

Key Words

governance • identity theft • neoliberalism • security • social control • technology

Contemporary insecurity now extends well beyond individual bodies, national borders and material infrastructures. It includes, as well, the electronic data required for people to function in societies. Identity theft, which is perceived as being one of the greatest threats to people's critical data, now represents the largest category of fraud-related complaints in the United States. According to

the Federal Trade Commission (FTC), roughly 9 million US adults are victims of identity theft each year (Federal Trade Commission, 2008). These include cases of credit card theft, illegal wire transfers, Internet scams, phone and utilities fraud and theft of business data. Police agencies have responded to this new crime threat by launching coordinated public education programs to teach consumers to 'protect themselves' better. Some police recommendations include buying paper shredders for home use, shielding the keypad when using an ATM, not disclosing any personal information over the telephone or the Internet and setting up network 'firewalls' to safeguard electronic data. Indeed, the general law-enforcement response to this rapidly growing crime is to push responsibility onto individuals (or victims) to protect themselves. While self-protection is crucially important within the current climate of enhanced data vulnerability, this approach neglects the political and economic forces and systemic vulnerabilities that may be contributing to identity theft in the first place.

This article analyzes identity theft as a generative case study for theorizing the ramifications of neoliberalism as a mode of crime control. Neoliberalism has been explained as a set of policies, systems and ideologies that enforce and justify: state withdrawal from the provision of social welfare (Bourdieu, 1998; Katz, 2006); privatization of public services, spaces and resources (Graham and Marvin, 2001; Giroux, 2004; Monahan, 2005); increasingly disciplinary control and surveillance of 'risky' populations (Garland, 2001; Wacquant, 2001; Haggerty, 2004a; O'Malley, 2004; Simon, 2006); and the rescripting of citizen rights as consumer choices, such that citizens are obligated to consume in order to meet their basic needs or solve social problems (Rose, 1999; Comaroff and Comaroff, 2000; Duggan, 2003; W. Brown, 2006; Fisher, 2007). Threats of identity theft and related discourses of individual responsibility indicate a neoliberal relationship among individuals, public institutions and private industries. The mythology of identity theft actively structures new relations of social control, whereby individuals adopt responsibility for certain police and social service functions of the State while deeper conditions of vulnerability and insecurity remain unaddressed.

Industry profits underpin the logics of social control that emerge. Moral panics surrounding identity theft propel concerned individuals toward consumption alternatives to state regulation—seen with the purchase of technological fixes such as paper shredders or with the purchase of services such as credit-monitoring alerts. Self-discipline and consumption merge neatly as risk-management techniques that fuel security industries but do not alter the structural conditions of identity theft. All the while, economic vulnerabilities caused by post-industrialization and reduced social welfare create an ecology within which identity theft thrives. Finally, relaxed regulations for data protection increase industry stockpiling and trading of personal data, thus facilitating capital accumulation and increasing data vulnerability.

Identity theft can be understood, at least initially, as a set of practices for stealing someone's personal information. This is usually done for the sake of receiving profit from a third party, which is a practice known as 'financial identity theft', but other forms include 'criminal identity theft', where one provides

law enforcement agents with someone else's information, and 'identity cloning', where one adopts someone else's identity to begin a new life or become a virtual doppelgänger of the victim (Levi and Wall, 2004; Cole and Pontell, 2006). For the purposes of this article, the term *identity theft* will be used primarily to indicate financial identity theft, which is its most widely publicized form. Such identity theft practices can include dumpster diving for personal information; stealing laptop computers, wallets or physical files; hacking into computer databases; planting 'Trojan horse' or keystroke-tracking programs on personal computers (which will then 'phone home' to send information back over the Internet); 'skimming' credit card or ATM information with magnetic strip readers; 'phishing' for valuable information through email solicitations that appear to come from legitimate sources; 'pharming' information by redirecting Internet traffic to illegitimate sites that appear credible and then asking users to enter or 'update' credit card numbers, passwords or other identifiers; and so on.

Beyond these practices, identity theft must be understood as a moral panic and as a powerful myth that enrolls individuals, whether victims, criminals, state agents or industry employees, into new social relations and forms of life. Moral panics are widespread—but largely spurious—beliefs in threats to the social order posed by dangerous groups, such as identity-theft perpetrators. The media act as 'moral entrepreneurs' that foster fear in the public of its vulnerability to identity-theft attack by online hackers capturing credit-card information, drug users sifting through one's trash or scam-artists calling to request sensitive personal information. By calling identity theft a 'myth', I do not mean to deny its occurrence or experiences of it. Instead, I am calling attention to the fact of its social construction and its symbolic force to organize social life and normalize neoliberal power relations. Identity theft has been called the 'fastest growing crime in America' (Cole and Pontell, 2006: 125), and while reported cases are growing rapidly, the rate of those arrested for it is simultaneously decreasing (Allison et al., 2005). Fear of identity theft is inculcated by the media, police agencies, banking and credit industries and personal stories of friends, relatives or neighbors who have experienced the taxing ordeal of trying to restore their identity documents or their good credit. Simon Cole and Henry Pontell (2006: 128) relate:

> The true damage and real victimization lies in the sense of personal violation, psychological trauma, possible medical care, family issues, and other ill effects, which of course include the time and expense involved in trying to restore one's financial identity ... Identity theft is thus analogous to the theft of a key. The key itself is not particularly valuable, but the theft engenders insecurity disproportionate to the value of the key, which entails further costs (i.e., changing the locks).

Because fear of being a victim of identity theft far outstrips its actual occurrence, and because extreme actions are taken to mitigate it, it can properly be called a moral panic (Goode and Ben-Yehuda, 1994). This conclusion is supported by the fact that most credit agencies and retailers currently cover expenses associated with fraudulent purchases; thus, the concern felt by individuals is out of proportion to the risk they face.

Identity theft represents as well an ongoing shift in the way people and institutions perceive of individual 'selves'. Brought about in large part by the proliferation of networked information infrastructures, identities are increasingly constructed through the selective concatenation of disparate, external representations of personal information, rather than being perceived as a unified, coherent core residing within people. Mark Poster (2006: 114) explains:

> The practice of identity theft is conditional on the heterogeneity of identity, the inextricable mixing of consciousness with information machines, the dispersal of the self across the spaces of culture, its fragmentation into bits and bytes, the nonidentical identity or better identities that link machines with human bodies in new configurations or assemblages, the suturing or coupling of pieces of information in disjunctive time and scattered spaces.

Although this articulation elides emotional affect, power relations and the persistent materiality of such informatized zones, Poster does pinpoint a phase shift in cultural perceptions and valuations of identity as fragmented data, the likes of which spark new struggles for control. In other words, the cultural externalization and circulation of identity—as data—afford its theft.

