CHAPTER

24

Terror, Justice and Freedom

Al-Qaida spent $500,000 on the event, while America, in the incident and its aftermath, lost – according to the lowest estimate – more than $500 billion.

— Osama bin Laden

Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficient . . . The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.

— Supreme Court Justice Louis Brandeis

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

— Benjamin Franklin

24.1 Introduction

The attacks of September 11, 2001, on New York and Washington have had a huge impact on the world of security engineering, and this impact has been deepened by the later attacks on Madrid, London and elsewhere. As everyone has surely realised by now — and as the quote from Osama bin Laden bluntly spells out — modern terrorism works largely by provoking overreaction.

There are many thorny issues. First, there's the political question: are Western societies uniquely vulnerable — because we're open societies with democracy and a free press, whose interaction facilitates fearmongering — and if so what (if anything) should we do about it? The attacks challenged our core values — expressed in the USA as the Constitution, and in Europe as the Convention on Human Rights. Our common heritage of democracy and the rule of law, built slowly and painfully since the eighteenth century, might have

been thought well entrenched, especially after we defended it successfully in the Cold War. Yet the aftermath of 9/11 saw one government after another introducing authoritarian measures ranging from fingerprinting at airports through ID cards and large-scale surveillance to detention without trial and even torture. Scant heed has been given to whether these measures would actually be effective: we saw in Chapter 15 that the US-VISIT fingerprinting program didn't work, and that given the false alarm rate of the underlying technology it could never reasonably have been expected to work. We've not merely compromised our principles; we've wasted billions on bad engineering, and damaged whole industries. Can't we find better ways to defend freedom?

Second, there's the economic question: why are such vast amounts of money spent on security measures of little or no value? America alone has spent over $14 bn on screening airline passengers without catching a single terrorist — and it's rather doubtful that the 9/11 tactics would ever work again, as neither flight crew nor passengers will ever be as passive again (indeed, on 9/11, the tactics only worked for the first 71 minutes). As I noted in Chapter 1, well-known vulnerabilities in screening ground staff, reinforcing cockpit doors and guarding aircraft on the ground overnight have been ignored by the political leadership. Never mind that they could be fixed for a fraction of the cost of passenger screening: invisible measures don't have the political impact and can't compete for budget dollars. So we spend a fortune on measures that annoy passengers but make flying no safer, and according to a Harvard study don't even meet the basic quality standards for other, less-political, screening programs [801]. Is there any way — short of waiting for more attacks — to establish protection priorities more sensibly?

Third, there are the effects on our industry. President Eisenhower warned in his valedictory speech that 'we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military industrial complex. The potential for the disastrous rise of misplaced power exists and will persist'. In the wake of 9/11, we saw a frantic stampede by security vendors, consultancy companies, and intelligence agencies hustling for publicity, money and power. We're seeing the emergence of a security-industrial complex that's capturing policy in the same ways that the defense industry did at the start of the Cold War. One might have thought that technological progress would have a positive effect on trade-offs between freedom and security; that better sensors and smarter processing would shift thr ROC curve towards greater precision. Yet the real-world outcome seems often to be the reverse. How is the civic-minded engineer to deal with this?

Fourth, technical security arguments are often used to bolster the case for bad policy. All though the Irish terrorist campaign, the British police had to charge arrested terrorist suspects within four days. But after 9/11, this was quickly raised to 28 days; then the government said it needed 90 days, claiming they might have difficulty decrypting data on PCs seized from suspects. That

argument turned out to be misleading: the real problem was police inefficiency at managing forensics. Now if the police had just said 'we need to hold suspects for 90 days because we don't have enough Somali interpreters' then common sense could have kicked in; Parliament might well have told them to use staff from commercial translation agencies. But security technology arguments are repeatedly used to bamboozle legislators, and engineers who work for firms with lucrative government contracts may find it difficult to speak out.

Finally, there is the spillover into public policy on topics such as wiretapping, surveillance and export control, that affect security engineers directly, and the corresponding neglect of the more 'civilian' policy issues such as consumer protection and liability. Even before 9/11, governments were struggling to find a role in cyberspace, and not doing a particularly good job of it. The attacks and their aftermath have skewed their efforts in ways that raise pervasive and sometimes quite difficult issues of freedom and justice. Authoritarian behaviour by Western governments also provides an excuse for rules in places from Burma to Zimbabwe to censor communications and spy on their citizens. Now the falling costs of storage may have made increased surveillance inevitable; but the 'war on terror' is exacerbating this and may be catalysing deeper and faster changes that we'd have seen otherwise.

In this chapter, I'm going to look at terrorism, then discuss the directly related questions of surveillance and control, before discussing some other IT policy matters and trying to put the whole in context.

24.2 Terrorism

Political violence is nothing new; anthropologists have found that tribal warfare was endemic among early humans, as indeed it is among chimpanzees [777]. Terror has long been used to cow subject populations — by the Maya, by the Inca, by William the Conqueror. Terrorism of the 'modern' sort goes back centuries: Guy Fawkes tried to blow up Britain's Houses of Parliament in 1605; his successors, the Irish Republican Army, ran a number of campaigns against the UK. In the latest, from 1970–94, some three thousand people died, and the IRA even blew up a hotel where Margaret Thatcher was staying for a party conference, killing several of her colleagues. During the Cold War the Russians supported not just the IRA but the Baader Meinhof Gang in Germany and many others; the West armed and supported partisans from France in World War 2, and jihadists fighting the Soviets in Afghanistan in the 1980s. Some terrorists, like Baader and Meinhof, ended up in jail, while others — such as the IRA leaders Gerry Adams and Martin McGuinness, the Irgun leader Menachim Begin, the French resistance leader Charles de Gaulle and the African anti-colonial leaders Jomo Kenyatta, Robert Mugabe and Nelson Mandela — ended up in office.

What general lessons can be drawn from this history? Well, there's good news and bad news.

24.2.1 Causes of Political Violence

The first piece of good news is that the trend in terrorist violence has been steadily downward [909]. There were many insurgencies in the 1960s and 70s, some ethnic, some anti-colonial, and some ideological. Many were financed by the Soviet Union or its allies as proxy conflicts in the Cold War, although a handful (notably the Nicaraguan Contras and the resistance to the Soviets in Afghanistan) were financed by the West. The end of the Cold War removed the motive and the money.

The second (and related) point is that the causes of civil conflict are mostly economic. An influential study by Paul Collier and Anke Hoeffler for the World Bank looked at wars from 1960-1999 to see whether they were caused largely by grievances (such as high inequality, a lack of political rights, or ethnic and religious divisions), or by greed (some rebellions are more economically viable than others) [315]. The data show convincingly that grievances play little role; the incidence of rebellion was largely determined by whether it could be sustained. (Indeed, Cicero said two thousand years ago that 'Endless money forms the sinews of war'.) Thus the IRA campaign continued largely because of support from the Soviet bloc and from Irish-Americans; when the former vanished and the latter decided that terror was no longer acceptable, the guns were put beyond use. Similarly, the conflict in Sierra Leone was driven by conflict diamonds, the Tamil revolt in Sri Lanka by funds from ethnic Tamils in the USA and India, and Al-Qaida was financed by rich donors in the Gulf states. So the economic analysis gives clear advice on how to deal with an insurgency: cut off their money supply.

24.2.2 The Psychology of Political Violence

Less encouraging findings come from scholars of psychology, politics and the media. I mentioned the affect heuristic in section 2.3.2: where people rely on affect, or emotion, calculations of probability tend to be disregarded. The prospect of a happy event, such as winning the lottery, will blind most people to the long odds and the low expected return; similarly, a dreadful event, such as a terrorist attack, will make most people disregard the fact that such events are exceedingly rare [1189]. Most of the Americans who died as a result of 9/11 did so since then in car crashes, after deciding to drive rather than fly.

There are other effects, too, at the border between psychology and culture. A study of the psychology of terror by Tom Pyszczynski, Sheldon Solomon and Jeff Greenberg looked at how people cope with the fear of death. They got 22 municipal court judges in Tucson, Arizona, to participate in an experiment

in which they were asked to set bail for a drug-addicted prostitute [1053]. They were all given a personality questionnaire first, in which half were asked questions such as 'Please briefly describe the emotions that the thought of your own death arouses in you' to remind them that we all die one day. The judges for whom mortality had become salient set an average bail of $455 while the control group set an average bond of $50 — a huge effect for such an experiment. Further experiments showed that the mortality-salience group had not become mean: they were prepared to give larger rewards to citizens who performed some public act. It turns out that the fear of death makes people adhere more strongly to cultural norms and defend their worldview much more vigorously.

