Henry Pontell [*]

'PLEASED TO MEET YOU...WON'T YOU GUESS MY NAME?'

IDENTITY FRAUD, CYBER-CRIME, AND WHITE-COLLAR DELINQUENCY

ABSTRACT

This paper documents the growing relationships between identity fraud, cyber-crime and 'white-collar delinquency' (which refers to adolescents — primarily hackers — who, by virtue of access to computers and the Internet, can now engage in major economic crimes that were once the exclusive realm of adults). Computer-savvy teenagers, who engage in cyber-crimes, including the theft and destruction of databases and personal information, increasingly commit serious economic offences, including identity fraud. Using available data from both Australia and the United States, etiology, control and policy issues are addressed through a review of case studies and theoretical concerns in criminology regarding juvenile delinquency, surveillance, technology, and white-collar crime.

> *Regard your good name as the richest jewels you can possibly be possessed of; for credit is like fire. When once you have kindled it you may easily preserve it, but if you once extinguish it, you will find it an arduous task to rekindle it again.*
>
> *Socrates*

Since it is not likely that Socrates could have envisioned the state of the world thousands of years after he wrote this, he most certainly could not have fathomed that his words would ring more true today than at any other time in history.

Identity fraud is primarily a tool used to facilitate some other criminal act. Stealing another person's identity does not have to enter into the picture. As the September 11 terrorists proved, identity theft was not necessary in the commission of one of the most heinous acts in history.[1] About a month before the attack on the World Trade Centre, Abdul Azziz Alomari and Ahmed Saleh Alghamdi, two of the terrorists who crashed planes into the north and south towers, used an accomplice to approach a

[*] University of California, Irvine; Visiting Professor, Centre for Tax System Integrity, Research School of Social Sciences, Australian National University. Paper presented by Professor Pontell at a Forum on Identity Fraud, held at the University of Adelaide Law School, 21 October 2002.

[1] N A Willox Jr and T M Regan, 'Identity Fraud: Providing a Solution' [2002] March, *Lexis Nexis*.

secretary of a Virginia lawyer.[2] The secretary was paid to complete false Virginia affidavits and residency certifications. The documents indicated that Alomari and Alghamdi lived in Virginia, when in fact they were residing in motels in the state of Maryland. The two men later used these false documents, which were notarised by the secretary, to obtain official identification papers from the state of Virginia. These documents allowed them to board the doomed planes.[3] They did not need to steal another's identity, or commit what is known as 'true person fraud'. The September 11 hijackers made wholesale use of fictitious social security numbers, false identities, and fraudulent identification documents in their attack on the United States.[4]

Identity fraud — or the use of false identities or fraudulent identification documents — has been the subject of much discussion, debate and legislation in recent years. In the United States prior to September 11, attention focused primarily on financial fraud, and retail and consumer crime matters. That attention has now been substantially broadened. No longer only the tool of the con-artist or organised criminal, identity fraud is central to almost any criminal enterprise, including cyber-crimes, terrorism, drug trafficking, alien smuggling, and common theft.

Identity fraud is one of the fastest growing and more insidious crime problems in the world today. Its myriad forms and use in facilitating other crimes pose unique and unprecedented challenges. These challenges require planning, coordination, and cooperation among government agencies and the private sector on both national and international levels.

Identity fraud is an effective crime tool employed by individuals, organised crime groups, and terrorists. It generally involves a person falsely representing himself or herself as either another person or a fictitious person. It may also take the form of persons fraudulently representing themselves through the misrepresentation of crucial facts regarding their own identity as in the case of the 9-11 attack. These misrepresentations of identity are made possible by either obtaining (through theft or fraud) documents and personal data of another individual or by the production of false documents themselves.

'Identity fraud' is a far more inclusive crime category than 'identity theft', where one uses the identity of another to enact a criminal offence. By taking advantage of weak or ineffective identification and authentication systems, criminals have victimised consumers, credit card companies, government agencies, businesses, and entire nations. The growth in such offences is linked to the increased use of computers and

[2] *United States v Zacarias Moussaoui*, USDC, ED Va., Dec 2001 term, Indictment [104]–[107].

[3] J Krim and R O'Harrow Jr, 'National ID Cards Gaining Support', *Washington Post*, 17 December 2001.

[4] Ibid.

the Internet. Given the accelerated pace of these crimes in recent years, computers have done for identity fraud what the microwave has done for popcorn. Moreover, financial crimes, many of which involve some form of identity fraud, are not only easily enacted through electronic means, but are increasingly committed by computer-savvy teenagers.

The once harmless pranks of computer hackers have evolved into major economic crimes and acts of terrorism — viruses causing worldwide damage, security breaches, large-scale economic crimes, and the illegal copying (pirating) of software. These offenses are not committed by 'juvenile delinquents' in the usual sense, since they can cause massive international destruction and loss. Activities of this nature are usually found within the realm of organised and white-collar crime. Yet, because they do not occupy the occupational positions that offer opportunities to engage in traditional white-collar crimes, economic crimes by juveniles have fallen between the cracks of conventional theory. Criminologists and others have failed to adequately account for these new forms of deviance.

The use of identity fraud as a tool for financial fraud has been enhanced by new technology. That technology is available to juveniles as well as adults and it is, in many respects, even more accessible to juveniles.

The Internet has been noted in numerous reports as a major factor in the tremendous growth of identity fraud. Information is more freely and widely available, and databases containing private information exist at numerous commercial and government sites. In too many instances, the security of this data has been compromised, or the information has been stolen, or improperly used. This can result from criminal activities by individuals both within and outside agencies and businesses that are charged with their protection. The anonymity afforded by cyberspace, coupled with technological advances, have outpaced effective regulatory and enforcement schemes, and broadened the scope and possibilities for crime in general. Many of these cyber-crimes are associated with e-commerce and involve the use of false or stolen identities.

It is clear from both the US and Australian experience that identity fraud poses serious challenges and policy choices that generally centre on issues of cost and control. Though cost and control may seem separate concerns, I will argue from a white-collar crime perspective that they are inexorably intertwined. Following this, I will relate the corresponding growth of cyber-crime and identity fraud to another phenomenon that has not yet received adequate attention; computer-savvy teenagers who engage in 'white-collar delinquency' and are responsible for increasing numbers of major economic crimes. Finally, I will offer some overarching concepts that bear directly on prevention strategies and means of control currently underway in Australia, and elsewhere.