Government institutions and the media have played a significant role in catalyzing this new orientation to the self. With the passage of the Identity Theft and Assumption Deterrence Act of 1998, the US government codified a disparate set of practices into a new crime category, which could then be transformed by the media into a moral panic. (In this respect, identity theft carves out a unique development trajectory because most moral panics move in the opposite direction: from media coverage to government action.) This law brought the crime to life in the public imaginary, so to speak, whereas prior to this the media and general public had largely ignored such crimes (Poster, 2006). Furthermore, many crimes that were previously classified as 'fraud' were absorbed into—or colonized by—the new crime category of 'identity theft', especially for theft of individual data with information technologies (Cole and Pontell, 2006). The label of 'fastest growing crime', therefore, is itself a misnomer that has become a social fact, generating further panic and demanding response (Cole and Pontell, 2006).

Drawing upon the case of identity theft, this article investigates the ramifications of neoliberalism as a mode of crime control. To do so, identity theft is analyzed in relation to discourses of self-protection, economic contexts and technological systems. Discourses of self-protection construct a certain kind of ideal citizen who can respond to threats of identity theft through consumption of products or services, information or media-generated fear. This modality of self-protection quickly folds into one of social control, whereby people embrace self-policing and normalize the absence of the State in providing for social needs. The political and economic context for identity theft is one of post-industrialization, particularly within regions that have lost their stable industries and have gained a host of social instabilities, such as the manufacture and use of methamphetamines. The second type of geography where identity theft thrives is in regions of heightened economic polarization

and sociospatial segregation, such as large cities in the southwestern USA. Finally, the technological systems that facilitate identity theft are those of large-scale databases that are poorly regulated and vulnerable to attack. Most of these are operated by credit and telecommunications industries that hold profit motives over those for social good, such as privacy, but government databases are similarly vulnerable to compromise.

To the existing literature on discourses of neoliberalism and crime control, the case study of identity theft highlights trends toward the transformation of the self into a possession and mundane criminal acts into national security threats. In addition, flexible multitasking, which has long been recognized as a valuable—if contingent—skill for grappling with the instabilities of post-industrial markets, is now mobilized as a tool for capital accumulation by 'criminals' as well as others, demonstrating some of the contradictions and shifting value systems of global production regimes. Finally, identity theft calls attention to the agential role of technological systems—especially new information and networked infrastructures—in establishing the social field for relationships of vulnerability, empowerment and control.

Self-protection or self-policing?

The central message for people concerned about identity theft is to protect themselves. But something interesting happens through the mobilization of arguments for individualized solutions to identity-theft risks: citizens are reframed as consumers who can best combat crime through consumption. Take, for example, a story in 2005 about the theft of Lexis-Nexis consumer data by what the reporter calls an 'online gang' known as Defonic Crew. After describing the theft, the story concludes with the sage advice: 'Let this serve as a potent reminder that we should all take precautions to safeguard our PCs. Who knows? You might have already inadvertently aided and abetted a criminal by not removing a Trojan horse' (Vamosi, 2005). In this case, individuals are metaphorically accused of aiding and abetting crimes by not purchasing anti-virus software or taking other precautions; by this logic, the victim of identity theft is not only blamed for being an easy target but is guilty of participating in the crime.

In the discourse of self-protection, the 'choice' not to consume is not only irresponsible—it is criminal. When citizens are recast as consumers in this way, the relationship between citizens and the State changes. Instead of the State being responsible for ensuring the safety of people, citizen-consumers are charged with regulating their localized territories through consumption. Additionally, government websites stress that the credit industry is the primary victim of identity theft, so if individuals are irresponsible enough not to protect themselves, by implication they are damaging the national economy upon which everyone depends. The City of Phoenix illustrates this logic by subordinating the violation of individuals to that of industry: 'Identity Theft is a "dual crime"—besides the financial institution that extended the credit being a victim,

you are also a victim' (Phoenix Police Department, 2006). This section argues that such a reframing of rights and responsibilities, which is by no means unique to identity theft, advances a uniquely neoliberal form of social control.

Although consumption may be presented as a requirement for individuals who choose to take data security seriously, it is analytically important to separate out three dominant modes of consumption in this context. The first, already mentioned, is the purchase of products and services: paper shredders, Internet firewalls, anti-virus programs, home safes, home alarm systems, credit-monitoring services and so on. For example, one such fraud protection service called 'Identity Guard' is offered by the website www.stopijacking.com. The site lures customers through well-placed, fear-inducing banner ads, which are disseminated widely across the Internet. They brand identity theft as 'iJacking', which they define as 'an emotionally devastating crime that drains your accounts, hurts your reputation and leaves you financially paralyzed when thieves assume your identity or use your social security number [to] commit fraud crimes' (stopijacking.com, 2006).

The second mode of consumption is that of consumer-protection information in the form of police workshops, university information sessions, government pamphlets and numerous government, industry and consumer advocacy websites. The stress of these information resources is always on individual responsibility. The FTC, for instance, has a 'Deter, Detect and Defend' campaign that places all the burden upon the public to protect themselves and act quickly to report identity theft as soon as they detect it (Federal Trade Commission, 2006a). The FTC (2006a) offers detailed instructions about the steps individuals should take immediately upon detecting that their identities have been compromised:

> 1. Place a fraud alert on your credit reports, and review your credit reports ... 2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently ... 3. File a report with your local police or the police in the community where the identity theft took place ... 4. File a complaint with the Federal Trade Commission.

In addition, individuals are explicitly told that they must 'prove' that they are identity theft victims.

Similarly, on local levels, the resources offered by city governments and police agencies clearly communicate where responsibility lies, such as Phoenix's campaign titled 'Identity Theft: Learn to Protect Yourself'. In this campaign, citizens are provided with an overwhelming list of precautions to take, ranging from implementing home-security systems, to 'cross-cut' shredding all potentially sensitive documents, to driving out of their way to place outgoing mail in secure postal boxes, to reviewing credit reports annually (Phoenix Police Department, 2006). The inclusion of credit reports is especially instructive for this analysis. Because US law mandates that annual credit reports be provided 'free of charge' from the main credit agencies, this effectively structures in additional responsibility for individuals to possess and

mobilize the information literacy and time required to access and scrutinize credit reports and act on any suspicious information they find. The law is couched in terms of empowerment and rights, but it is a form of empowerment whereby the State delegates data-security responsibilities to citizens. These examples illustrate that in addition to the demand for citizens to purchase goods and services and alter their practices, they are also charged with seeking out and consuming the information needed to protect themselves wisely. In this way, these two modes of consumption both overlap and reinforce one another.