Thinkers have long known that, given the transience of human existence in such a large and strange cosmos, people search for meaning and permanence through religion, through their children, through their creative works, through their tribe and their nation. Different generations of philosophers theorised about this in different languages, from the medieval 'memento mori' through psychonalysis to more recent writings on our need to assuage existential anxiety. Pyszczynski and his colleagues now provide an experimental methodology to study this; it turns out, for example, that mortality salience intensifies altruism and the need for heroes. The 9/11 attacks brought mortality to the forefront of people's minds, and were also an assault on symbols of national and cultural pride. It was natural that the response included religion (the highest level of church attendance since the 1950s), patriotism (in the form of a high approval rating for the President), and intensified bigotry. It was also natural that, as the memory of the attacks receded, society would repolarise because of divergent core values. The analysis can also support constructive suggestions: for example, a future national leader trying to keep a country together following an attack could do well to constantly remind people what they're fighting for. It turns out that, when they're reminded that they'll die one day, both conservatives and liberals take a more polarised view of an anti-American essay written by a foreign student — except in experiments where they are first reminded of the Constitution [1053].

Some countries have taken a bipartisan approach to terrorism — as when Germany faced the Baader-Meinhof Gang, and Britain the IRA. In other countries, politicians have given in to the temptation to use fearmongering to get re-elected. The American political scientist John Mueller has documented the Bush administration's hyping of the terror threat in the campaign against John Kerry [909]; here in the UK we saw Tony Blair proposing the introduction of ID cards, in a move that brilliantly split the opposition Conservative party in the run-up to the 2005 election (the authoritarian Tory leader Michael Howard was in favour, but the libertarian majority in his shadow cabinet forced a U-turn). How can we make sense of a world in which critical decisions, with huge costs and impact, are made on such a basis?

24.2.3 The Role of Political Institutions

In fact, there's a whole academic subject — *public-choice economics* — devoted to explaining why governments act the way they do, and for which its founder James Buchanan won the Nobel Prize in 1986. As he put it in his prize lecture, 'Economists should cease proffering policy advice as if they were employed by a benevolent despot, and they should look to the structure within which political decisions are made'. Much government behaviour is easily explained by the incentives facing individual public-sector decision makers. It's natural for officials to build empires as they are ranked by their span of control rather than, as in industry, by the profits they generate. Similarly, politicians maximise their chances of reelection rather than the abstract welfare of the public. Understanding their decisions requires methodological individualism — considering the incentives facing individual presidents, congressmen, generals, police chiefs and newspaper editors, rather than the potential gains or losses of a nation. We know it's prudent to design institutions so that their leaders' incentives are aligned with its goals — we give company managers stock options to make them act like shareholders. But this is harder in a polity. How is the national interest to be defined?

Public-choice scholars argue that both markets and politics are instruments of exchange. In the former we seek to optimise our utility individually, while in the latter we do the same but using collective actions to achieve goals that we cannot attain in markets because of externalities or other failures. The political process in turn is thus prone to specific types of failure, such as deficit financing. Intergenerational bargaining is hard: it's easy for politicians to borrow money to buy votes now, and leave the bill with the next generation. But then why do some countries have much worse public debt than others? The short answer is that institutions matter. Political results depend critically on the rules that constrain political action.

Although public-choice economics emerged in response to problems in public finance in the 1960s, it has some clear lessons. Constitutions matter, as they set the ground rules of the political game. So do administrative structures, as officials are self-interested agents too. In the UK, for example, the initial response to 9/11 was to increase the budget for the security service; but this hundred million dollars or so didn't offer real pork to the security-industrial complex. So all the pet projects got dusted off, and the political beauty contest was won by a national ID card, a grandiose project that in its original form would have cost £20 billion ($40 billion [809]). Observers of the Washington scene have remarked that a similar dynamic may have been involved in the decision to invade Iraq: although the 2001 invasion of Afghanistan had been successful, it had not given much of a role to the Pentagon barons who'd spent careers assembling fleets of tanks, capital ships and fighter-bombers. Cynics remarked that it didn't give much of a payoff to the defense industry either.

Similar things were said in the aftermath of World War 1, which was blamed on the 'merchants of death'. I suppose we will have to wait for the verdict of the historians.

24.2.4 The Role of the Press

The third locus of concern must surely be the press. 'If it bleeds, it leads', as the saying goes; bad news sells more papers than good. Editors want to sell more papers, so they listen to the scariest versions of the story of the day. For example, in 1997, I got some news coverage when I remarked that British Telecom was spending hundreds of millions more on bug-fixing than its Korean counterpart: was BT wasting money, I asked, or was the infrastructure in middle-income countries at risk? In 1999, after we'd checked out all the university systems, I concluded that although some stuff would break, none of it really mattered. I wrote up a paper and got the University to send out a press release telling people not to worry. There was an almost total lack of interest. There were doomsayers on TV right up till the last midnight of 1999; but 'We're not all going to die' just isn't a story.

The self-interest of media owners combines with that of politicians who want to get re-elected, officials who want to build empires, and vendors who want to sell security stuff. They pick up on, and amplify, the temporary blip in patriotism and the need for heroes that terrorist attacks naturally instil. Fearmongering gets politicians on the front page and helps them control the agenda so that their opponents are always off-balance and following along behind.

24.2.5 The Democratic Response

Is this a counsel of despair? I don't think so: people learn over time. On the 7th July 2005, four suicide bombers killed 52 people on London's public transport and injured about 700. The initial response of the public was one of gritty resignation: 'Oh, well, we knew something like this was going to happen — bad luck if you were there, but life goes on.'[1] The psychological effect on the population was much less than that of the 9/11 bombings on America — which must surely be due to a quarter-century of IRA bombings. Both bombers and fearmongers lose their impact over time.

And as populations learn, so will political elites. John Mueller has written a history of the attitudes to terrorism of successive U.S. administrations [909]. Presidents Kennedy, Johnson, Nixon and Ford ignored terrorism. President

[1]One curious thing was that the press went along with this for a couple of days: then there was an explosion of fearmongering. It seems that ministers needed a day or two of meetings to sort out their shopping lists and decide what they would try to shake out of Parliament.

Carter made a big deal of the Iran hostage crisis, and like 9/11 it gave him a huge boost in the polls at the beginning, but later it ended his presidency. His Secretary of State Cyrus Vance later admitted they should have played down the crisis rather than giving undeserved credibility to the 'students' who'd kidnapped U.S. diplomats. President Reagan mostly ignored provocations, but succumbed to temptation over the Lebanese hostages and shipped arms to Iran to secure their release. However, once he'd distanced himself from this error, his ratings recovered quickly. Now President Bush's fear-based policies have led to serious problems round the world and tumbling popularity; the contenders for the 2008 election all propose policy changes of various kinds. Much the same has happened in the U.K., where Tony Blair's departure from office was met with a great sigh of relief and a rebound in the polls for the ruling Labour Party. His successor Gordon Brown has forbidden ministers to use the phrase 'war on terror'. The message is getting through: fearmongering can bring spectacular short-term political gains, but the voters eventually see through it. And just as this book went to press, in early January 2008, the voters of Iowa selected a Republican candidate who says 'The quickest way to get out of Iraq is to win', and a Democract who promises to end the war in Iraq and be a President 'who understands that 9/11 is not a way to scare up votes but a challenge that should unite America and the world against the common threats of the 21st century'. So it looks like the voters will get their say.

24.3 Surveillance

One of the side-effects of 9/11 has been a huge increase in technical surveillance, both by wiretapping and through the mining of commercial data sources by government agencies. Recent disclosures of unlawful surveillance in a number of countries, together with differing U.S. and European views on privacy, have politicised matters. Wiretapping was already an issue in the 1990s, and millions of words have been written about it. In this section, all I can reasonably try to provide is a helicopter tour: to place the debate in context, sketch what's going on, and provide pointers to primary sources.

24.3.1 The History of Government Wiretapping

Rulers have always tried to control communications. In classical times, couriers were checked at customs posts, and from the Middle Ages, many kings either operated a postal monopoly or granted it to a crony. The letter opening and codebreaking facilities of early modern states, the so-called *Black Chambers*, are described in David Kahn's history [676].

The invention of electronic communications brought forth a defensive response. In most of Europe, the telegraph service was set up as part of the

Post Office and was always owned by the government. Even where it wasn't, regulation was usually so tight that the industry's growth was severely hampered, leaving America with a clear competitive advantage. A profusion of national rules, which sometimes clashed with each other, so exasperated everyone that the *International Telegraph Union* (ITU) was set up in 1865 [1215]. This didn't satisfy everyone. In Britain, the telegraph industry was nationalized by Gladstone in 1869.