The Identity Fraud Problem in the US and Australia: Questions of Numbers and Prevalence

The numbers associated with identity fraud have become staggering in recent years, and continue to increase. The United States Secret Service (USSS), which along with other agencies has jurisdiction over financial crimes, reported in 1997 that of the nearly 10,000 arrests by its agents, 94 per cent involved identity fraud.[5] Similarly, US Postal Inspectors and the USSS have ascertained that organised crime groups have made identity fraud a major part of their international operations in the commission of financial crimes, drug shipments, immigration violations, and violent crimes.[6] The victimisation of individuals and corporations through identity theft has also been documented. For example, one recent report notes that almost all (96 per cent) of the approximate US$407 million in fraud losses reported by MasterCard in 1997 were attributed to identity theft.[7] The USSS also reported that the losses due to identity theft in 1997 for which arrests were made totaled almost three-quarters of a billion dollars, which represented twice the figure of the previous two years.[8] This figure is likely to be higher now, as the Internet and computer use have expanded considerably over the past five years.

A study issued by the US General Accounting Office (GAO) in March 2002 reports numerous problems in the collection of pertinent identity fraud information by government agencies and businesses. The study is limited to identity theft and the victimisation of consumers and e-commerce. It does not extend to fraud involving government entitlement programs, which cover such areas as social security, health care, and welfare. This narrow focus on consumer identity theft, can only lead to a vast underestimate of the true prevalence and cost of identity fraud. The GAO found no systematic data to test assumptions regarding non-reporting or whether those who made reports were actual victims, or 'preventative' callers (those who had lost documents, or had them physically stolen in wallets or purses). Using anecdotal data, the GAO concluded that the problem seemed to be increasing in both prevalence and cost.

The GAO findings reflect the rather dismal state of affairs in the United States regarding efforts to prevent and control identity fraud. Coordination efforts of various agencies are not mentioned, nor are they likely to be optimal, given past history. Moreover, the FBI and USSS have adopted the 'back-end enforcement stance' that identity fraud is not a 'stand alone' crime, but rather a component of white-collar and financial crimes, such as bank, credit card or electronic device frauds or counterfeiting.

[5] General Accounting Office, 'Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited', May 1998, 29 (GAO/GCD-98-100BR).

[6] *Identity Theft and Assumption Deterrence Act*, S. Rep. No. 105–274, 7. (1998).

[7] GAO, above n 5, 44.

[8] Ibid 28.

AUSTRALIAN TRENDS

In 2000, the House of Representatives Standing Committee on Economics, Finance and Public Administration of the Parliament of Australia published a study entitled, *Numbers on the Run*, which reviewed the findings of the Australian National Audit Office (ANAO) Report on the Management of Tax File Numbers (TFN).[9] The ANAO study of the TFN system found: 3.2 million more TFNs than people in Australia at the last census; 185,000 potential duplicate tax records for individuals; 62 per cent of deceased clients not recorded as such in a sample match; and 40 per cent of deregistered companies still recorded as active.[10] These findings, together with an estimate of almost half a billion dollars in uncollected tax revenue, led to the overall conclusion that the Australian Tax Office (ATO) was

> … an organisation that is reactive rather than proactive; where emphasis is placed on strategies that return a short term financial gain rather than ensuring the long term integrity of the system; and where management philosophies are not well translated through the organisation.[11]

While this unflattering portrait undoubtedly applies in varying degrees to many, if not most, public bureaucracies and large corporations in the world today, it was a call to clean up and ensure the integrity of the nation's TFN system. The Parliamentary inquiry provided 26 recommendations, covering the areas of ATO data and systems quality, data matching, TFN registration, tax treatment and work rights of non-residents, identity fraud and proof of identity processes, extending the TFN quotation, and the implications for the Australian business number. Most of the recommendations relate to improving data integrity and quality, improving internal processes, proactive links with other agencies, additional audits, preventing frauds, and the provision of better proof of identity processes and better assessment of the problems of identity fraud.

The Standing Committee noted that there are numerous agencies and groups investigating identity fraud, and the provision of better data integrity and document processing in public agencies. These include the Office of Strategic Crime Assessments, a working group chaired by AUSTRAC, the Australian Registrars Conference, the Heads of Fraud Conference, and the Australian Bureau of Criminal Intelligence.[12]

[9] Australian National Audit Office, *Management of Tax File Numbers —Australian Taxation Office*, Audit Report No. 37, 1998–99, Canberra.

[10] House of Representatives Standing Committee on Economics, Finance and Public Administration, Parliament of the Commonwealth of Australia, *Numbers on the Run*, August 2000, Canberra.

[11] Ibid, Foreword.

[12] Ibid 65–6.

The ANAO report noted the ease with which identity fraud could be committed through obtaining false documents, and the associated problems for government agencies involved in the verification of identity. It also found that identity fraud posed a significant and growing problem especially with the development of new technology related to electronic commerce. This was indicated by the estimate that 25 per cent of frauds reported to the Australian Federal Police involved the theft of identity, the availability of 'identity kits' to generate high quality false documents, and the trade in fabricated documents of identity via the Internet and other avenues of sale.[13]

The Parliamentary Committee recommended that: Commonwealth government agencies work with other levels of government and industry to develop statistics regarding the extent and cost of identity fraud; that the ATO improve internal processes for both establishing identity and preventing identity fraud; that the government begin a formal process for assessing risks of identity fraud and that the Commonwealth government develop a process for working with official agencies and industry to develop strategies for reducing and preventing identity fraud, including the possibility of a national electronic gateway for verifying documents. These efforts are currently underway. It is important to note that the Inquiry's report and recommendations highlight that the problem of identity fraud is a 'whole of community problem'.

INHERENT PROBLEMS IN MEASURING COST AND PREVALENCE: IDENTITY FRAUD AS WHITE-COLLAR CRIME

A substantial body of research on the hidden and costly nature of white-collar crime in the United States, Australia and elsewhere suggests that governmental efforts to produce more data, 'cost and prevalence estimates', and to 'quantify the economic impact of identity fraud' as providing 'a powerful step toward ensuring support for reform across all levels of government, business and the community', may not prove to be particularly effective.

Major white-collar crimes, especially financial frauds, remain undetected unless victims report them, systematic investigation leads to discovery, or serendipitous events lead to their recognition. Financial crimes can be enacted through a number of mechanisms such as identity frauds, accounting frauds, and insider control frauds, which can result in massive losses to both organisational and individual victims. There is much evidence that has already been amassed in the United States to establish this as fact. How much crime 'actually exists' is determined by the organisational resources available to uncover and investigate it, prosecute it, and more generally, enforce what most experts already regard as inadequate laws aimed at

[13] Ibid 67.

its control. Moreover, there is a general unwillingness of government bureaucracies and large financial institutions to publicly admit that their systems are not working, which contributes to the under-reporting of fraud. Hence, the problem that has yet to be resolved is the accurate assessment of the level of undetected and unreported crime.