The third mode of consumption is the consumption of fear. Although less tangible than the purchasing of products or services or the active collection of safety information, the consumption of fear describes a critical component in the social construction of identity theft as a moral panic. Fear is not simply transmitted from the media to the public. Instead, it involves the collaborative cultivation of subjects who are receptive to moral panics as compelling explanations for everyday insecurities. A consumerist orientation to messages of fear facilitates this process. The obvious source for these goods is the mainstream media, with their many horror stories about personal trauma inflicted by identity theft. These stories almost always lead with sensational trials and tribulations experienced by innocent victims who are desperately trying to restore their credit. The convenient linking of identity theft to illegal drugs—or more recently to illegal immigrants—helps to fuel the fears that people might have about vulnerability because the perpetrators are constructed as transgressing social norms and spatial boundaries in pursuit of short-term economic gain at the expense of law-abiding individuals. For instance, an MSNBC story begins:

> Police in the small Olympic Peninsula town of Port Orchard, Wash., sensed something was wrong when they approached the pickup truck sitting in the town's RV park. To begin with, its occupants were naked. Inside the truck, an even more bizarre scene: Piles and piles of mail. The truck's occupants quickly confessed: The mail was stolen, lifted from mailboxes in the hopes of trading it for hits of methamphetamine at a nearby mobile home.
>
> (Sullivan, 2004)

The 'facts' are presented in such a way as to highlight the supposed irrationality and otherness, if not dangerousness, of identity theft criminals: the perpetrators are sitting naked and poring over stacks of other people's mail in search of information that could be traded for hits of methamphetamine.

Identity theft has now been yoked to illegal immigration and national security concerns as well. This has occurred in large part courtesy of US Immigration and Customs Enforcement (ICE) Agency raids on meat-processing plants in Colorado in 2006 and Iowa in 2008, and subsequent news briefings by the Department of Homeland Security (DHS) and reports by the mainstream media. Because undocumented workers in the meat-processing plants borrowed social security numbers in order to receive paychecks, and pay taxes, DHS characterized them as identity theft criminals who were

compromising the security of the country and well-being of its citizens (Cooper, 2007; Saulny, 2008). DHS secretary Michael Chertoff explained:

> This is not only a case about illegal immigration, which is bad enough ... It's a case about identity theft and violation of the privacy rights and the economic rights of innocent Americans ... the issue of fraudulent identification is one which, as the 9/11 Commission recognized, poses a homeland security challenge [because terrorists could use false documents to board airplanes].
>
> (Department of Homeland Security, 2006)[1]

The tone for new cultures of control is set in conjunction with the media (Cavender, 2004), that in this case readily picked up and circulated the official framing of personal and national security risks associated with supposed 'identity theft' by undocumented workers (e.g. Leinwand, 2006). What is particularly interesting here are the levels of conflation at work in this state and media production: first, the borrowing of social security numbers is framed as identity theft, somehow in the same category as running up the debt of others; next, this form of identity theft is folded into national security concerns, such that it would be ethically irresponsible for state agents not to employ the most punitive of measures. The combined result is a message of individual risk (economic insecurity) and absolute threat (national insecurity). Thus, one of the emerging dimensions of neoliberal crime control is harsh, disciplinary state action for overtly political issues, such as 'illegal immigration', along with heightened individual responsibility for most other cases. It is the convergence of neoconservative with neoliberal rationalities, respectively, with the former asserting a moral-political force and the latter a market-political one (W. Brown, 2006).

Apart from high-profile round-ups of undocumented workers, which are only tenuously about identity theft, the increasing abdication of institutional responsibility for addressing this crime signals a dramatic shift in modes of governance and policing. The preferred response is the delegation of responsibility to citizen-consumers in the battle against identity theft. One might still say that there is a reactive form of law enforcement at work because police agencies and lawmakers are apparently responding to the demands of citizens to crack down on identity theft with harsher laws. It is my contention that the reactive law-enforcement mode is present but largely symbolic, especially in the USA. For instance, a common complaint among law-enforcement agencies is that they lack the personnel and resources to contend with the flood of complaints, let alone to intervene in any meaningful way. A US government report supports this conclusion: 'police departments are more inclined to use their limited resources for investigating violent crimes and drug offenses rather than handling complicated identity theft cases that, even if successfully prosecuted, often lead to relatively light sentences' (US General Accounting Office, 2002).

The role of the State is becoming one of minimized social programs coupled with disciplinary demands upon citizens for meeting the needs of society, whether in the form of consumption to drive economic prosperity

(Landau, 2004), philanthropy or voluntarism to provide for the needs of the community (Monahan, 2006b), or policing to ensure personal safety and security (Garland, 2001; Katz, 2006). Of course, at the same time that the State is crafting a new relationship with the public in terms of social services, it is advancing mechanisms of control through military, security and prison apparatuses. This is a larger pattern that is contributed to (and in part rendered visible) by dominant approaches to identity theft, but it has been well documented and theorized in other domains as well. David Garland (2001: 18), for instance, writes:

> The last few decades have seen important changes in the objectives, priorities and working ideologies of the major criminal justice organizations. The police now hold themselves out less as a crime-fighting force than as a responsive public service, aiming to reduce fear, disorder and incivility ...

Policing, Garland asserts, has become geared toward risk-management and the redistribution of crime control functions to communities and private security forces (see also Haggerty, 2004a; Singh, 2005; Ericson, 2007). The official law enforcement response to identity theft supports this observation: the police will provide information to help the public 'contain' the problem, but it is up to consumer-citizens to engage it more or less on their own.

State outsourcing of police and security responsibilities to the public facilitates, in turn, the privatization of public spaces and services. The rise of fortified enclaves such as gated communities, shopping malls and business centers creates barriers between social classes and marginalizes the poor by removing them (and public responsibility for poverty) from sight (Davis, 1990; Blakely and Snyder, 1997; Caldeira, 2000; Monahan, 2006a). The turn toward home-based security systems such as alarms, video surveillance and weapons (and now Internet firewalls too) offers a sense of security for those who can afford them while normalizing other forms of public human insecurity—e.g. poverty, lack of health care, vulnerability to natural disasters—as the responsibility of individuals, not the State (Katz, 2006). Finally, privatized security forces or services, such as security personnel for patrolling neighborhoods or credit-monitoring services for minimizing identity theft, have profit-imperatives as their primary motivation, not the social good. And, at least with the case of private security personnel, due process and other legal safeguards that regulate police and military conduct do not hold true for contractors (Singer, 2003; Singh, 2005; Davis, 2006). These are important points to consider in relation to identity theft, because if social polarization and economic insecurity contribute to identity theft crime and methamphetamine use, as the next section contends, then the dominant responses of outsourcing and privatizing may only exacerbate the situation.