The invention of the telephone further increased both government interest in surveillance and resistance to it, both legal and technical. In the USA, the Supreme Court ruled in 1928 in *Olmstead vs United States* that wiretapping didn't violate the fourth amendment provisions on search and seizure as there was no physical breach of a dwelling; Judge Brandeis famously dissented. In 1967, the Court reversed itself in *Katz vs United States*, ruling that the amendment protects people, not places. The following year, Congress legalized Federal wiretapping (in 'title III' of the Omnibus Crime Control and Safe Streets Act) following testimony on the scale of organized crime. In 1978, following an investigation into the Nixon administration's abuses, Congress passed the Federal Intelligence Surveillance Act (FISA), which controls wiretapping for national security. In 1986, the Electronic Communications Protection Act (ECPA) relaxed the Title III warrant provisions. By the early 1990s, the spread of deregulated services from mobile phones to call forwarding had started to undermine the authorities' ability to implement wiretaps, as did technical developments such as out-of-band signaling and adaptive echo cancellation in modems.

So in 1994 the Communications Assistance for Law Enforcement Act (CALEA) required all communications companies to make their networks tappable in ways approved by the FBI. By 1999, over 2,450,000 telephone conversations were legally tapped following 1,350 court orders [434, 851]. The relevant law is 18 USC (U.S. Code) 2510–2521 for telco services, while FISA's regulation of foreign intelligence gathering is now codified in U.S. law as 50 USC 1801–1811 [1272].

Even before 9/11, some serious analysts believed that there were at least as many unauthorized wiretaps as authorized ones [387]. First, there's phone company collusion: while a phone company must give the police access if they present a warrant, in many countries they are also allowed to give access otherwise — and there have been many reports over the years of phone companies being cosy with the government. Second, there's intelligence-agency collusion: if the NSA wants to wiretap an American citizen without a warrant they can get an ally to do it, and return the favour later (it's said that Margaret Thatcher used the Canadian intelligence services to wiretap ministers who were suspected of disloyalty) [496]. Third, in some countries, wiretapping is uncontrolled if one of the subscribers consents — so that calls from phone boxes are free to tap (the owner of the phone box is considered to

be the legal subscriber). Finally, in many countries, the police get hold of email and other stored communications by subpoena rather than warrant (they used to do this in America too before a court stopped the practice in June 2007 [795]).

But even if the official figures had to be doubled or tripled, democratic regimes used wiretapping very much less than authoritarian ones. For example, lawful wiretapping amounted to 63,243 line-days in the USA in 1999, or an average of just over 173 taps in operation on an average day. The former East Germany had some 25,000 telephone taps in place, despite having a fraction of the U.S. population [474]. There was also extensive use of technical surveillance measures such as room bugs and body wires. (It's hardly surprising that nudist resorts became extremely popular in that sad country.)

The incidence of wiretapping was also highly variable within and between democracies. In the USA, for example, only about half the states used it, and for many years the bulk of the taps were in the 'Mafia' states of New York, New Jersey and Florida (though recently, Pennsylvania and California have caught up) [582]. There is similar variation in Europe. Wiretaps are very common in the Netherlands, despite Dutch liberalism on other issues [248]: they have up to 1,000 taps on the go at once with a tenth of America's population. In a homicide investigation, for example, it's routine to tap everyone in the victim's address book for a week to monitor how they react to the news of the death. The developed country with the most wiretaps is Italy, thanks to its tradition of organised crime [794]. In the UK, wiretaps are supposed to need a ministerial warrant, and are rarer; but police use room bugs and similar techniques (including computer exploits) quite a lot in serious cases. To some extent, the technologies are interchangeable: if you can mount a rootkit in a gangster's laptop you can record, and mail home, everything said nearby, whether it's said to someone in the same room, or over a phone.

The cost of wiretapping is an issue. Before CALEA was introduced, in 1993, U.S. police agencies spent only $51.7 million on wiretaps — perhaps a good estimate of their value before the issue became politicised [582]. The implementation of CALEA has supposedly cost over $500 m, even though it doesn't cover ISPs. The FCC has recently (2006–7) extended the CALEA rules to VOIP, which has provoked much grumbling from the industry about the added costs of compliance, loss of some of the flexibility which IP-based services offer, loss of opportunities to innovate, and potential security problems with VOIP services. Certainly it's a lot harder to wiretap VOIP calls: as the critics point out, 'The paradigm of VoIP intercept difficulty is a call between two road warriors who constantly change locations and who, or example, may call from a cafe in Boston to a hotel room in Paris and an hour later from an office in Cambridge to a giftshop at the Louvre' [156]. So how can policymarkers figure out whether it's worth it? If the agencies had to face the full economic costs of wiretapping, would they cut back and spend the money

on more gumshoes instead? Once you start molding an infrastructure to meet requirements other than cost and efficiency, someone has to pay: and as the infrastructure gets more complex, the bills keep on mounting. If other people have to pay them, the incentives are perverted and inefficiency can become structural.

Since 9/11, though, economic arguments about surveillance have been more or less suspended. 43 days after the attacks, Congress passed the Patriot Act, which facilitated electronic surveillance in a number of ways; for example, it allowed increased access by law enforcement to stored records (including financial, medical and government records), 'sneak-and-peek' searches of homes and businesses without the owner's knowledge, and the use by the FBI of National Security Letters to get access to financial, email and telephone records. While access to email is often wiretapping, access to call records is really traffic analysis, which I'll deal with in the next section, and may account for most of the actual volume of interception.

The result has been a steady increase in wiretapping rather than a step change. The 1350 wiretaps authorized by State and Federal courts in 1999 fell to 1190 in 2000, rose to 1491 in 2001, fell to 1358 in 2002, and then rose to 1,442 in 2003, 1,710 in 2004 and 1,773 in 2005. There has been a sharper increase in FISA warrants, from 934 in 2001 to 1228 in 2002, 1724 in 2003 and eventually 2176 in 2006 [435]. This reflects the greater interest in foreign nationals and the Patriot Act's provision that FISA warrants could be used in national-security cases. (These used to be extremely rare: in 1998, for example, only 45 of the FBI's 12,730 convictions involved what the Justice Department classified as internal security or terrorism matters [1259]).

In December 2005, the New York Times revealed that the NSA had been illegally wiretapping people in the U.S. without a warrant. The Administration proposed a rewrite of FISA to legalise this activity, the result was the recently enacted 'Protect America Act', which amends the FISA and sunsets early in 2008. Under this Act, the NSA no longer needs even a FISA warrant to tap a call if one party's believed to be outside the USA or a non-U.S. person. This in effect allowed warrantless surveillance of large numbers of U.S. calls. However, due to the very visible dispute between the President and the Congress over U.S. wiretap law, it's not clear whether and how Congress will revise this when it comes up for renewal. The current action (October 2007) is about granting retrospective immunity to phone companies who cooperated with unlawful wiretapping activities.

24.3.2 The Growing Controversy about Traffic Analysis

However the great bulk of police communications intelligence in developed countries does not come from the surveillance of content, but the analysis of telephone toll records and other communications data. I examined in the

chapter on telecomms security how criminals go to great lengths to bury their signals in innocuous traffic using techniques such as pre-paid mobile phones and PBX hacking; and the techniques used by the police to trace networks of criminal contacts nonetheless.

Again, this is nothing new. Rulers have long used their control over postal services to track the correspondents of suspects, even when the letters weren't opened. The introduction of postage stamps in 1840 was an advance for privacy as it made it much easier to send a letter anonymously. Some countries got so worried about the threat of sedition and libel that they passed laws requiring a return address to be written on the back of the envelope. The development of the telegraph, on the other hand, was an advance for surveillance; as messages were logged by sender, receiver and word count, traffic totals could be compiled and were found to be an effective indicator of economic activity [1215]. The First World War brought home to the combatants the value of the intelligence that could be gleaned from listening to the volume of enemy radio traffic, even when it couldn't conveniently be deciphered [676, 923]. Later conflicts reinforced this.

Traffic analysis continues to provide the bulk of police communications intelligence. For example, in the USA, there were 1,329 wiretap applications approved in 1998 (the last year for which comparable statistics were available when I wrote the first edition of this book) while there were 4886 subpoenas (plus 4621 extensions) for *pen registers* (devices which record all the numbers dialed from a particular phone line) and 2437 subpoenas (plus 2770 extensions) for *trap-and-trace* devices (which record the calling line ID of incoming calls, even if the caller tries to block it). In other words, there were more than ten times as many warrants for communications data as for content. What's more, these data were even more incomplete than for wiretapping. The trend in recent years — even before 9/11 — was to switch to using subpoenas for the call-detail records in the phone companies' databases, rather than getting pen-register data directly from the switch (a move facilitated by CALEA). Bell Atlantic, for example, indicated that for the years 1989 through 1992, it had responded to 25,453 subpoenas or court orders for toll billing records of 213,821 of its customers, while NYNEX reported that it had processed 25,510 subpoenas covering an unrecorded number of customers in 1992 alone [279]. Scaled up across the country, this suggests perhaps half a million customers are having their records seized every year, and that traffic data are collected on perhaps a hundred times as many people as are subjected to wiretapping. Statistics have become much more patchy and sporadic since 9/11, but there's no reason to believe that traffic data have become less important: they have been more important for years, and across many countries. (Indeed, recently we're getting indications of further qualitative increases in traffic surveillance, which I'll discuss below.) Why should this be?