The irony here is that the capacity to do this in an effective manner is itself determined by the political will to take fraud seriously enough to devote investigative resources in the first place. If that same political will is dependent on proving, through the production of numbers, that there is a significant problem, the cycle of non-discovery and non-recognition remains intact. This is central to understanding the cost and prevalence of white-collar crime, which is apt to be neither reported nor recorded in a timely or accurate manner.

In fact, as we have seen over the past two decades, the most consequential white-collar crimes such as the savings and loan debacle and the recent corporate scandals in the United States, which have affected not only national but international markets, are brought to public attention only *after* massive losses are realised, and even then, the cost, nature, and causes of fraud continue to be debated. The collapse of Enron caught the markets by surprise. The day before the mammoth company declared bankruptcy, six major research analysts still had a *strong buy* rating on the company.[14] By the time the dust had cleared (or, to use more appropriate imagery, Anderson's accounting documents had been shredded) the company was in a fraud-induced multi-billion dollar bankruptcy that was, at the time, the largest in history. The discovery of phony accounting schemes and internal fraud at Enron provided the 'wake up call' that led to closer scrutiny of other major companies, in what became the largest set of corporate scandals the world has ever seen.

Similarly, during the savings and loan crisis of the 1980s, the focus on Charles Keating's Lincoln Savings and Loan, the largest of the financial institution failures (over $4 billion), neglected the fact that similar frauds were occurring throughout the entire thrift industry. Years later, after it was acknowledged that this was in fact the case, the bill to taxpayers amounted to over $150 billion. Given time and resource constraints, enforcers adopted a 'rifle shot' approach to investigating cases. Limited organisational capacity, time limits for prosecution, and the overwhelming complexity and volume of cases forced this course of action. Bringing charges for all wrongdoing was simply impossible, although substantial evidence was likely to exist. Even with the largest single infusion of supplemental enforcement resources in US history, criminal investigators were only able to pursue the largest cases, and to charge only those acts of wrongdoing that were the most simple and straightforward to prove. Adjudicating all acts of fraud would have been impossible. Many known

[14] 'Enron in Perfect Hindsight', BusinessWeek.com. 19 December 2001.

and suspected crimes were never charged or recorded as such in official reports which document the extent, nature, and role of financial institution fraud during the savings and loan debacle.

These two cases also illuminate the operational definition of cost. Should the 'cost' be calculated based on the specific transactions that were fraudulent? Only those activities that bring criminal charges? Only those criminal activities that end up being adjudicated? Fraud costs cited in actual convictions? The cost of the bankruptcies and failures caused by fraudulent activity? Costs of investigation and prosecution? Investor and taxpayer losses? Some combination of these? Each of these headings represents the true 'costs' of fraud. To take a more recent case, what price tag would a potential cost study put on the World Trade Centre disaster that could be considered 'reasonable' or encompassing of all losses?

Simply put, studies can never fully recognise the cost of fraud because of its hidden and unreported nature, and the inability or unwillingness of agencies and businesses to discover, or record it in a timely manner. Rather, they are bound to arrive at figures that under-represent the true extent of the problem.[15]

Thus, any extrapolation from existing reported figures, or those gained through surveys will necessarily produce an absolutely conservative estimate of identity fraud. Moreover, given the rapidly increasing number of identity fraud cases, its growth curve will need to be taken into account as well. These are manifest considerations for future policy, especially in regard to realistic resource allocations.

Ethnographic and qualitative study of the behavior of official agencies regarding the treatment and processing of identity fraud, and the attitudes, beliefs and behaviors of private industry and consumers would provide important information for properly grounding cost estimates, as well as for prevention and control strategies. These factors speak to organisational capacities for generating the information upon which cost and prevalence estimates are ultimately based. For example, a recent report issued by the GAO in the US notes numerous problems regarding non-enforcement that directly affect the production of cost and prevalence estimates by official agencies and organisations. These problems include shortages in police department resources, turf battles, lack of awareness of the importance of reporting identity theft, and jurisdictional issues.[16] The study notes, for example, that about one third of victims who contacted the US Federal Trade Commission's identity fraud hotline between November 1999 and October 2000 had tried and failed to file a report with

[15] A Biderman and A J Reiss Jr, *Data Sources on White-Collar Law-Breaking,* US Government Printing Office, 1980.

[16] L Kellman, Government: 'Identity Theft is Fastest-Growing U.S. Crime, But Laws Aren't Widely Enforced', *Associated Press*, 30 July 2002.

local police.[17] There was some improvement in 2001, when the proportion declined to about one fifth.[18] Since no standardised data yet exists, the GAO collected qualitative data from 10 states with the highest reported incidence of identity theft and found that many law enforcement agencies do not file reports, and that there are inadequate numbers of prosecutors to take cases. One chief prosecutor in a major city noted the problem of enforcement capacity bluntly: 'given competing priorities and other factors, there is little incentive' for police departments to spend money on identity theft probes.[19]

Cyber Crime, White-Collar Delinquency and Identity Fraud

As mentioned earlier, much of the growth in identity fraud, regardless of its exact amount or cost, is a result of the Internet and the corresponding unprecedented access it allows to numerous databases where personal information is stored. Moreover, service standards typically overrule compliance and integrity functions, and the speed of financial transactions that are enabled by new technology, makes it difficult to discover frauds and recover losses. Problems are exacerbated by the diversity of criminal groups involved. Apart from con-artists, organised crime groups, and opportunistic individual criminals, another criminal element is lurking. They are the astutely computer-literate youth of the world who have become part of the deviant sub-culture of hacking. The proliferation of identity fraud and the crimes it facilitates, is directly related to the proliferation of cyber-crime. The following discussion of cases illustrates the enormous implications of computer hacking, and the equally serious problem of associated 'white-collar delinquency' as they relate to identity fraud. The problems encountered in these cases are compounded by the difficulty in identifying the perpetrators. Regarding terrorism, for example, computer-based attacks may be much easier carry out than more traditional acts, in large part because they can be carried out by perpetrators who are many thousands of miles from the target and concealed by the anonymity afforded by cyberspace. A senior CIA official has said that foreign cyber-attackers can easily obtain technology that enables them 'to conceal points of origin by hopping through several intermediate way stations in cyberspace [and then] erase cyber-footprints from victim computers'. It may even be possible to make it appear that an attack has been carried out by an ally.[20]

Moreover, two generations of hackers, crackers, cyber-punks, phone phreaks, viruses, worms, logic-bombs, trap-doors, trojan horses, and salami slicers have underscored the

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] C L Staten, 'Recent DoS Attacks Point Out Already Known Vulnerability of US Infrastructure', *Daily Intelligence Report* – ERRI Risk Assessment Services, Vol 6, 20 March 2000, 1–6.

first law of electronic crime: *If it can be done, someone will do it.* It is important to keep this 'law' in mind, because almost none of the worst-case cyber-white-collar delinquency scenarios have yet occurred. Computer crimes, many of which involve identity fraud, are considered the fastest growing category of crime in the US. If white-collar delinquents — some of them too young to buy a drink — have successfully attacked banks, corporations, telecommunication systems, government and commercial websites and information systems, sometimes with devastating consequences, can their increased participation in identity frauds be far behind?