Ultimately, individual self-protection against identity theft functions through self-policing. The State may monitor the crime and provide information, but citizens are required to take matters into their own hands. If they do not, then the media tell them that they are aiding and abetting the crimes, and the State tells them that they are hurting credit industries and the

economy. The privileged mode of individual self-protection is consumption, or the self-transformation of citizens into citizen-consumers (Rose, 1999). The modes of consumption are purchasing products and services, participating in workshops and other information-gathering activities, and actively exposing oneself to and internalizing fear. The modality of self-protection is disciplinary. It requires individuals to regulate their practices, their homes, their loved ones and their data. It conscripts them as citizen-soldiers in the wars on crime, drugs, terror and weak national economies. Such citizen-consumer-soldiers really are armies of one. If they fail in any way, they will be blamed and—at least discursively—held guilty for their shortcomings. In the final analysis, however, self-protection against identity theft or any other social problem is part of a much larger transformation in state functions and purposes, away from the provision of social goods and services and toward industry profits. All the while, this form of governance advances cultures of control that ignore root causes of crime, poverty and insecurity.

Post-industrial context

Tweakers, meth heads, dope fiends. These are some of the descriptors applied to identity theft criminals by law enforcement and the media. Methamphetamine addiction and identity theft go hand in hand, so it seems, because of the specific nature of the 'high' achieved by meth use. Meth users stay awake for days on end; they are risk-adverse, low-profile and often technology savvy; they are obsessive compulsive and so incredibly detail-oriented that they can focus intensely for hours on tedious tasks (Sullivan, 2004; Cole and Pontell, 2006). This makes them perfectly suited—so authorities contend—for the daunting challenges of sorting through vast quantities of people's mail for valuable information; cracking into protected computer networks; sending out 'trojan horses' to people's computers and sifting through data sent back; painstakingly removing ink from used checks with special acid washes; and creating near-perfect counterfeits of checks, drivers licenses and other documents.

The underlying message of most news stories on methamphetamine addiction and identity theft is one of demonizing the users/criminals, bemoaning the constraints placed on law enforcement and stressing the vulnerability of innocent people who must take precautions to guard their information. Rarely, if ever, is there any discussion of the politics behind recent interpretations of meth use or the specific economic conditions within which meth use and identity theft flourish. The overlaps between meth use and identity theft reveal a contemporary economic dimension of the USA's ongoing 'war on drugs'. In the 1980s and early 1990s meth—or 'crank'—was explicitly feminized and racialized white (vis-a-vis crack cocaine). Nancy Campbell (2000: 3) writes of the main constructions of drug use during this time period:

> Crank [meth] enables white women to meet their obligations as mothers and workers—the drug helps them juggle service jobs and child-care responsibilities. Crack using women [by contrast] are not afflicted with the compulsion

> to clean, work, or care for their children—they are represented as sexual compulsives, bad mothers, and willing prostitutes who lack even the capacity for remorse that might redeem them.

Methamphetamine has now been recast as a dangerous, homemade narcotic manufactured and used predominately by people in low-income, white, rural communities. It is now one of the primary targets in 'the war on drugs'. The detailed multitasking capabilities engendered by the drug still compensate for the decline in state support for social reproduction, as Nancy Campbell (2000) wrote about, but the activities of drug-users are now directed externally toward illegal capital accumulation, rather than internally toward childcare and household management. As a result, the discursive linking of meth use and identity theft cultivates a moral panic wherein potential concern for meth users is supplanted by fear of them.

While quickly spreading throughout the USA, meth labs appear to crop up first in economically depressed, working-class regions where community-sustaining industries have been downsized or eliminated, such as the towns of the Midwest that historically relied on farming, truck driving, factory work and coal mining for reliable jobs (Bonné, 2001b) or those in the Northwest that have depended upon logging and farming (Bonné, 2001a). The second area where meth labs and identity theft thrive are cities with extreme social and economic polarization. Phoenix is an ideal example of this. It is the fifth largest city in the USA, home of many poor immigrants and affluent retirees and geographically defined by numerous gated communities separating people of different classes and backgrounds (Monahan, 2006a). Notably, Phoenix also has the highest number of reported identity theft complaints per capita in the country (Federal Trade Commission, 2006b).

There are links worth exploring, therefore, between the social problem of identity theft (and identity thieves) and changes in the political economy. The contours of post-industrialization and globalization are an obvious starting point. More than simply indicating the loss of factory jobs or the outsourcing of them to other countries, post-industrialization signals a shift in the mode and logic of capital accumulation (Kupchik and Monahan, 2006). The hierarchical and stable industrial models of the past have been transformed, since the early 1970s, into decentralized, mutable organizations operating through rapid exchange of goods and services (Sassen, 1991; Castells, 1996). Capital accumulation is now facilitated by telecommunications infrastructures, just-in-time production models and flexible employees with few benefits and little job security (Harvey, 1990; Hardt and Negri, 2000). Accompanying these industrial changes are alterations in public institutions and social policy, such that public programs are minimized, privatized or otherwise harmonized with the needs of industry (Duggan, 2003; Giroux, 2004; Monahan, 2005). Finally, large private industries (e.g. energy, telecommunications) have been deregulated in such a way that services are increasingly 'unbundled' for those who cannot afford to pay additional fees (Graham and Marvin, 2001), which is a condition that is also apparent with consumerist approaches to security provision. For the discussion of identity

theft, therefore, several key results of these transformations include (1) increased economic instability and social polarization, and (2) the emergence of database infrastructures that serve as resources for capital accumulation both for industry and for identity theft criminals.

In addition to these structural changes seen on the level of the political economy, a certain cultural logic accompanies post-industrialization, further entrenching it in social practice (Jameson, 1984). It should not be seen as a coincidence that today's descriptions of ideal workers and methamphetamine users are remarkably similar. They both thrive on instability, work long hours on tedious projects, multitask, adjust flexibly to changing conditions and are technologically proficient. As Emily Martin (2000, 2007) has written about manic depression and attention deficit hyperactivity disorder (ADHD), not only does post-industrial work reward certain pscyho-social pathologies, it actively cultivates them. The most successful people in today's marketplace are 'always adapting by scanning the environment for signs of change, flying from one thing to another, while pushing the limits of everything, and doing it all with an intense level of energy focused totally on the future' (Martin, 2000: 515). The ideal flexible worker does not expect job security or state assistance; instead, he or she gets 'high' on the danger associated with having everything to lose. But, as a result of the prevalence of this cultural logic of individual adaptation and responsibility, and non-accountability of government or industry, many are left in dire straights. Those, such as identity theft perpetrators, who deftly exploit the system by embodying the values of post-industrialization but who do not increase the profit of companies are demonized and criminalized.