Wiretaps are so expensive to listen to and transcribe that most police forces use them only as a weapon of last resort. In contrast, the numbers a suspect calls, and that call him, give a rapid overview of his pattern of contacts. Also, while wiretaps usually have fairly strict warrantry requirements, most countries impose little or no restrictions on the police use of communications data. In the USA, no paperwork was required until ECPA. Even after that, they have been easy to get: under 18 USC 3123 [1272], the investigative officer merely had to certify to a magistrate 'that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation'. This can be any crime — felony or misdemeanour — and under either Federal or State law. Unlike with wiretaps, the court has no power to deny a subpoena once a formally correct application has been made, and there is no court supervision once the order has been granted. Since the passage of CALEA, warrants are still required for such communications data as the addresses to which a subscriber has sent e-mail messages, but basic toll records could be obtained under subpoena — and the subscriber need not be notified.

The most controversial current issue may be access to multiple generations of call data and indeed to whole phone-company databases. In section 19.3.1, I described the snowball search, in which the investigator not only looks at who the target calls, but who they call, and so on recursively, accumulating n-th generation contacts like a snowball rolling downhill, and then eventually sifting the snowball for known suspects or suspicious patterns. If a pen-register, trap-and-trace, or call-detail subpoena is needed for every node in the search, the administrative costs mount up. There were thus rumours in many countries for years that the phone companies simply give the intelligence services access to (or even copies of) their databases.

24.3.3 Unlawful Surveillance

In 2006, it emerged that the rumours were correct. AT&T had indeed given the NSA the call records of millions of Americans; the agency's goal is 'to create a database of every call ever made within the nation's borders' so it can map the entire U.S. social network for the War on Terror [277]. Apparently this data has now been collected for the 200 m customers of AT&T, Verizon and BellSouth, the nation's three biggest phone companies. The program started just after 9/11. Qwest did not cooperate, because its CEO at the time, Joe Nacchio, did not believe the NSA's claim that Qwest didn't need a court order (or approval under FISA). The NSA put pressure on Qwest by threatening to withhold classified contracts, and Qwest's lawyers asked NSA to take its proposal to the FISA court. The NSA refused, saying the court might not agree with them. It's since emerged that the NSA had put pressure on Qwest to hand over data even before 9/11 [528]. In October 2007, further confirmation was obtained by Democrat senators when Verizon admitted to them that it had given the FBI

second-generation call data on its customers against national security letters on 720 occasions since 2005 [925]; and in November 2007, the Washington Post revealed that the NSA had tapped a lot of purely domestic phone calls and traffic data, and had also tapped AT&T's peering centre in San Francisco to get access to Internet traffic as well [926].

Both phone and computer service records can be provided to bodies other than law enforcement agencies under 18 USC 2703(c); thus, for example, we find Virginia and Maryland planning to use mobile phone tracking data to monitor congestion on the Capital Beltway [1179]. Toll data use for marketing purposes was also expressly envisioned by Congress when this law was passed. However, the growing availability of mobile phone records has now made them available to criminals too, enabling gangsters to track targets and find out if any of their colleagues have been calling the police [830].

In the UK, files of telephone toll tickets were provided to the police without any control whatsoever until European law forced the government to regulate the practice in the Regulation of Investigatory Powers Act in 2000. It was long rumoured that the large phone companies gave the spooks copies of their itemised billing databases as a matter of course. Since then, communications data requires only a notice from a senior police officer to the phone company or ISP, not a warrant; and data can be provided to a wide range of public-sector bodies, just as in the USA. (There was a public outcry when the Government published regulations under the Act, which made clear that your mobile phone records could be seized by anyone from your parish council to the Egg Marketing Board.)

24.3.4 Access to Search Terms and Location Data

One problem is that communications data and content are becoming intermixed, as what's content at one level of abstraction is often communications data at the next. People might think of a URL is just the address of a page to be fetched, but a URL such as `http://www.google.com/search?q=marijuana+cultivation+UK` contains the terms entered into a search engine as well as the search engine's name. Clearly some policemen would like a list of everyone who submitted such an enquiry. Equally clearly, giving this sort of data to the police on a large scale would have a chilling effect on online discourse.

In the USA, the Department of Justice issued a subpoena to a number of search engines to hand over two full months' worth of search queries, as well as all the URLs in their index, claiming it needed the data to bolster its claims that the Child Online Protection Act did not violate the constitution and that filtering could be effective against child pornography. (Recall we discussed in section 9.3.1 how when AOL released some search histories, a number of them were easily identifiable to individuals.) AOL, Microsoft and Yahoo quietly complied, but Google resisted. A judge ruled that the Department would get

no search queries, and only a random sample of 50,000 of the URLs it had originally sought [1353].

In the UK, the government tried to define URLs as traffic data when it was pushing the RIP bill through parliament, and the news that the police would have unrestricted access to the URLs each user enters — their *click-stream* — caused a public outcry against 'Big Browser', and the definition of communications data was trimmed. For general Internet traffic, it means IP addresses, but it also includes email addresses. All this can be demanded with only a notice from a senior policeman.

More subtleties arise with the phone system. In Britain, all information about the location of mobile phones counts as traffic data, and officials get it easily; but in the USA, the Court of Appeals ruled in 2000 that when the police get a warrant for the location of a mobile, the cell in which it is active is sufficient, and that to require triangulation on the device (an interpretation the police had wanted) would invade privacy [1273]. Also, even cell-granularity location information would not be available under the lower standards applied to pen-register subpoenas. Subpoenas were also found insufficient for *post-cut-through* dialed digits as there is no way to distinguish in advance from digits dialed to route calls and digits dialed to access or give information. What this means in practice is that if a target goes down a 7−11 store and buys a phone card for a few dollars, the police can't get a list of who he calls without a full wiretap warrant. All they can get by subpoena are the digits he dials to contact the phone card operator, not the digits he dials afterwards to be connected.

24.3.5 Data Mining

The analysis of call data is only one aspect of a much wider issue: law enforcement *data matching*, namely the processing of data from numerous sources. The earliest serious use of multiple source data appears to have been in Germany in the late 1970s to track down safe houses used by the Baader Meinhof terrorist group. Investigators looked for rented apartments with irregular peaks in utility usage, and for which the rent and electricity bills were paid by remote credit transfer from a series of different locations. This worked: it yielded a list of several hundred apartments among which were several safe houses. The tools to do this kind of analysis are now shipped with a number of the products used for traffic analysis and for the management of major police investigations. The extent to which they're used depends on the local regulatory climate; there have been rows in the UK over police access to databases of the prescriptions filled by pharmacists, while in the USA doctors are alarmed at the frequency with which personal health information is subpoenaed from health insurance companies by investigators. There are also practical limits imposed by the cost of understanding the many proprietary data formats used by commercial and government data processors. But it's

common for police to have access at least to utility data, such as electricity bills which get trawled to find marijuana growers.

However, there are many indications that the combination of more aggressive searches and mounting data volumes are making data-mining operations since 9/11 less productive. Terrorists are just so rare as a percentage of the population that any tests you use to 'detect' them would require extraordinary sensitivity if you're not to drown in false positives. Adding more data doesn't necessarily help; as I explained in section 15.9, combining multiple sensors is hard and you're unlikely to improve both the false positive and false negative error rates at the same time. Simply put, if you're looking for a needle in a haystack, the last thing you need to do is to build a bigger haystack. As Jeff Jonas, the chief scientist at IBM's data-mining operation, put it, 'techniques that look at people's behavior to predict terrorist intent are so far from reaching the level of accuracy that's necessary that I see them as nothing but civil liberty infringement engines' [519].

Finally, policemen (and even divorce lawyers) are increasingly using subpoenas to get hold of email from service providers once the recipient has read it. The legal reasoning is that whereas it takes an interception warrant to get the postman to hand over physical mail, a simple search warrant will do once the letter lands on your doormat; and so although a proper warrant is needed to seize email on its way through an ISP to you, once it's sitting in your mail folder at AOL or Google it's just stored data. You might think it prudent to use a mail service provider that deletes mail once you've read it; but in the UK at least, a court found that police who ordered an ISP to preserve email that they'd normally overwritten were acting lawfully [974], and in March 2006 the European Union adopted a Directive compelling Member States to enact laws compelling communication services to retain traffic data for between six months and two years. It's unclear how many ISPs will go to the trouble of deleting email contents; if they have to retain the headers anyway, they might as well keep the lot. And in the long term, absolutely anything that gets monitored and logged is potentially liable to be subpoenaed.