In other words, it may be highly instructive to suggest what *might* be done, by revealing what already *has* been done. Take the same tools and methods used by white-collar criminals and place them in the hands of juveniles, and innocent computer misdeeds become massive economic crimes, minor nuisances become major corporate losses, and showing-off becomes identity fraud. It is not my intent to cry that the sky is falling. Rather, I want to underscore the fact that white-collar delinquency is a serious and growing problem with ramifications for control efforts aimed at both cyber-crime and identity fraud.

Most hackers display what Jay 'Buck' Bloombecker, director of the US National Center for Computer Crime Data, terms a 'playpen mentality'.[21] They see breaking into a system as a goal, not a means to a criminal end.

At least two categories of 'playpen' hackers have been identified: creative 'showoffs', who break into databases for fun, rather than profit; and 'cookbook hackers', the most common category, defined as computer buffs who coast along the global Internet computer network without any specific target, twisting electronic door knobs to see what systems fly open.[22] The 'recipes' used by the 'cookbook' hackers generally are those that have been developed by the more knowledgeable 'showoffs'. Many of these recipes are apparently of gourmet quality. A security analyst for AT&T has estimated that less than 5 per cent of intrusions into computer systems by outsiders are even detected, let alone traced.[23]

Hackers might be thought of as a deviant sub-culture. They subscribe to a set of norms, which apparently they take very seriously, but which often conflicts with the norms of the dominant society. They have their own peculiar code of ethics, known as the 'cyberpunk imperatives'. For instance, they believe computerised data is public property and that passwords and other security features are only hurdles to be jumped

[21] Quoted in B Beyers, 'Are You Vulnerable to Cybercrime? Hackers Tap in for Fun, Profit.' *USA Today*, 20 February 1995, 3B.

[22] '"Billy the Kid" Hacker Was not a Threat to Networks', *Houston Post*, 17 February 1995, 15.

[23] Ibid.

in pursuit of this communal data.[24] A famous hacker known as The Knightmare has summed up his haughty creed: 'Whatever one mind can hide, another can discover'.[25] There is even an ultimate proscription: 'Hackers will do just about anything to break into a computer except crashing the system. That's the only taboo'.[26]

Another way of looking at young hackers is from the perspective of Sykes and Matza's well-known 'drift' theory of delinquency.[27] From this perspective, hackers are fundamentally conforming youths who drift into occasionally deviant behavior through the use of such 'neutralisations' as the claim that they are only trying to expose lax security systems or merely trying to learn more about computers.[28] These may seem like lame rationalisations, but more than one young hacker has justified his misconduct on those very grounds.

Furthermore, even the most sophomoric intentions can go terribly awry. A group of seven Milwaukee high school students — devoted electronic joy riders who called themselves the '414' gang — learned this lesson in 1983. They were from all accounts nice young men; loving sons, Eagle Scouts, exemplary students. But in the name of 'fun-and-games', they managed to break into a file at the Los Alamos, New Mexico, nuclear weapons facility and they were also able to erase a confidential file at New York's Memorial Sloan-Kettering Cancer Center.[29] When they were apprehended, they denied any criminality in their actions. Their public statements seemed to be drawn directly from Sykes and Matza's inventory of neutralisation techniques: '[I]t's not our fault' [denial of responsibility]; 'We didn't intend harm' [denial of injury]; 'There was no security' [denial of victim].[30]

Beyond the 'playpen mentality', however, there is a dark side to hacking, personified by a very different species of 'stunt hacker' whose motivations are undeniably malicious and ostensibly criminal. One such individual revealed his dark side in an article he wrote under the ominous pen name Mr X:

[24] J T McEwen, 'Computer Ethics', *National Institute of Justice Reports*. January/February 1991, 8–11.

[25] Quoted in R A Cizmadia, 'Secrets of a Super Hacker' (Book Review). *Security Management* 38, September 1994, 197.

[26] Ibid 9.

[27] G M Sykes and D Matza, 'Techniques of Neutralization: A Theory of Delinquency' (1957) 22 *American Sociological Review*, 664–6.

[28] P Keefe, 'Portraits of Hackers as Young Adventurers Not Convincing', (1992) *Computerworld* 26, 33.

[29] P O'Driscoll, 'At 17, a Pro at Testifying on Computers', *USA Today*, 26 September 1983, 2A.

[30] D B Francis, *Computer Crime* (1987) 28.

> I can turn off your electricity or phone, destroy your credit rating – even take money out of your bank account – without ever leaving the keyboard of my home computer. And you would never know I was the one ruining your life![31]

If one doubts the plausibility of Mr X's frightening boast, consider that in 1985 seven New Jersey teenagers were arrested for stealing $30,000 worth of computer equipment, which they had billed to total strangers on hacked credit card numbers.[32] Hackers have also invaded credit files — including those at TRW, the America's largest credit information storage system.[33] As one victim has lamented, 'There's only one problem with having good credit. Someone may steal it'.[34] His comment reiterates Socrates' warning, and places it in a 21st century context.

Consider as well the career of 'Dr Demonicus'. A bright young man with awesome computer skills, his lack of interest in academic study landed him behind the counter of a fast-food restaurant after graduation from high school. His ambition, however, soon transformed him from a classic under-achiever to a wealthy alleged felon. According to charges in a federal indictment, he would scan telephone directories for the names of presumably well-heeled doctors and lawyers, then hack the local credit bureau for their credit card numbers. He was further accused of using those numbers to buy $200,000 worth of merchandise, directing deliveries to vacant houses held by the Department of Housing and Urban Development. Later, like a postman in reverse, he would drive his daily route and collect his packages.[35]

A journalist has offered a first-person account of his own brush with identity fraud.[36] A hacker 1000 miles away had pulled the journalist's file from a credit-reporting agency:

> In minutes…he had a virtual summary of my life: past addresses and employers, Social Security number, credit card numbers, mortgage information, bank accounts and all the other personal data that appear on the credit reports for me and 160 million other Americans. Armed with that information, he was able to open nearly 30 separate loan, checking and credit accounts at banks, department stores, electronics retailers, appliance outlets and other merchants. And he did it as fast as kids unwrap birthday presents.[37]

[31] Ibid 35.