One could view identity thieves instead as entrepreneurs with highly specialized skills. They are individuals who have carved out niche markets for sustaining themselves by appropriating the dominant rationalities of flexible accumulation and the technologies of network interconnection. Identity theft is not entirely unlike the occult economies created by others throughout the world in response to economic vulnerabilities. Jean and John Comaroff (2000), for instance, describe practices of gambling, pyramid schemes, witchcraft, zombie conjuring, organ theft and trade and so on as innovative cultural responses to instabilities of advanced capitalism and neoliberal policies to privatize all collective goods and services. Seen from this perspective, the demarcation between innovative identity thieves and law-abiding workers is not so clear. Many people are subjected to the post-industrial risks of social instability, human insecurity and downward economic mobility. Only by attending to the political and economic context of this crime can it be seen as part of larger social problems that are easily obscured by simply targeting those labeled criminals.

Data vulnerability

The very technological systems that facilitate communication, commerce and trade also open people up to intrusive forms of electronic surveillance, whether

perpetrated by identity thieves or others. This is a point often overlooked in discussions of electronic monitoring or crime. People have been told that adopting the latest technologies is necessary to stay in touch with friends and relatives, to conduct business more efficiently, to maintain competitive advantage over other countries or to ensure military superiority over modern-day enemies. Most people believe that technological systems are synonymous with progress (Winner, 1977, 1986). But in accepting this formula, societies have neglected to question the ways in which information systems increase vulnerability to surveillance abuses (Haggerty, 2004b), whether by identity thieves, government agencies or private industries. When risks are seen through an individualistic lens, it is difficult to perceive and address the systemic vulnerabilities enabled by information infrastructures.

Nonetheless, vulnerable information databases and their related industries are key to undermining data security and increasing avenues for identity theft (Whitson, 2006; Whitson and Haggerty, 2007). For instance, while hundreds of thousands of individual complaints may be filed with the FTC each year (Federal Trade Commission, 2006b), millions of data records have been compromised in mass identity thefts. In one of several recent high-profile cases, for example, 40 million credit cards were compromised when hackers penetrated the database of CardSystems Solutions, Inc. in Tucson, Arizona in 2004 (Krim and Barbaro, 2005). In the same year, the consumer data aggregator company ChoicePoint admitted to losing over 163,000 records to criminals, leading to over 800 documented cases of identity theft (Kawamoto, 2006). In 2006, personal information from 26.5 million military veterans was stolen from the home of an analyst for the US Department of Veterans Affairs who was not authorized to take the records home in the first place (Reuters, 2006). Similar cases of massive theft or loss of sensitive data happen frequently because organizations fail to implement serious data-protection protocols. For instance, in 2007 a laptop computer containing personal information, including social security numbers for 800,000 people, was stolen from The Gap clothing company, which admits that it did not have the data encrypted on the computer (Konrad, 2007). Also in 2007, it came to light that international retail company TJX's central databases were hacked into without their awareness, giving hackers access to 45 million credit and debit card numbers (Konrad, 2007). The British government has also had a slew of data-loss incidents recently from the private security companies to which they outsource responsibilities, including losing 'next of kin details, passport and National Insurance numbers, drivers' license and bank details, and National Health Service' numbers in 2008 for up to 1.7 million people expressing interest in joining the armed forces (Murakami Wood, 2008).

Whether implicating private industries or the Government, these cases underscore not only the lax security for sensitive data systems but also the lax enforcement of policies for data protection. These are not isolated cases that any individual action, such as using an anti-virus program, could have prevented. Indeed, while police authorities and the media play upon fears of methamphetamine users and dumpster divers,[2] the truth is that most people

do not know how their information was stolen (Leland and Zeller, 2006). It could very well have been a result of third-parties who had legitimate access to the data. These examples point to compromised information systems and policies that extend far beyond the control exercised by any individual.

Such cases of large-scale data theft are enabled by vulnerable information systems and their companies or government agencies. The fact that industries poorly manage their networks, fail to ensure proper encryption, share data liberally and maintain records far longer than is necessary compounds the problem (O'Harrow, 2005). Given these problems, the approach to identity theft that prioritizes individual protection may unwittingly reinforce the conditions that support these crimes. Because there has not been informed public debate about the kinds of technologies that are necessary to adopt, or about the important safeguards that should be implemented for the preservation of social goods (such as crime prevention or privacy), vulnerable information systems proliferate. In effect, individual consumers, employees or others are blamed for their own victimization, but the systems or the industries that make them such easy targets are seldom reevaluated. These systems are the massive databases of consumer information that are stockpiled by credit agencies, telecommunications companies and others for targeted advertising and lucrative sharing arrangements among companies. Once the systems are in place, they also enable multiple uses far beyond the original intent for them, which can be seen clearly with major telecommunications companies willingly (and illegally) turning over their databases to US government agencies to sift through and spy on US citizens, ostensibly for counterterrorism purposes (Electronic Frontier Foundation, 2006). When confronted with the problem of easily compromised databases and data-security practices, the major industries respond by saying that the systems are too profitable to impose serious restrictions upon them and that customers desire the instant credit that such systems afford (Leland and Zeller, 2006). It is a market-based decision that has little to do with concerns about crime or privacy rights.

Presently the FTC can fine companies that have not taken 'reasonable' precautions to ensure confidentiality of consumer data. For instance, a $15 million fine was imposed upon ChoicePoint in January 2006 for its loss of records (Kawamoto, 2006). Notwithstanding the potential for fines to galvanize better data protection by companies, this approach to regulation presupposes that violations will come to the attention of the FTC, when it is much more likely that most cases are not identified or are only partially revealed. Fines do not address the problem of data stockpiling and exchange among companies. They do not call for the redesign of information architectures to ensure anonymity and confidentiality at every step of the way with the generation and circulation of data. Most importantly, they ignore the pressing need in the USA for serious data protection laws—the likes of which do exist in other countries (e.g. the UK's Data Protection Act of 2000). The USA, for example, does not presuppose that everyone opts-out of data sharing as a default. Currently it is almost always the opposite: everyone is opted 'in' for data sharing, forcing individuals to contact credit companies and others to request that their information is not shared.

Similarly, the USA does not have clear guidelines for who has access to personal data (especially for data not pertaining to credit or medical records), how it can be shared, and when it will be destroyed (Blanchette and Johnson, 2002). It is likely that until data vulnerability is addressed as a systemic problem, rather than as an individual one, identity theft will continue to increase and exceed society's capacity for dealing with it.

Because there are few regulations for data protection, industries may profit from consumer information and governments may benefit from easier surveillance of populations. One way of interpreting such practices of fluid information exchange is that they shift power away from individuals while affording greater control of individuals for purposes of capital accumulation or counterterrorism investigations. This illustrates another property of neoliberal governance. While individuals and their data are made vulnerable by ubiquitous information infrastructures and exchange practices, the primary trade-off articulated as justification for exposure to such risk is the availability of 'easy credit' for consumers. Not only is consumption depicted as the 'good' that makes exposure to identity theft worthwhile (Leland and Zeller, 2006), it is also the means by which individuals can protect themselves. Meanwhile the State is almost completely absent, unless it is drawing upon the vast information systems for 'national security' purposes, or, more likely, outsourcing that task to contractors.