24.3.6 Surveillance via ISPs – Carnivore and its Offspring

One big recent development is intrusive surveillance at Internet Service Providers (ISPs). Tapping data traffic is harder than voice used to be; there are many obstacles, such as transient IP addresses given to most customers and the increasingly distributed nature of traffic. In the old days (say 2002), an ISP might have had modem racks, and a LAN where a wiretap device could be located; nowadays many customers come in via DSL, and providers use switched networks that often don't have any obvious place to put a tap.

Many countries have laws requiring ISPs to facilitate wiretapping, and the usual way to do it at a large ISP is to have equipment already installed that will split a target network so that copies of packets of interest go to a separate classified network with wiretap equipment. Small ISPs tend not to have such facilities. In the late 1990s, the FBI developed a system called Carnivore that they could lug around to smaller ISPs when a wiretap was needed; it was a PC with software that could be configured to record a suspect's email, or web browsing, or whatever traffic a warrant or subpoena specified. It became controversial in 2000 when an ISP challenged it in court; it was being used to record email headers as traffic data, without a wiretap warrant. Congress legalized this practice in the Patriot Act in 2001, and in about 2002 Carnivore was retired in favour of more modern equipment. We have recent FOI revelations about the FBI's current wiretapping network, DCSNet, which is very slick –allowing agents remote and near-instantaneous access to traffic and content from participating phone companies [1178].

Access by the police and intelligence services to ISPs is patchy for a number of reasons. No-one bothers about small ISPs, but they can grow quickly; large ISPs' systems can be hard to integrate with law-enforcement kit, and the project can remain stuck in the development backlog for years as it brings no revenue; ISPs coming into contact with the world of surveillance for the first time they usually don't have cleared staff to operate government equipment; and the wiretap equipment is very often poorly engineered [1151]. As a result, it's often not practical for the police to tap particular ISPs for months or even years on end, and the information about which providers are wiretap-resistant is rather closely held. (Smart bad guys still use small ISPs.) In addition, it is often difficult for the authorities to get IP traffic data without a full wiretap warrant; for assorted technical reasons, all the traffic data that it's usually convenient to provide against a subpoena are extracts from those logs that the ISP keeps anyway. And things often go wrong because the police don't understand ISPs; they subpoena the wrong things, or provide inaccurate timestamps so that the wrong user is associated with an IP address. For an analysis of failure modes, see Clayton [300].

24.3.7 Communications Intelligence on Foreign Targets

I discussed the technical aspects of signals intelligence in Chapter 19; now let's look briefly at the political and organizational aspects.

The bulk of communications intelligence, whether involving wiretaps, traffic analysis or other techniques, is not conducted for law enforcement purposes but for foreign intelligence. In the U.S. the main agency responsible for this is the National Security Agency, which has huge facilities and tens of thousands of employees. While law enforcement agencies have 150–200 active wiretaps at any one time, the NSA utterly dwarfs this. The situation is similar in other

countries; Britain's Government Communications Headquarters (GCHQ) has thousands of employees and a budget of about a billion dollars, while for many years one single police officer at New Scotland Yard handled the administration of all the police wiretaps in London (and did other things too).

Information has steadily trickled out about the scale and effectiveness of modern signals intelligence operations. David Kahn's influential history of cryptography laid the groundwork by describing much of what happened up till the start of World War Two [676]; an anonymous former NSA analyst, later identified as Perry Fellwock, revealed the scale of NSA operations in 1972 [462]. 'Information gathering by NSA is complete', he wrote. 'It covers what foreign governments are doing, planning to do, have done in the past: what armies are moving where and against whom; what air forces are moving where, and what their capabilities are. There really aren't any limits on NSA. Its mission goes all the way from calling in the B-52s in Vietnam to monitoring every aspect of the Soviet space program'.

While Fellwock's motive was opposition to Vietnam, the next major whistleblower was a British wartime codebreaker, Frederick Winterbotham, who wanted to write a memoir of his wartime achievements and, as he was dying, was not bothered about prosecution. In 1974, he revealed the Allies' success in breaking German and Japanese cipher systems during that war [1350], which led to many further books on World War 2 sigint [296, 677, 1336]. Thereafter there was a slow drip of revelations by investigative journalists, quite of few of whose sources were concerned about corruption or abuse of the facilities by officials monitoring targets they should not have, such as domestic political groups. For example, whistleblower Peg Newsham revealed that the NSA had illegally tapped a phone call made by Senator Strom Thurmond [258, 259]. James Bamford pieced together a fair amount of information on the NSA from open sources and by talking to former employees [112], while the most substantial recent source on the organization and methods of U.S. and allied signals intelligence was put together by New Zealand journalist Nicky Hager [576] following the New Zealand intelligence community's failure to obey an order from their Prime Minister to downgrade intelligence cooperation with the USA.

The end of the Cold War forced the agencies to find new reasons to justify their budgets, and a common theme was developing economic intelligence operations against competitor countries. This accelerated the flow of information about sources and methods. The most high-profile exposé of US economic espionage was made in a 1999 report to the European parliament [443], which was concerned that after the collapse of the USSR, European Union member nations were becoming the NSA's main targets [262].

The picture that emerged from these sources was of a worldwide signals intelligence collection system, *Echelon*, run jointly by the USA, the UK, Canada, Australia and New Zealand. Data, faxes and phone calls get collected at a large number of nodes which range from international communications cables that

land in member countries (or are tapped clandestinely underwater), through observation of traffic to and from commercial communications satellites and special sigint satellites that collect traffic over hostile countries, to listening posts in member states' embassies [443]. The collected traffic is searched in real time by computers known as *dictionaries* according to criteria such as the phone numbers or IP addresses of the sender or receiver, plus keyword search on the contents of email. These search criteria are entered by member countries' intelligence analysts; the dictionaries then collect traffic satisfying them and ship them back to the analyst. Echelon appears to work very much like Google, except that instead of searching web pages it searches through the world's phone and data network traffic in real time.

24.3.8 Intelligence Strengths and Weaknesses

Echelon seems impressive — if scary. But several points are worth bearing in mind.

First, the network built up by the NSA and its allies was mainly aimed at the old USSR, where human intelligence was difficult, and hoovering up vast quantities of phone calls gave at least some idea of what was going on. But the resulting political and economic intelligence turned out to be poor; the West thought that Russia's economy was about twice as large as it actually was, and was surprised by its collapse post-1989. (The agencies' incentives to talk up the threat are clear.) In any case, much of the effort was military, aimed at understanding Soviet radar and communications, and at gaining a decisive advantage in location, jamming and deception. Without an ability to conduct electronic warfare, a modern state is not competitive in air or naval warfare or in tank battles on the ground. So it's not surprising that most of the personnel at NSA are military, and its director has always been a serving general. There is still a lot of effort put into understanding the signals of potential adversaries.

Second, there have been some successes against terrorists — notably the arrest of the alleged 9/11 mastermind Khalid Shaikh Mohammed after he used a mobile phone SIM from a batch bought by a known terrorist in Switzerland. But electronic warfare against insurgents in Iraq has proved to be unproductive, as I discussed in Chapter 19. And it's long been clear that much more effort should have been put into human intelligence. In an article published just before 9/11, an analyst wrote 'The CIA probably doesn't have a single truly qualified Arabic-speaking officer of Middle Eastern background who can play a believable Muslim fundamentalist who would volunteer to spend years of his life with shitty food and no women in the mountains of Afghanistan. For Christ's sake, most case officers live in the suburbs of Virginia. We don't do that kind of thing'. Another put it even more bluntly: 'Operations that include diarrhea as a way of life don't happen' [521]. The combination of stand-off technical intelligence plus massive firepower suits

the private interests of bureaucrats and equipment vendors, but it makes allied forces ineffective at counterinsurgency, where the enemy blends with the civilian population. Similar perverse incentive hamper the military. For example, Britain is spending billions on two new aircraft carriers and on modernising the nuclear deterrent, but even six years after 9/11 we haven't trained enough soldiers to carry a basic conversation in Arabic. The big debate now brewing in the Pentagon is not just about intelligence, but how to evolve a smarter approach to counterinsurgency across the board [414].