[32] Ibid.

[33] R Benedetto, 'Computer Crooks Spy on Our Credit', *USA Today* 22–24 July 1984, 1A.

[34] S J Shaw, 'Credit Crime', *St Petersburg Times,* 23 August 1992, 1D.

[35] M Meyer, 'Stop! Cyberthief!', *Newsweek* 6 February 1995, 36–8.

[36] N J Perry, 'How to Protect Yourself From the Credit Fraud Epidemic', *Money* 24, August 1995, 38–42.

[37] Ibid 1D.

Using the pilfered credit, the thief went on a $100,000 shopping spree.

In a celebrated case, a Brooklyn NY resident was arrested by the NYC Police Department in March 2001, and charged with attempted grand larceny and possession of forged devices. What makes this case unique is that he used the Internet to pilfer huge amounts of money from the financial accounts of celebrities and business executives he found on the Forbes list of '400 Richest People in America'. Indeed, the investment accounts of alleged victims reads like a Who's Who of the country's rich and famous, including Oprah Winfrey, Steven Spielberg, George Lucas, Martha Stewart, Ross Perot, Ted Turner, and investors George Soros and Warren Buffett. The subject, who worked as a busboy in a New York restaurant, allegedly duped credit companies into providing credit histories of the celebrities by sending them forged document requests on the stationery of leading investment banks, including Merrill, Lynch and Goldman Sachs. Several of the alleged victims' social security numbers were found in his apartment.[38]

Many hackers seem to be petulant egomaniacs. For example, one hacker, who calls himself 'Garbage Heap', has bitterly complained to ComputerWorld magazine that his talents deserve more appreciation. If respect is really his goal, then 'Garbage Heap' might want to think about picking a new pseudonym.

In 1992, a group of young hackers, ranging in age from 18 to 22 and calling themselves by such exotic names as Phiber Optik, Acid Phreak, Outlaw, and Scorpion[39] were arrested for corrupting the databases of some of the largest corporations in America. The MOD, alternately known as the Masters of Destruction[40] or the Masters of Deception,[41] allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies, Martin Marietta, ITT, and the other Fortune 500 companies, several big crĕdit agencies, two major universities, and the Educational Broadcasting Network. The damage caused by these hackers was extensive. One company alone, Southwestern Bell, suffered losses of $370,000.[42]

[38] J G Huse Jr, 'Identity Fraud: A Twenty-First Century Challenge' A Presentation to the Association of Government Accountants National Conference, Boston, MA, 16 July 2001.

[39] B Brown, 'Indictment Handed Down on 'Masters of Disaster'', *Network World* 29, 1992, 34.

[40] J M Moses, 'Wiretap Inquiry Spurs Computer Hacker Charges', *Wall Street Journal,* 9 July 1992, B8.

[41] M E Thyfault, 'Feds Tap Into Major Hacker Ring', *Information Week*, 13 July 1992, 15.

[42] W Schwartau, 'Hackers Indicted for Infiltrating Corporate Networks', (1992) *Infoworld* 14, 56.

One of the most disturbing aspects of malicious hacking involves an area of government that one would expect to be the *most guarded* of all social institutions — national security. Such intrusions are not new. Over 20 years ago, a 24-year-old hacker known as Captain Zap was arrested for breaking into the White House computer system. In 1983, a 19-year-old UCLA student used his PC to enter the Defense Department's international communications system.[43] In 1991, a gang of Dutch hackers managed to crack Pacific Fleet computers during the Gulf War.[44] Two young hackers broke into computers at Boeing Corporation — a major defence contractor[45] — and later used their home computers to examine confidential government agency files.[46] More recently, an 18-year-old Israeli hacker was accused of the most organised attack ever on the Pentagon's computer system.[47] A report from the American military's inspector-general found 'serious deficiencies in the integrity and security' of a Pentagon computer used to make US$67 billion per year in payments.[48]

Even more alarming is a report released by the United States GAO in 1996, which determined that hackers had attacked Pentagon computer systems as many as 250,000 times the previous year and had gained entry in two of every three attempts.[49] The agency concluded; 'At a minimum, these attacks are a multimillion dollar nuisance to defense. At worst, they are a serious threat to national security.'[50] Members of Congress have expressed great concern over such stories, calling for tougher sanctions and federalisation of all computer crime.

'THE MOUNT EVEREST EFFECT'

In early 1998, the Pentagon's computer networks were hit by what was described as the 'most organized and systematic assault'[51] ever launched against them. Although no classified documents appeared to have been tampered with, a deputy defense secretary called the matter 'a very serious long term problem'.[52] A few weeks later, two California teenagers, aged 16 and 17, were arrested by the FBI and accused of the

[43] S Meddis, 'Lawmakers: Pull Plug on Hackers', *USA Today*, 4 November 1983, 3A.

[44] 'Blabbermouth Computers', *USA Today*, 27 July 1993, 8A.

[45] 'US Charges Young Hackers', *New York Times*, 15 November 1992, 40.

[46] 'Feds Charge 2 in Computer Break-in', *Government Computer News*, 23 November 1992, 8.

[47] 'Netanyahu Lauds Teen-Age Hacker Who Broke into Pentagon Site', *Houston Chronicle,* 20 March 1998, 21A.

[48] C Collins, 'Hackers Paradise', *USA Today*, 6 July 1993, 5A.

[49] M J Zuckerman, 'Hackers Crack Pentagon' *USA Today,* 23 May 1996, 1A.

[50] Quoted in ibid, 1A.

[51] 'Pentagon Battling 'Systematic Assault' by Hackers', *Houston Chronicle,* 26 February 1998, 15A.