Conclusion

Identity theft is an everyday form of insecurity that reveals dominant shifts in modern forms of governance and highlights new dimensions of neoliberalism as a mode of crime control. As a set of social practices and as a socially constructed crime category, identity theft illustrates transformations in social control toward individual responsibility for crime deterrence through self-policing and toward the abdication of the State for providing for social needs, whether in the forms of economic stability, social services or necessary regulations upon information industries. In many ways, identity theft manifests the instabilities and contradictions of modernity. Crosscutting and comprising the identity theft assemblage are conditions of economic inequality, demands for flexible labor forces, creative appropriations of technology, demonization of drug users and 'Internet gangs', fear of crime, dependence on information systems and databases, vast industry profits, minimal regulation and individual consumption as a privileged response to problems of insecurity. Identity theft is catalyzed by and actively reproduces these conditions. The overall effect is one of intensified social control, which takes place with the onset of governmentalities of hyper-individualized responsibility, privatized 'solutions' to identity theft and other crimes and crime containment, risk management and outsourcing as the primary responses of the State.

First, the article identified discourses of self-protection as contributing to the production of an ideal type of modern citizen. This citizen is foremost

a consumer and a disciplined protector of self, home, family and data. Both the media and law enforcement agencies call upon citizen-consumers to fortify their lives and police their practices to minimize exposure to risk. It is rather facile, but nonetheless true, to say that consumption as a privileged response to social problems feeds security industries. What is less obvious to see are the ways that governmentalities of individual responsibility penetrate into social fabrics and cultural dispositions to normalize non-reliance on the State. Panoptic levels of discipline are internalized by citizens in the neoliberal state and are demonstrated by the discursive construction of and sanctioned responses to identity theft. Beyond that, however, the State's mode of engagement through risk management and crime containment presents a discernable articulation of biopower, which Michel Foucault understood to be different from yet complementary to panoptic self-discipline and technologies of the body (Foucault, 1977, 2003; Dupont and Pearce, 2001). Foucault (2003: 245) writes:

> Disciplines, for their part, dealt with individuals and their bodies in practical terms ... Biopolitics deals with the population, with the population as political problem, as a problem that is at once scientific and political, as a biological problem and as power's problem.

The site for biopower, therefore, is not the individual body but the population as a whole, which is regulated and managed through a series of measurement techniques—of reproduction, morbidity, epidemics and so on. Crime can be added to the list of sites for biopolitical regulation: as it is measured, contained and controlled, so too is the population as a whole managed in very particular, historically specific ways. This article has sought to show how the discourses surrounding identity theft signal emergent disciplinary and biopolitical relations among individuals, public institutions and private industries. These relations are those of increased vulnerability, responsibility and social control of populations.

Second, I analyzed identity theft as situated in a specific political and economic context of post-industrialization. The correspondence between economically unstable geographical regions and identity theft has been largely ignored by the media and the State. The reasons are not hard to see. To call identity theft a social problem, rooted in economic instability and social polarization, is to imply the need for systemic responses that have historically been the charge of the State. By interpreting identity theft instead as a drug-based (or illegal immigrant-based) crime that is facilitated by the carelessness of individuals with their personal data, no public solutions are required beyond informing individuals about risks and perhaps conducting well-strategized and well-publicized police raids on methamphetamine labs, crime rings or places that employ undocumented workers. The field for possible responses is therefore restricted to those that support neoliberal governance of minimized social services and increased punitive measures—or, as Loïc Wacquant (2001: 97) provocatively characterizes it: the invisible hand of free-market solutions coupled with the iron fist of discipline and control.

Third, identity theft was addressed as a product of vulnerable databases and minimally regulated information industries. Technological systems possess certain valences for uses, and electronic databases are no exception: they lend themselves to information storing, sorting and sharing such that vulnerabilities are part of the system, not merely unintended outcomes. Technological systems are thoroughly social entities (Bijker and Law, 2002; S. Brown, 2006) whose design influences the social roles that they play and their capacity to structure social relations (Latour, 1992; Hess, 2007). Recognizing these 'politics' of information systems means understanding that they already embody certain codes or regulations for use and that these are non-neutral in their effects (Winner, 1986; Lessig, 1999). Judging from the numerous instances of compromised databases, whether due to malicious intent, employee negligence or government demands, these systems are designed to maximize the flow of information with minimal friction. Friction could purposefully be increased through many sociotechnical forms: encrypted data, closed networks, opt-in rather than opt-out policies, data retention policies and data protection laws (Monahan, 2006c). As these systems are currently structured, especially in the USA, they harmonize with the profit imperatives of industry and the intelligence needs of government but at the expense of public data security and privacy.

Analysis of identify theft contributes to criminology's theoretical understanding of neoliberal forms of crime control, especially in relation to risk management and individual responsibilization in the face of insecurities. Although identity theft provides an excellent example of these trends, it also highlights new information dependencies and vulnerabilities made possible by vast integrated databases that are often owned by private companies with loose data protection policies and practices. Identity theft depends upon the presumption of digitized selves, or 'data doubles', that circulate within information networks as intimate, disembodied possessions that can be stolen or compromised (Schwartz, 1996; Whitson and Haggerty, 2008). The self is commodified as something external to people. Both law enforcement agencies and the media fan the embers of identity theft threats into raging conflagrations of moral panic such that individual vulnerabilities are reframed in absolute terms as national security threats. Responsibilization extends beyond the individual to encompass the entire body politic. The creative appropriations and innovations of identity thieves harmonize well with the flexible production ideologies of the post-industrial labor market. The fact that such tactics of flexible accumulation are criminalized while others are celebrated demonstrates some of the contradictions and contingencies in new modalities of capitalism and crime construction. Flexible tactics for the sake of industry profit are embraced, while those that threaten neoliberal orthodoxy are demonized.[3] Lastly, technological systems play a crucial role in the construction and governance of vulnerability, insecurity and responsibility. As long as technologies are seen as neutral tools, their systemic effects will be masked, thereby allowing individualizing frames to be forced over social and institutional problems.

Notes

I would like to thank Aaron Kupchik, *Theoretical Criminology* Editor Lynn Chancer and the anonymous reviewers for helpful comments on this article.

1. This cultivation of fear about potential terrorist attacks by illegal residents conveniently ignores the fact that all of the 9/11 terrorists entered the United States legally with the requisite visas (Monahan, 2006c).
2. According to Jeff Ferrell's (2006) ethnographic study of dumpster divers, they are seldom interested in the credit information of others anyway, and they often throw personal documents back in the trash when they stumble across them.
3. One can witness the same trend with the demonization of anti-globalization protestors who utilize flexible tactics for organizing and demonstrating (Fernandez, 2008; Juris, 2008).