Third, while the proliferation of mobile phones, wireless LANs and online services presents the agencies with a cornucopia of new information sources, the volume is a huge problem. Even with a budget of billions of dollars a year and tens of thousands of staff, not even the NSA can collect all the electronic communications everywhere in the world. The days in which they could record all transatlantic phone calls with a rack of 16-track tape recorders are no more. Equipment for tapping high-speed backbone links does exist [167], but it's expensive. Sprint's budget is bigger than the NSA's, and is spent on low-cost commercial products rather than high-cost classified ones, so they can put in lines much faster than the NSA can tap them. Data volumes force most traffic selection to be done locally, and in real time [770]. Suppose, for example, that the NSA got interested in the UK university system — let's call it a hundred institutions at 2 Gbit/sec each. They couldn't ship all the bits across the Atlantic to Fort Meade as there just isn't enough transatlantic bandwidth. Tapping all the data streams of all the corporations in Japan would be an order of magnitude harder.

Fourth, although other countries may complain about U.S. sigint collection, for them to moralize about it is hypocritical. Other countries also run intelligence operations, and are often much more aggressive in conducting economic and other non-military espionage. The real difference between the WASP countries and the others is that no-one else has built the Echelon 'system-of-systems'. Indeed, there may be network effects at work in sigint as elsewhere: the value of a network grows faster than its size, and the more you tap, the cheaper it gets. There have thus been moves to construct a 'European Echelon' involving the police and intelligence agencies of continental European countries [430, 445].

The mature view, I think, is that signals intelligence is necessary for a nation's survival but potentially dangerous — just like the armed forces it serves. An army can be a good servant but is likely to be an intolerable master. The issue is not whether such resources should exist, but how they are held accountable. In the USA, hearings by Senator Church in 1975 detailed a number of abuses such as the illegal monitoring of U.S. citizens [292]. Foreign intelligence gathering is now regulated by U.S. law in the form of 50 USC 1801–1811 [1272], which codifies FISA. This isn't perfect; as already noted, it's the subject of fierce tussles between the executive and the legislature about

the recent provision that the NSA can wiretap U.S. calls so long as one of the parties is believed not to be a U.S. person. Even before this, the number of FISA warrants has risen steadily since 9/11 to exceed the number of ordinary (title III) wiretap warrants. But at least Congress has got interested. And the USA is lucky: in most countries, the oversight of intelligence isn't even discussed.

Finally, poor accountability costs more than just erosion of liberty and occasional political abuse. There is a also real operational cost in the proliferation of intelligence bureaucracies that turn out to be largely useless once the shooting starts. In Washington during the Cold War, the agencies hated each other much more than they hated the Russians. In the UK, one of the most vicious intelligence battles was not against the IRA, but between the police and MI5 over who would be the lead in the fight against the IRA. There are numerous accounts of intelligence inefficiency and infighting by well-placed insiders, such as R.V. Jones [671]. It is in this context of bureaucratic turf wars that I'll now describe the 'Crypto Wars' of the 1990s, which were a formative experience for many governments (and NGOs) on issues of surveillance and technology policy.

24.3.9 The Crypto Wars

Technology policy during the 1990s was dominated by acrimonious debates about *key escrow* — the doctrine that anyone who encrypted data should give the government a copy of the key, so that the civilian use of cryptography would not interfere with intelligence gathering by the NSA and others.

Although some restrictions on cryptography had existed for years and irritated both academic researchers and civilian users, they shot to the headlines in 1993 when President Clinton astonished the IT industry with the *Escrowed Encryption Standard*, more popularly known as the *Clipper chip*. This was a proposed replacement for DES, with a built-in back door key so that government agencies could decipher any traffic. The NSA had tried to sell the program to the cabinet of President Bush senior and failed; but the new administration was happy to help.

American opinion polarized. The government argued that since cryptography is about keeping messages secret, it could be used by criminals to prevent the police gathering evidence from wiretaps; the IT industry (with a few exceptions) took the conflicting view that cryptography was the only means of protecting electronic commerce and was thus vital to the future development of the net. Civil liberties groups lined up with the industry, and claimed that cryptography would be the critical technology for privacy. By 1994, the NSA had concluded that they faced a war with Microsoft that Bill would win, so they handed off the policy lead to the FBI while continuing to direct matters from behind the scenes.

The debate got rapidly tangled up with export controls on weapons, the means by which cryptography was traditionally controlled. U.S. software firms were not allowed to export products containing cryptography which was too hard to break (usually meaning a keylength of over 40 bits). A U.S. software author, Phil Zimmermann, was hauled up before a grand jury for arms trafficking after a program he wrote — PGP — 'escaped' on to the Internet. He immediately became a folk hero and made a fortune as his product grabbed market leadership. The conflict became international: the U.S. State Department tried hard to persuade other countries to control cryptography too. It became one of the personal missions of Vice-President Gore (a reason why many in Redmond and the Valley contributed to the Bush campaign in 2000).

The results were mixed. Some countries with memories of oppressive regimes, such as Germany and Japan, resisted American blandishments. Others, such as Russia, seized the excuse to pass harsh crypto control laws. France thumbed its nose by relaxing a traditional prohibition on non-government use of crypto; Britain obediently changed from a liberal, laissez-faire policy under John Major in the mid 1990s to a draconian law under Tony Blair. The *Regulation of Investigatory Powers* (RIP) Act of 2000 enables the police to demand that I hand over a key or password in my possession, and the Export Control Act of 2002 instructs me to get an export license if I send any cryptographic software outside Europe that uses keys longer than 56 bits. Oh, and the government has also taken powers to vet foreign research students studying dangerous subjects like computer science, and to refuse visas to those they consider a proliferation risk.

I was involved in all this as one of the academics whose research and teaching was under threat from the proposed controls, and in 1998 I was one of the people who set up the Foundation for Information Policy Research, the UK's leading internet-policy think-tank, which wrestled with crypto policy, export policy, copyright and related issues. In the next few sections I'll lay out a brief background to the crypto wars, and then describe the consequences for export controls today, and for what we can learn about the way governments have failed to get to grips with the Internet.

24.3.9.1 The Back Story to Crypto Policy

Many countries made laws in the mid-19th century banning the use of cryptography in telegraph messages, and some even forbade the use of languages other than those on an approved list. Prussia went as far as to require telegraph operators to keep copies of the plaintext of all messages [1215]. Sometimes the excuse was law enforcement — preventing people obtaining horse race results or stock prices in advance of the 'official' transmissions — but the real concern

was national security. This pattern was to repeat itself again in the twentieth century.

After the immense success that the Allies had during World War 2 with cryptanalysis and signals intelligence in general, the UK and US governments agreed in 1957 to continue intelligence cooperation. This is known as the UKUSA agreement, although Canada, Australia and New Zealand quickly joined. The member nations operated a crypto policy whose main goal was to prevent the proliferation of cryptographic equipment and know-how. Until the 1980s, about the only makers of cryptographic equipment were companies selling into government markets. They could mostly be trusted not to sell anything overseas which would upset their major customers at home. This was reinforced by export controls which were operated 'in as covert a way as possible, with the minimum of open guidance to anyone wanting, for example, an export licence. Most things were done in behind-the-scenes negotiation between the officials and a trusted representative of the would-be exporter'. [142]

In these negotiations, the authorities would try to steer applicants towards using weak cryptography where possible, and where confronted with a more sophisticated user would try to see to it that systems had a 'back door' (known in the trade as a *red thread*) which would give access to traffic. Anyone who tried to sell decent crypto domestically could be dissuaded by various means. If they were a large company, they would be threatened with loss of government contracts; if a small one, they could be strangled with red tape as they tried to get telecomms and other product approvals.

The 'nonproliferation' controls were much wider than cryptography, as computers also fell within their scope. By the mid-1980s, the home computers kids had in their bedrooms were considered to be munitions, and manufacturers ended up doing lots of paperwork for export orders. This pleased the bureaucrats as it gave them jobs and power. The power was often abused: in one case, an export order for a large number of British-made home computers to the school system in Yugoslavia was blocked at the insistence of the U.S. authorities, on the grounds that it contained a U.S. microprocessor; a U.S. firm was promptly granted a license to export into this market. Although incidents like this brought the system into disrepute, it persists to this day.

Crypto policy was run in these years along the same lines as controls on missile technology exports: to let just enough out to prevent companies in other countries developing viable markets. Whenever crypto controls got so onerous that banks in somewhere like Brazil or South Africa started having crypto equipment custom built by local electronics firms, export licensing would ease up until the threat had passed. And, as I described in the chapter on API security, the hardware security modules sold to banks throughout this

period had such poor interface designs that compromising them was trivial anyway.

Vulnerabilities in bank crypto merely increased the risk of fraud slightly, but bad crypto elsewhere exposed its users to surveillance. The Swedish government got upset when they learned that the 'export version' of Lotus Notes which they used widely in public service had its cryptography deliberately weakened to allow NSA access; and at least one (U.S. export approved) cipher machine has broadcast its plaintext in the clear in the VHF band. But the most notorious example was the Bühler case.