[52] Ibid.

cyber-attacks. The boys, who went by the code names 'Makaveli' and 'TooShort', had used 'sniffer' programs to intercept Pentagon passwords. They also placed 'back door' programs in the military computers in order to re-enter at will.[53] They had leapfrogged from their local Internet Service Provider (ISP) into the Pentagon systems, as well as systems at the University of California at Berkeley, MIT, and two sites in Mexico.[54]

Makaveli and TooShort pleaded guilty to charges of juvenile delinquency and received three years probation and were deprived of any unsupervised computer access. They were also ordered to perform 100 hours of community service and pay $5,525 in restitution.[55] This case strongly underscores the gaping moral schism between hackers and victims. The government stressed that the boys' activities 'had the potential to disrupt military communications throughout the world'.[56] TooShort's lawyer argued that the hackers had no malicious intentions and were simply trying to explore advanced computer systems. He added, 'I call it the Mount Everest effect. They did it to prove they could.'[57]

When deviance and criminological texts discuss computer crime, they tend to treat it in largely unitary and descriptive terms (for example, 'cyber-deviance'), or to view computers as 'tools' for adults to commit various occupational crimes, such as embezzlement and fraud, that generally involve their roles in organizations and businesses. A popular textbook notes, 'Computers provide tools for a relatively recent type of occupational behavior usually targeted at or benefiting businesses...Computers offer increasingly obvious capabilities as weapons'.[58] The same text also discusses (at some length) computer crime in regard to sexual deviance as 'cyber-sex', or 'the use of computers to flirt, exchange romantic messages, and even acquire sexual satisfaction – all on line'.[59] Computers are also commonly implicated in the proliferation of pornography.[60]

It is not my purpose here to explain why hackers exist. Given the current trends in computer crime, however, acts that could be considered white-collar delinquency need more criminological attention, both through explanation and theory testing and ethnographic and descriptive study. Failure to do so, given the growing magnitude of white-collar delinquency, weakens the foundation of criminology as both an

[53] 'Pentagon Teen Hackers Ordered to Stay Off Line', *Houston Chronicle,* 6 November 1998, 2A.

[54] Ibid.

[55] Ibid.

[56] Quoted in ibid 2A.

[57] Quoted in ibid 2A.

[58] M B Clinard and R F Meier, *Sociology of Deviant Behavior* (10th ed, 1998) 198.

[59] Ibid 327.

[60] Ibid 351.

integrative and applied science. Failure to study a criminal phenomenon that has worldwide impact makes the field even more vulnerable to criticisms of irrelevance, of a misguided focus on the crimes of the relatively powerless and a general indifference towards understanding major forms of emerging deviant and criminal behaviors.

The rather lame reaction to such behavior to date has at least one plausible explanation. Edwin Lemert, perhaps the most thoughtful and brilliant observer of deviance and crime over the past century, noted in his classic formulation of the concept of 'unstable equilibrium in the societal reaction to deviance', that social response is essentially a 'compound of acceptance and rejection, frequently manifesting itself as the tacit tolerance of variant social patterns coupled with a nominal or formal disapproval and rejection'.[61] Lemert uses the examples of begging and gambling to make his point, but the same conception is useful for explaining new manifestations of deviance, such as white-collar delinquency. Given the accelerated pace of technological development and the lag between such innovation and the cultural, social, and legal responses to resulting deviant behaviors that take advantage of the technology, Lemert's formulation may be even more useful for understanding emergent forms of deviance such as white-collar delinquency than it was a half century ago in characterising responses to more established patterns of behavior. The 'ambivalent attitudes' on the part of the population and legal system toward white-collar delinquency can be partly explained, as Lemert says, by 'generalized culture conflict which affects such a large majority of the population that little consistent action is possible'.[62] This is the case for at least two reasons. First, there may be disinterest or ignorance on the part of many persons who may not have the necessary skills or background to make informed judgments. Second, as Lemert originally suggested in regard to gambling, many persons may have engaged in some form of deviance themselves. In the current case, this would entail such acts as software piracy, disk swapping, or knowingly buying illegal programs or hardware. This, Lemert argues, may result in a situation 'in which community tolerance is precariously stabilized just short of a critical point in the tolerance quotient at which collective action is taken'.[63]

Another useful rubric can be found in Jack Katz's novel work, *Seductions of Crime*.[64] Katz's conception of the criminal psyche may be particularly relevant for the study of white-collar delinquency. Katz concludes that the study of white-collar crime by conventional methods involving 'background determinism' is inherently doomed to

[61] E M Lemert, 'Societal Reaction, Differentiation, and Individuation', in Charles C Lemert and Michael F Winter, (eds), *Crime and Deviance: Essays and Innovations of Edwin M. Lemert* (2000) 34.

[62] Ibid.

[63] Ibid.

[64] J Katz, '*Seductions of Crime: Moral and Sensual Attractions in Doing Evil*' (1988).

failure because of the contradictory relationship between white-collar crime and the enforcement mechanism to control it. His point is that the categorisation of much conduct as 'white-collar crime' would be abandoned if enforcement was taken more seriously, as pressure would build from conventional sectors of society to reduce the reach of the law. White-collar delinquency may neatly fit Katz's perspective on deviance as a form of individual transcendence and projection of self. Moreover, the qualities of experience of delinquents engaged in such activities — though likely to differ in many ways from common forms of delinquency and crime — may, in many respects, mimic those of street thugs and murderers in the images of control they espouse over *victims*, whether they be faceless investors, governments, consumers, or the entire E-Commerce system.

One final distinction needs to be made. White-collar delinquency involves major financial crimes and other crimes of great cost to society (for example, server shutdowns, and related system costs) committed by juveniles. The term has no application to run-of-the mill 'computer delinquency' which may entail hacking, trespass, and system violations of small consequential, material, or fiscal impact. An ordinary juvenile hacker, who causes no great fiscal damage or loss, cannot therefore be said to be engaged in white-collar delinquency. Phony internet scams, pump and dumps, dissemination of viruses onto the world wide web and similar activities that cause massive damage to data systems, when committed by juveniles, would certainly fall into the category of white-collar delinquency. The concept can be defined as: *serious economic crimes committed by juveniles, by and large through the use of computers*. This is an important theoretical distinction. Just as Sutherland's conception of the term 'white-collar crime' was meant to denote the crimes of relatively powerful members of society, 'white-collar delinquency' refers to the crimes of computer delinquents that have serious consequences in financial terms and is clearly distinguishable from individual acts that constitute a 'nuisance'.

The distinction between white-collar delinquency and computer mischief perpetuated by juveniles is analagous to the distinction between the serious condemnation reserved for felonies and the lesser condemnation of misdemeanours. This is an important conceptual step in recognising the significance of white-collar delinquency as opposed to the general category of computer delinquency. It also allows societal and legal reactions as well as public policy discussions of computer violations by juveniles to be properly grounded, and accounts for major differences between white-collar delinquency and other acts of computer vandalism and delinquency of little, or minor consequence.