References

Allison, Stuart F.H., Amie M. Schuck and Kim Michelle Lersch (2005) 'Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics', *Journal of Criminal Justice* 33(1): 19–29.

Bijker, Wiebe E. and John Law (1992) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge: MIT Press.

Blakely, Edward James and Mary Gail Snyder (1997) *Fortress America: Gated Communities in the United States*. Washington, DC: Brookings Institution Press.

Blanchette, Jean-François and Deborah G. Johnson (2002) 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness', *The Information Society* 18(1): 33–45.

Bonné, Jon (2001a) 'Lab-Busting in the Northwest: Stalking an Elusive Foe', *MSNBC*, February. Available at http://www.msnbc.msn.com/id/3071775

Bonné, Jon (2001b) 'Scourge of the Heartland: Meth Takes Root in Surprising Places', *MSNBC*, February. Available at http://www.msnbc.msn.com/id/3071773

Bourdieu, Pierre (1998) 'The Essence of Neoliberalism', *Le Monde Diplomatique*, December. Available at http://mondediplo.com/1998/12/08bourdieu

Brown, Sheila (2006) 'The Criminology of Hybrids: Rethinking Crime and Law in Technosocial Networks', *Theoretical Criminology* 10(2): 223–44.

Brown, Wendy (2006) 'American Nightmare: Neoliberalism, Neoconservatism, and De-Democratization', *Political Theory* 34(6): 690–714.

Caldeira, Teresa P.R. (2000) *City of Walls: Crime, Segregation, and Citizenship in São Paulo*. Berkeley & Los Angeles, CA: University of California Press.

Campbell, Nancy D. (2000) *Using Women: Gender, Drug Policy, and Social Justice*. New York: Routledge.

Castells, Manuel (1996) *The Rise of the Network Society*. Cambridge, MA: Blackwell Publishers.

Cavender, Gray (2004) 'Media and Crime Policy: A Reconsideration of David Garland's *The Culture of Control*', *Punishment & Society* 6(3): 335–48.

Cole, Simon A. and Henry N. Pontell (2006) '"Don't Be Low Hanging Fruit": Identity Theft as Moral Panic', in T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*, pp. 125–47. New York: Routledge.

Comaroff, Jean and John L. Comaroff (2000) 'Millennial Capitalism: First Thoughts on a Second Coming', *Public Culture* 12(2): 291–343.

Cooper, Marc (2007) 'Lockdown in Greeley: How Immigration Raids Terrorized a Colorado Town', *The Nation*, 26 February, pp. 11–16.

Davis, Mike (1990) *City of Quartz: Excavating the Future in Los Angeles*. New York: Vintage.

Davis, Mike (2006) 'Who Is Killing New Orleans?', *The Nation*, 10 April. Available at http://www.thenation.com/doc/20060410/davis

Department of Homeland Security (2006) 'Remarks by Secretary of Homeland Security Michael Chertoff, Immigration and Customs Enforcement Assistant Secretary Julie Myers, and Federal Trade Commission Chairman Deborah Platt Majoras at a Press Conference on Operation Wagon Train', 13 December. Available at http://www.dhs.gov/xnews/releases/pr_1166047951514.shtm

Duggan, Lisa (2003) *The Twilight of Equality? Neoliberalism, Cultural Politics, and the Attack on Democracy*. Boston, MA: Beacon Press.

Dupont, Danica and Frank Pearce (2001) 'Foucault Contra Foucault: Rereading the "Governmentality" Papers', *Theoretical Criminology* 5(2): 123–58.

Electronic Frontier Foundation (2006) *EFF Sues AT&T to Stop Illegal Surveillance* [website]. Electronic Frontier Foundation, 31 January. Available at http://www.eff.org/news/archives/2006_01.php#004369 (accessed 5 June 2006).

Ericson, Richard V. (2007) *Crime in an Insecure World*. Cambridge: Polity.

Federal Trade Commission (2006a) *Federal Trade Commission: Your National Resource about ID Theft* [website]. Federal Trade Commission. Available at http://www.consumer.gov/idtheft (accessed 5 June 2006).

Federal Trade Commission (2006b) *FTC Releases Top 10 Consumer Fraud Complaint Categories* [website]. Federal Trade Commission. Available at http://www.ftc.gov/opa/2006/01/topten.htm (accessed 5 June 2006).

Federal Trade Commission (2008) *About Identity Theft* [website]. Federal Trade Commission. Available at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (accessed 19 October 2008).

Fernandez, Luis A. (2008) *Policing Dissent: Social Control and the Anti-Globalization Movement*. New Brunswick, NJ: Rutgers University Press.

Ferrell, Jeff (2006) 'Notes from the Trash Heaps of America', School of Justice and Social Inquiry lecture at Arizona State University, 23 March.

Fisher, Jill A. (2007) 'Coming Soon to a Physician Near You: Medical Neoliberalism and Pharmaceutical Clinical Trials', *Harvard Health Policy Review* 8(1): 61–70.

Foucault, Michel (1977) *Discipline and Punish: The Birth of the Prison*. New York: Vintage.

Foucault, Michel (2003) *'Society Must Be Defended': Lectures at the College de France, 1975–76*. New York: Picador.

Garland, David (2001) *The Culture of Control: Crime and Social Order in Contemporary Society*. Chicago, IL: University of Chicago Press.

Giroux, Henry A. (2004) *The Terror of Neoliberalism: Authoritarianism and the Eclipse of Democracy*. Boulder, CO: Paradigm Publishers.

Goode, Erich and Nachman Ben-Yehuda (1994) *Moral Panics: The Social Construction of Deviance*. Cambridge, MA: Blackwell.

Graham, Stephen and Simon Marvin (2001) *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. New York: Routledge.

Haggerty, Kevin D. (2004a) 'Displaced Expertise: Three Constraints on the Policy-Relevance of Criminological Thought', *Theoretical Criminology* 8(2): 211–31.

Haggerty, Kevin D. (2004b) 'Technology and Crime Policy: Reply to Michael Jacobson', *Theoretical Criminology* 8(4): 491–7.

Hardt, Michael and Antonio Negri (2000) *Empire*. Cambridge: Harvard University Press.

Harvey, David (1990) *The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change*. Cambridge, MA: Blackwell.

Hess, David J. (2007) *Alternative Pathways in Science and Industry: Activism, Innovation, and the Environment in an Era of Globalization*. Cambridge: MIT Press.

Jameson, Fredric (1984) 'Postmodernism, or the Cultural Logic of Late Capitalism', *New Left Review* 146: 53–92.

Juris, Jeffrey S. (2008) *Networking Futures: The Movements Against Corporate Globalization*. Durham, NC: Duke University Press.