Hans Bühler worked as a salesman for the Swiss firm Crypto AG, which was a leading supplier of cryptographic equipment to governments without the technical capability to build their own. He was arrested in 1992 in Iran and the authorities accused him of selling them cipher machines which had been tampered with so that the NSA could get at the plaintext. After he had spent some time in prison, Crypto AG paid 1.44 billion Rials — about a million U.S. dollars — to bail him, but then fired him once he got back to Switzerland. Bühler then alleged on Swiss radio and TV that the firm was secretly controlled by the German intelligence services and that it had been involved in intelligence work for years [238]. The interpretation commonly put on this was that ultimate control resided with the NSA (the founder of Crypto, Boris Hagelin, had been a lifelong friend of William Friedman, the NSA's chief scientist) and that equipment was routinely red threaded [824]. A competing interpretation is that these allegations were concocted by the NSA to undermine the company, as it was of the third world's few sources of cryptographic equipment. Bühler's story is told in [1228].

24.3.9.2 DES and Crypto Research

Despite the very poor implementation quality of early banking cryptosystems, the NSA still worried in the seventies that the banking sector might evolve good algorithms that would escape into the wild. Many countries were still using rotor machines or other equipment that could be broken using the techniques developed in World War 2. How could the banking industry's thirst for a respectable cipher be slaked, not just in the U.S. but overseas, without this cipher being adopted by foreign governments and thus adding to the costs of intelligence collection?

The solution was the Data Encryption Standard (DES). At the time, as I mentioned in section 5.4.3.2, there was controversy about whether 56 bits were enough. We now know that this was deliberate. The NSA did not at the time have the machinery to do DES keysearch; that came later. But by giving the impression that they did, they managed to stop most foreign governments adopting it. The rotor machines continued in service, in many cases reimplemented using microcontrollers, and the traffic continued to be

harvested. Foreigners who encrypted their important data with such ciphers merely solved the NSA's traffic selection problem.

A second initiative was to undermine academic research in cryptology. In the 1970s this was done directly by harassing the people involved; by the 1980s it had evolved into the subtler strategy of claiming that published research work was all old hat. The agencies opposed crypto research funding by saying 'we did all that stuff thirty years ago; why should the taxpayer pay for it twice?' The insinuation that DES may have had a 'trapdoor' inserted into it fitted well with this play. A side effect we still live with is that the crypto and computer security communities got separated from each other in the early 1980s as the NSA worked to suppress one and build up the other.

By the mid 1990s this line had become exhausted. Agency blunders in the design of various key escrow systems showed that they have no special expertise in cryptology compared with the open research community, and as attempts to influence the direction of academic research by interfering with funding have become less effective they have become much less common.

24.3.9.3 The Clipper Chip

Crypto policy came into the open in 1993 with the launch of the Clipper chip. The immediate stimulus was the proposed introduction by AT&T to the U.S. domestic market of a high-grade encrypting telephone that would have used Diffie-Hellman key exchange and triple-DES to protect traffic. The NSA thought that the government could use its huge buying power to ensure the success of a different standard in which spare keys would be available to the agencies to decrypt traffic. This led to a public outcry; an AT&T computer scientist, Matt Blaze, found a protocol vulnerability in Clipper [183] and the proposal was withdrawn.

Several more attempts were made to promote the use of cryptography with government access to keys in various guises. Key escrow acquired various new names, such as *key recovery*; certification authorities which kept copies of their clients' private decryption keys became known as *Trusted Third Parties* (TTPs) — somewhat emphasising the NSA definition of a trusted component as one which can break security. In the UK, a key escrow protocol was introduced for the public sector, and this was used to try to get the private sector to adopt it to; but a number of vulnerabilities were found in it too [76].

Much of the real policy leverage had to do with export licensing. As the typical U.S. software firm exports most of its product, and as maintaining a separate product line for export is expensive, many firms could be dissuaded from offering strong cryptography by prohibiting its export. Products with 'approved' key escrow functionality were then granted preferential U.S. export license treatment. The history of this struggle is still to be fully written, but

a first draft is available from Diffie and Landau [387] and many of the U.S. source documents, obtained under FOIA, have been published in [1135].

One of the engineering lessons from this whole process is that doing key escrow properly is hard. Making two-party security protocols into three-party protocols increases the complexity and the risk of serious design errors, and centralizing the escrow databases creates huge targets [4]. Where escrow is required it's usually better done with simple local mechanisms. In one army, the elegant solution is that every officer must write down his passphrase on a piece of paper, put it into an envelope, stamp it 'Secret' and hand it to his commanding officer, who puts it in his office safe. That way the keys are kept in the same place as the documents whose electronic versions they protect, and there's no central database for an airplane to bomb or a spy to steal.

24.3.10 Did the Crypto Wars Matter?

When the key escrow debate got going in the UK in 1994–5, I took a line that was unpopular at the time with both the pro-escrow and the anti-escrow lobbies. The pro-escrow people said that as crypto provided confidentiality, and confidentiality could help criminals, there needed to be some way to defeat it. The anti-escrow lobby said that since crypto was necessary for privacy, there must not be a way to defeat it. I argued in [35] that essentially all the premises behind these arguments were wrong. Most crypto applications (in the real world, as opposed to academia) are about authentication rather than confidentiality; they help the police rather than hindering them. As for criminals, they require unobtrusive communications — and encrypting a phone call is a good way to bring yourself to the attention of the agencies. As for privacy, most violations result from abuse of authorized access by insiders. Finally, a much more severe problem for policemen investigating electronic crimes is to find acceptable evidence, for which decent authentication can be helpful.

This is not to say that the police have no use for wiretaps. Although many police forces get by quite happily without them, and many of the figures put forward by the pro-wiretap lobby are dishonest [387], there are some occasions where wiretapping can be economic as an investigative tool. The Walsh report — by a senior Australian intelligence officer — gives a reasonably balanced examination of the issues [1311]. Walsh compared the operational merits of wiretaps, bugs and physical surveillance, and pointed out that wiretaps were either the cheapest or the only investigative technique in some circumstances. He nonetheless found that there is 'no compelling reason or virtue to move early on regulation or legislation concerning cryptography', but he did recommend that police and intelligence agencies be allowed to

hack into target computers to obtain access or evidence[2]. It took the view that although there will be some policing costs associated with technological advances, there will also be opportunities: for example, to infect a suspect's computer with software that will turn it into a listening device. This hit the nail on the head. The police — like the intelligence services — are reaping a rich harvest from modern technology.

We all knew, of course, that the police forces who argued in favour of key escrow did so under orders and as a front for the spooks[3]. Now the aims and objectives of policemen and spies are not quite identical, and confusing them has clouded matters. It is perhaps an oversimplification that the former try to prevent crimes at home, while the latter try to commit them abroad; but such aphorisms bring out some of the underlying tension. For example, policemen want to preserve evidence while spies like to be able to forge or repudiate documents at will. During the discussions on a European policy toward key escrow ('Euroclipper') that led up to the Electronic Signature Directive, the German government demanded that only confidentiality keys should be escrowed, not signature keys; while Britain wanted signature keys to be escrowed as well. The British view followed the military doctrine that deception is at least as important as eavesdropping, while the Germans supported the police doctrine of avoiding investigative techniques that undermine the value of any evidence subsequently seized.

The key goal of the intelligence community in the 1990s, as we later learned, was to minimise the number of systems that used crypto by default. If a significant proportion of data traffic were encrypted, then the automated keyword searching done by systems such as Echelon would be largely frustrated. The NSA was quite aware that many new network systems were being built rapidly during the dotcom boom, and if cryptography wasn't built in at the start, it should usually be too expensive to retrofit it later. So each year the NSA held the line on crypto controls meant dozens of systems open to surveillance for decades in the future. In these terms, the policy was successful: little of the world's network traffic is encrypted, the main exceptions being DRM-protected content, Skype, the few web pages that are protected by TSL, opportunistic TLS encryption between mail servers, SSH traffic, corporate VPNs and online computer games. Everything else is pretty much open to interception — including masses of highly sensitive email between companies.

[2]The Walsh report has an interesting publishing history. Originally released in 1997 as an unclassified document, it was withdrawn three weeks later after people asked why it wasn't yet on sale in the shops. It was then republished in redacted form. Then researchers found unexpurgated copies in a number of libraries. So these were published on the web, and the redacted parts drew attention at once to the issues the government considered sensitive. As late as 1999, the Australian government was still trying to suppress the report [1311].

[3]This was admitted in an unguarded moment in 1996 by the UK representative on the European body responsible for crypto policy [596].