Cyber-attacks on government agencies are an escalating problem. It is now believed that at least six or seven government computers are hacked successfully every day. Moreover, many government systems in the US are invaded for months before the violation is noticed. Recently, a group called GlobalHell defaced websites operated by the White House and the Senate.[65] In 1997, a hacker interfered with the transmission of medical data from astronauts orbiting the earth.[66] In 1998, a hacker gang, called Noid, broke into military computers and was able to download software that controls the positioning of satellites.[67]

Anti-fraud systems, such as voice-recognition spectrographs, are appearing on the market. Similarly, unauthorised computer access can be obstructed through biometric technology, including retina scanners, hand print readers,[68] and DNA identification devices, as well as by the development of highly sophisticated 'firewall' software that shields private information from hackers and thieves.[69] But computer criminals respond to improved security technology with improved criminal technology[70] and they will no doubt in time find a way to keep pace. This, in turn, will encourage still more advances in security, so continuing the never-ending cycle of thrust and parry. This points to the primary significance of security in organisations handling computer data and the constant dynamic process that surrounds successful implementation of such efforts.

RESPONSES

Trying to deal with identity fraud through criminalisation alone is not an effective means of control. Yet, a few years ago, in response to a growing recognition of the problem, the US passed the *Identity Theft and Assumption Deterrence Act of 1998* (ITADA). The law states that an identity thief is anyone who '[k]nowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law'.[71] The ITADA law is limited to the use of the '[m]eans of identification of *another person*'. Thus, the use of the law is confined to 'true person fraud', or the harm that is caused by a thief assuming the identity of another. The statute does not extend to identity fraud in general. To illustrate the utter futility of attempts to build a better mousetrap merely through criminalisation, the two September 11 terrorists mentioned

[65] J J Goldman and U L McFarlane, 'Man Accused of Hacking into NASA Computers', *Los Angeles Times*, 14 July 2000, A15.

[66] Ibid.

[67] Ibid.

[68] T Falconer, 'Cyber Crooks', *CA Magazine* 128, December 1995, 12–7.

[69] W R Cheswick and S M Bellovin, '*Firewalls and Internet Security: Repelling the Wily Hacker*' (1994).

[70] G T Marx, 'Privacy and Technology', a revision of material that appeared in *The World and I*, September 1990, and *Teletronik,* January 1996.

[71] 18 USC s 1028(a)(7).

earlier did not break this law in obtaining falsified documents. Moreover, it represents an extremely limited and reactive response that focuses primarily on consumer frauds and on general deterrence as a solution. The law was followed by the *Patriot Act* of 2001,[72] which allocated major funding to national electronic crime task forces designed to enforce the laws regarding identity frauds. These laws and funds are also aimed at criminal investigation and prosecution of identity fraud after the fact. A proactive and preventive stance needs to be taken if the burgeoning threats posed by identity fraud are to be substantially reduced in the future. The agencies that might best foster this do not involve law enforcement, but the documentation and authentication of identity itself.

Professor Gary T. Marx, one of the world's leading authorities on surveillance, technology and social control mechanisms, points out that in complex settings in democratic societies 'relying primarily on technology to control human behavior has clear social and ethical limitations'.[73] Regardless of how ideal a technical control system may appear to be in the abstract, it is inevitably subject to the harsh realities of implementation and actual practice. 'The perfect technical solution is akin to the donkey incessantly chasing a carrot suspended before it'.[74] Larger systemiç contexts, consequences and alternatives may be ignored. As Marx notes,

> The complexity, and fluidity of human situations makes this a rich area for the study of trade-offs, irony and paradox. There are some parallels to iatrogenic medical practices in which one problem is cured, but at the cost of creating another. Technical efforts to insure conformity may be hindered by conflicting goals, unintended consequences, displacement, lessened equity, complacency, neutralization, invalidity, escalation, system overload, a negative image of personal dignity and the danger of the means determining, or becoming the ends.[75]

Moreover, the lack of privacy concerns and the careless use of personal information provide structural gaps in the social control of personal identity that criminals exploit.

A major irony that confronts efforts to ensure greater control is that new controls naturally create a demand for neutralisation devices in a free market economy. Moreover, an escalation in crime can result from increased control mechanisms, as violators can be convicted of multiple offences arising from the principal offence and their use of illegal means to commit the offence or avoid detection.[76]

[72] USA Patriot Act of 2001. Public Law 107-56, H.R. 3162 RDS.

[73] G T Marx, 'Technology and Social Control: The Search for the Illusive Silver Bullet', *International Encyclopedia of the Social and Behavioral Sciences*, (2001) 1.

[74] Ibid.

[75] Ibid.

[76] Ibid.

Aside from the technological aspects of control, which can be compromised in any number of ways by competing technology and various other neutralisation mechanisms and techniques, the *human context* of control also remains particularly vulnerable. This can be easily overlooked, as it exists in the long shadow of expensive and sophisticated technology and complex operational systems. Nonetheless, it can prove absolutely disastrous as illustrated by the case of 9-11. Marx provides another telling example that underscores the point that state-of-the-art control systems can be completely undermined through simple human interactions:

> ...a thief who could not break a manufacturer's sophisticated encryption code nevertheless managed to embezzle millions of dollars through generating fake invoices. He did this by having an affair with the individual who had the encryption codes.[77]

Cyber-crimes provide illustrative cases. The best (and easiest) way to break into such systems is from within the organisation. For system developers and managers, this leads to the conclusion that for any control system to be successful, both the scale and importance of internal controls grow in direct proportion to the scale of the technological controls that are developed to foil system intruders.

Much more needs to be done. New legislation that concurrently allows for individual privacy and confidentiality while giving authorities the ability to analyze existing data strictly for purposes of prevention and control may be the best answer to current and future problems. Legislation will also be necessary to fund such activities at realistic levels, and to correspondingly increase the capacity of the criminal justice system to respond to identity fraud crimes. The functions of prevention, detection, investigation, and control all go hand in hand, and require equal and sustained attention. Obviously, the better mechanisms are able to work at the front end, the less loss, system strain, and control need to result at the back end. Better mechanisms, involving the cooperative use of existing data, are available to prevent and control identity fraud.

New legislation may be the only answer at this point, and it will need to consider issues of privacy and anonymity, and specifically how data can be used, and by whom. Such legislation does not need to be complex, as a striking example of the official use of sensitive data in the United States illustrates. In 2000 it was found that people were able to steal the identity of others by accessing Federal records online.[78] Ironically, the government had been an unwitting accomplice in identity thefts by collecting Social Security numbers from Social Security Administration lists of dead persons, the Securities and Exchange Commission's mandatory filings, the Congressional Record and criminal wanted posters posted on web sites. One web site

[77] Ibid.