Katz, Cindi (2006) 'The State Goes Home: Local Hypervigilance of Children and the Global Retreat from Social Reproduction', in T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*, pp. 27–36. New York: Routledge.

Kawamoto, Dawn (2006) 'ChoicePoint to Pay $15 Million Over Data Leak', *CNET News.com*, 26 January. Available at http://news.com.com/ChoicePoint+to+pay+15+million+over+data+leak/2100–7350_3–6031629.html

Konrad, Rachel (2007) 'Gap Job Applicants' Data Stolen', *Associated Press*, 28 September.

Krim, Jonathan and Michael Barbaro (2005) '40 Million Credit Card Numbers Hacked: Data Breached at Processing Center', *Washington Post*, 18 June, p. A01. Available at http://www.washingtonpost.com/wp-dyn/content/article/2005/06/17/AR2005061701031.html

Kupchik, Aaron and Torin Monahan (2006) 'The New American School: Preparation for Post-Industrial Discipline', *British Journal of Sociology of Education* 27(5): 617–31.

Landau, Saul (2004) *The Business of America: How Consumers Have Replaced Citizens and How We can Reverse the Trend*. New York: Routledge.

Latour, Bruno (1992) 'Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts', in W.E. Bijker and John Law (ed.) *Shaping Technology/Building Society: Studies in Sociotechnical Change*, pp. 225–58. Cambridge: MIT Press.

Leinwand, Donna (2006) 'Immigration Raid Linked to ID Theft, Chertoff Says', *USAToday.com*, 13 December. Available at http://www.usatoday.com/news/nation/2006–12–13-immigration_x.htm

Leland, John and Tom Zeller Jr (2006) 'Technology and Easy Credit Give Identity Thieves an Edge', *New York Times*, 30 May. http://www.nytimes.com/2006/05/30/us/30identity.html

Lessig, Lawrence (1999) *Code: And Other Laws of Cyberspace*. New York: Basic Books.

Levi, Michael and David S. Wall (2004) 'Technologies, Security, and Privacy in the Post-9/11 European Information Society', *Journal of Law and Society* 31(2): 194–220.

Martin, Emily (2000) 'Flexible Survivors', *Cultural Values* 4(4): 512–17.

Martin, Emily (2007) *Bipolar Expeditions: Mania and Depression in American Culture*. Princeton, NJ: Princeton University Press.

Monahan, Torin (2005) *Globalization, Technological Change, and Public Education*. New York: Routledge.

Monahan, Torin (2006a) 'Electronic Fortification in Phoenix: Surveillance Technologies and Social Regulation in Residential Communities', *Urban Affairs Review* 42(2): 169–92.

Monahan, Torin (2006b) 'Securing the Homeland: Torture, Preparedness, and the Right to Let Die', Social Justice 33(1): 95–105.

Monahan, Torin (2006c) 'Questioning Surveillance and Security', in T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*, pp. 1–23. New York: Routledge.

Murakami Wood, David (2008) *I'm Back But Things are Much the Same* [Blog]. Available at http://blogs.ncl.ac.uk/blogs/index.php/d.f.j.wood/2008/10/13/i_m_back_but_things_are_much_the_same (accessed 19 October 2008).

O'Harrow, Robert (2005) *No Place to Hide*. New York: Free Press.

O'Malley, Pat (2004) *Risk, Uncertainty, and Government*. London: GlassHouse.

Phoenix Police Department (2006) *Identity Theft: Learn to Protect Yourself* [Website]. Phoenix Police Department 2006. Available at http://www.ci.phoenix.az.us/POLICE/idthef1.html (accessed 5 June 2006).

Poster, Mark (2006) *Information Please: Culture and Politics in the Age of Digital Machines*. Durham, NC: Duke University Press.

Reuters (2006) 'Data on 26.5 Million Veterans Stolen from Home', *CNN.com*, 22 May. Available at http://www.cnn.com/2006/US/05/22/vets.data.reut/index.html

Rose, Nikolas S. (1999) *Powers of Freedom: Reframing Political Thought*. New York: Cambridge University Press.

Sassen, Saskia (1991) *The Global City: New York, London, Tokyo*. Princeton, NJ: Princeton University Press.

Saulny, Susan (2008) 'Hundreds Are Arrested in U.S. Sweep of Meat Plant', *New York Times*, 13 May. http://www.nytimes.com/2008/05/13/us/13immig.html

Schwartz, Hillel (1996) *The Culture of the Copy: Striking Likenesses, Unreasonable Facsimiles*. New York: Zone Books.

Simon, Jonathan (2006) *Governing through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. New York: Oxford University Press.

Singer, P.W. (2003) *Corporate Warriors: The Rise of the Privatized Military Industry*. Ithaca, NY: Cornell University Press.

Singh, Anne-Marie (2005) 'Private Security and Crime Control', *Theoretical Criminology* 9(2): 153–74.

Stopijacking.com (2006) Stopijacking.com [Website]. Available at Stopijacking.com (accessed 30 June 2006).

Sullivan, Bob (2004) 'The Meth Connection to Identity Theft: Drug Addiction Plays a Part in Many Crime Rings, Cops Say', *MSNBC*, 10 March. Available at http://www.msnbc.msn.com/id/4460349/

US General Accounting Office (2002) *Identity Theft: Greater Awareness and Use of Existing Data Are Needed* (June). Washington, DC. Available at http://www.gao.gov/new.items/d02766.pdf

Vamosi, Robert (2005) 'Of ID Theft, Paris Hilton, and Methamphetamines', *CNET Reviews*, 27 May. Available at http://reviews.cnet.com/4520–3513_7–6231353–1.html

Wacquant, Loïc (2001) 'Deadly Symbiosis: When Ghetto and Prison Meet and Mesh', *Punishment & Society* 3(1): 95–134.

Whitson, Jennifer. R. (2006) 'Assumed Identities: Responses to Identity Theft in an Era of Information Capitalism', Masters thesis, Edmonton, University of Alberta.

Whitson, Jennifer R. and Kevin D. Haggerty (2007) 'Stolen Identities', *Criminal Justice Matters* 68: 39–40.

Whitson, Jennifer R. and Kevin D. Haggerty (2008) 'Identity Theft and the Care of the Virtual Self', *Economy and Society* 37(4): 572–94.

Winner, Langdon (1977) *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought*. Cambridge: MIT Press.

Winner, Langdon (1986) *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago, IL: University of Chicago Press.

TORIN MONAHAN is Associate Professor of Human and Organizational Development and Associate Professor of Medicine at Vanderbilt University. He is Editor of *Surveillance and Security: Technological Politics and Power in Everyday Life* (Routledge, 2006) and author of *Globalization, Technological Change, and Public Education* (Routledge, 2005).