[78] D Blank, 'Data from Federal Records Used to Commit Identity Theft', *Government Computer News*, 2 Oct 2000, v19 i29, 8.

in Pennsylvania refused a request from the USSS to remove 4,800 military officers' Social Security numbers. Although the Government Printing Office has stopped placing the social security numbers on military promotion lists, it has been reported that many other sites continue to post them.[79]

THE NATIONAL ID DEBATE

Security and privacy issues associated with large government databases present major problems. As a result of the September 11 attacks, legislation was introduced before the United States Congress to initiate a standardised identification system that would link existing information in state motor vehicle databases to 'create a standardized driver's license equipped with technology capable of uniquely identifying the cardholder'.[80] The promoters of the bill claimed that their goal was *not* to create a national ID, but simply to stop identity fraud and terrorism that relied on the use of phony drivers licenses. The proposal, supported by the American Association of Motor Vehicle Administrators, would have allowed states to 'share demographic and driving record information in real time, and would mandate the use of security features such as holograms, fingerprints or other biometric identifiers on all state-issued ID cards'.[81]

In response to this proposed legislation, an April 2002 report from the National Academies of Science argued against a national ID card due to concerns over privacy and security of personal data collected by official agencies. The study was endorsed by the National Research Council's Computer Science and Telecommunications Board, which is comprised of a number of private sector and academic institutions including Microsoft, AT&T, MIT and Stanford. It warned that current efforts to establish a national identification system could produce more harm than good, unless policymakers first paid serious attention to an array of privacy, security, and logistical matters.[82] It also noted that the 'costs of abandoning, correcting or redesigning a system after broad deployment might well be extremely high'.[83]

The study concluded:

> Given the wide range of technological and logistical challenges, the likely direct and indirect costs, the serious potential for infringing on the rights and freedoms of ordinary citizens, and the gravity of the policy issues raised, any

[79] Ibid.

[80] B Krebs, 'National Academies Study Tempers Call for National ID', Newsbytes, 11 April 2002.

[81] Ibid.

[82] Ibid.

[83] Ibid.

> proposed nationwide identity system requires strict scrutiny and significant deliberation well in advance of design and deployment.[84]

Besides the conservative cost estimate of $100 million to make changes to the country's 200 million existing drivers' licenses, the report also warned of 'function creep' or future uses of a national ID in ways not originally intended. This phenomenon is well illustrated by the current use of Social Security numbers, which were created solely for administering Social Security benefits (that is, as an 'internal identifier'), but are now used as the major national generic identifier. Moreover, securing against the misuse of information becomes more difficult as the system of users expands beyond original boundaries, and the system itself becomes a larger and more attractive target for malicious hackers.

SELF-MONITORING AND SURVEILLANCE

Just as important as insuring the accuracy and integrity of data and systems is the major responsibility of self-policing and evaluation on an ongoing basis. One mechanism to monitor system integrity involves the use of government agents posing as persons trying to compromise it using known techniques. In discussing ideas regarding the detection of 'dirty data', for example, some researchers have pointed to the use of deceptive techniques to allow access to information that would not otherwise be available or known to others. Officials using deceptive techniques on their own agencies should raise no major ethical concerns. This allows for constant system monitoring and the identification of weak spots in need of immediate improvement. It involves proactive enforcement and regulation of identity fraud rather than reacting to system weaknesses on a case-by-case basis after the fact. Such monitoring could take the form of sophisticated and controlled field experiments that would provide substantial systematic data regarding system weaknesses upon which necessary organizational changes could be based. These system weaknesses are, after all, the crux of the identity fraud problem. This approach also entails working forward towards increased system integrity at both the human and technological levels versus simply working backwards from actual reported crimes as 'trace elements'. Moreover, there is variability in the visibility of trace elements that make them less than ideal for plugging gaps in the system. For example, Marx notes,

> Trace elements involving victims are likely to become publicly known to the extent that (a) the gap between victimization and its discovery is short, (b) the victim is personally identifiable, (c) the victim is aware of the victimization, and (d) does not fear retaliation for telling others about it. There is a parallel

[84] Ibid.

> here to the ease of discovering victim as against victimless crimes. The former are much more likely to be known about.[85]

Forming partnerships among agencies to enact such self-surveillance should not involve much new legislation, if any at all. It would allow for proactive enforcement while avoiding the usual pitfalls and practical stumbling blocks associated with the extreme positions of those who would not release or share any data with others, and those who desire that all agency data be made public. Self-surveillance would allow government agencies to avoid individual privacy issues as no data would be released. The agencies would, in effect, be 'victimising themselves' and using information internally to correct flaws in their own identification and authentication systems.

Various commentators have noted that laws and policies for the protection of personal information are much weaker in the US than in Europe, citing the absence of privacy commissions or commissioners in the United States. Personal information is commodified and data can be bought and sold without the consumer's consent or knowledge. While privacy and anonymity are important for individuals and society as a whole, taken to an extreme, they can also prove harmful. A delicate balance exists, which should bring into focus the numerous ethical, technological and control issues associated with the use of personal information in a free society. Too much privacy can protect criminals and destroy communities.

> Without appropriate limitations it can trigger backlash, as citizens engage in unregulated self-help and direct action. The private subversion of public life carries dangers as well as the public intrusion into private life.[86]

CONCLUSION

So where does all this leave us? Certainly without a pat solution, but with hope of better understanding as a prelude to achieving a solution. Moral choices need to be aired and discussed regarding the appropriate use of private information in both the public and private sectors in light of concerns about individual freedom and privacy, and criminal efforts aimed at destroying them. The well-known phenomena of cultural lag, the natural inertia of large organisations and bureaucracies, and the slow and sometimes misdirected political process all stand in the way of needed changes, especially in regard to getting ahead of those who would take advantage of such structural lags, discrepancies and misdirected efforts. Public attitudes must also change to allow the political system to protect citizens and their personal data. The

[85] G T Marx, 'Notes on the Discovery, Collection, and Assessment of Dirty Data', in Joseph W Schneider and John I Kitsuse (eds), *Studies in the Sociology of Social Problems* (1984).

[86] See G T Marx, 'Privacy and Technology', above n 70.

private sector's use of personal data needs better regulation as well, as privacy concerns, the misuse of information, and theft loom large here. All of these are necessary components of a working solution. Any one by itself will not be effective, nor will some without the others.

Technology alone cannot provide the solution to social problems, including identity fraud. In a list of what he terms 'techno-fallacies', Marx provides illustrations of the uncritical use of technology to provide control and order through surveillance. A sampling of those most related to identity fraud include: the fallacy of perfect containment or non-escalation (or the Frankenstein fallacy that technology will *always* remain the solution rather than become the problem); the fallacy of permanent victory; the fallacy of the 100 per cent fail-safe system; the fallacy of assuming that personal information on customers, clients and cases in the possession of a company is just another kind of property to be bought and sold the same as raw materials; and the more general fallacy of rearranging the deck chairs on the Titanic instead of looking for icebergs.[87] Someone needs to be on deck paying attention to the horizon ahead.

[87] Ibid.