In the end, the crypto wars ended in the USA because Al Gore felt he needed to woo Silicon Valley in 2000 and gave up on the initiative (too late — many software millionaires supported the Republicans that year), and in Europe because the European Commission felt that it was getting in the way of building confidence in online banking and commerce — so they passed an Electronic Signature Directive that said in effect that signature keys couldn't be escrowed or they would lose their legal effectiveness. The Germans had won the argument. As for whether it mattered, U.S. government reports of Title III wiretaps since then disclose only one case in which cryptography prevented the authorities from recovering the plaintext [435].

24.3.11 Export Control

The main spillover from the crypto wars was the imposition of much more stringent export controls than before, particularly in Europe. There is a survey of cryptography law at [736]; here's a quick summary.

International arms control agreements (COCOM and Wassenaar) bind most governments to implement export controls on cryptographic equipment, and the latter is implemented in the European Union by an EU regulation compelling Member States to control and license the export of *dual-use goods* — goods which have both civilian and military uses. Cryptanalytic products fall under the military regime, whereas the great bulk of software that just uses cryptography for protection falls under dual-use.

But national implementations vary. UK law didn't control the export of intangibles until 2002, so crypto software could be exported electronically; the Belgian government grants licences for almost anything; and Switzerland remains a large exporter of crypto equipment. Domestic controls also varied. The French government started off from a position of prohibiting almost all civilian cryptography and moved to almost complete liberalisation, while Britain went the other way.

What this meant in practice during the 1990s was that European researchers like me could write crypto software and publish it on our web pages, while our counterparts in the USA were prevented from doing that by the U.S. International Trafficking in Arms Regulations (ITAR). Non-U.S. companies started to get a competitive advantage because they could export software in intangible form. The U.S. government got annoyed and in 1997, Al Gore persuaded the incoming British Prime Minister Tony Blair to get Europe to extend export control to intangibles. Meanwhile the USA relaxed its own controls, so now the positions are reversed, and Europe has the fiercest rules. Tens of thousands of small software companies are breaking the law without knowing it by exporting products (or even by giving away software) containing crypto with keys longer than 56 bits.

There are several ways to deal with this. In many countries people will just ignore the law and just pay a bribe if, by misfortune, they are targeted for enforcement. In Northern Europe, one course of action is to try to use various Open General Export Licenses (OGELs) that provide specific exemptions for particular products and activities, but these require a cumbersome registration process and will often be unsuited to an innovative company. Another is to use the exemption in export law for material being put in the public domain; make your software (or the relevant parts of it) free or open-source and make your money on support and services. Another, in the UK, at least, is to use the fact that placing something on a web server isn't export; the exporter, in law, is any person outside Europe who downloads it. So a developer can leave material online for download without committing an offence. Yet another is of course to actually apply for an export license, but the licensing system is geared to small numbers of large companies that export military hardware and are known to the licensing authorities. If large numbers of small software firms were to deluge them with applications for licenses, the system would break down. At present some officials are trying to empire-build by 'raising awareness' of export controls among academics (who ignore them); thankfully there are no signs of the controls being marketed to the software industry.

24.4 Censorship

I wrote in the first edition that 'the 1990s debate on crypto policy is likely to be a test run for an even bigger battle, which will be over anonymity, censorship and copyright'. Although (as I discussed in Chapter 22) copyright law has largely stabilised, there is still pressure from Hollywood for ISPs to filter out file-sharing traffic. However censorship has become a much bigger issue, over the past few years.

Censorship is done for a variety of motives. China blocks not just dissident websites, but even emails mentioning forbidden movements. Some countries switch censorship on during elections, or after crises; Burma imposed curfews after suppressing a wave of demonstrations. The live debate in the USA is about whether ISPs who are also phone companies should be able to block VOIP, and whether ISPs who also run cable channels should be able to block P2P: the principle of *net neutrality* says that ISPs should treat all packets equally. Net neutrality isn't as much of an issue in Europe where there's more competition between ISPs; the issue is that different European countries ban different types of content (France and Germany, for example, ban the sale of Nazi memorabilia, and won't let Amazon sell copies of Mein Kampf). Many countries have made attempts to introduce some kind of controls on child pornography — it's become a standard excuse for politicians who want to 'do something' about the Internet — and as I write there's a European initiative to ban radical

Islamist websites. Finally, censorship is sometimes imposed by courts in the context of civil disputes, such as the ban on publishing the DeCSS code that I mentioned in Chapter 22.

Censorship also takes a number of forms, from blocking certain types of traffic to IP address filtering, DNS poisoning, content inspection, and out-of-band mechanisms such as the punishment of individuals who downloaded (or were alleged to have downloaded) discountenanced material. I'll look now at a number of cases. (Declaration of interest: I've been funded by the Open Net Initiative as a result of which my students and postdocs have been busy measuring censorship in a number of countries.)

24.4.1 Censorship by Authoritarian Regimes

Rulers have long censored books, although the invention of the printing press made their job a whole lot harder. For example, John Wycliffe translated the Bible into English in 1380–1, but the Lollard movement he started was suppressed along with the Peasants' Revolt. When William Tyndale had another go in 1524–5, the technology now let him spread the word so quickly that the princes and bishops could not suppress it. They had him burned at the stake, but too late; over 50,000 copies of the New Testament had been printed, and the Reformation got under way. After that upset, printers were closely licensed and controlled; things only eased up in the eighteenth century.

The invention of the Internet has made the censors' job easier in some ways and harder in others. It's easier for the authorities to order changes in material that not many people care about: for example, courts that find a newspaper guilty of libel order the offending material to be removed, and changing the historical record wasn't possible when it consisted of physical copies in libraries rather than, as now, the online archive. It's easier for the authorities to observe the transmission of disapproved material, as they can monitor the content of electronic communications much more easily than physical packages. But mostly it's harder for them, as nowadays everyone can be a publisher; governments can still crack down on mainstream publishers, but have to contend with thousands of bloggers. A good reason for hope comes from observation of countries that try hard to censor content, such as China.

China had 137 million Internet users at the end of 2006, including a quarter of the population in the big cities. The government of Hu Jintao is committed to control and has invested hugely in filtering technology. People refer to 'the Great Firewall of China' although in fact the controls in that country are a complex socio-technical system that gives defence in depth against a range of material, from pornography to religious material to political dissent [984].

First, there are the perimeter defences. Most of China's Internet traffic flows through routers in Shenzhen near Hong Kong which filter on IP addresses to block access to known 'bad' sites like the Voice of America and the BBC;

they also use DNS cache poisoning. In addition, deep packet inspection at the TCP level is used to identify emails and web pages containing forbidden words such as 'Falun Gong': TCP reset packets are sent to both ends of such connections to tear them down. (I described the mechanisms in section 21.4.2.3 and noted there that while they can be fairly easily circumvented, anyone who did so regularly might expect a visit from the police.) Keyword filtering based on about 1000 wicked words is also implemented in Chinese search engines and blogs, while some individual Internet service providers also implement their own blocking and Internet cafés are required to by law.

Second, there are application-level defences. Some services are blocked and some aren't, depending on the extent to which the service provider plays along with the regime. There was a huge row when Google agreed to censor its search results in China (what they actually do is to populate their China index using spiders that search from within China, and thus only see material that's visible there anyway). The incentives created by China's rapidly growing markets enable its government to bully large international firms into compliance. One effect is that, as more and more of the online action moves to server farms run by transnational firms, the borders that matter are those of firms rather than of nations [918] (this is still probably an improvement, as new companies are easier to start than new countries).

Third, there are social defences. These range from 30,000 online police, through trials of cyber-dissidents and laws requiring cyber-cafés to identify customers, to a pair of Internet police cartoon mascots (Jingjing and Chacha) who pop up everywhere online to remind users that they're in social space rather than private space.

Yet the controls appear to be falling behind. There are more than 20 million blogs in China, and although the online police are vigorous at taking down openly seditious material, the online discussion of local news events has led to the emergence of a proper 'public opinion' that for the first time is not in thrall to media managers [985]. This is not just a function of email and blogs but also the rapid growth in mobile phone use. Local events such as land seizures by corrupt officials can now rapidly climb the news agenda, exposing the government to pressures from which it was previously insulated. It will be interesting to see how things go as China hosts the Olympics in 2008 and continues to develop beyond that.

A somewhat different example is Burma. There, a sudden increase in fuel prices in August 2007 led to mass protests and a violent crackdown by the army from September 26th that left perhaps several hundred people dead. During the protests and at the start of the crackdown, Burmese citizens used the Internet and mobile phone services to send photos, videos and other information to the outside world, with the result that their insurrection grabbed world headlines and the crackdown brought widespread condemnation on the ruling junta.

This happened despite the fact that Burma is one of only 30 countries in the world with less than 1% of its population online.

Other authoritarian states — such as Belarus, Uganda and the Yemen — had imposed Internet censorship around elections and other political events, and initially the Burmese junta concentrated on filtering political information arriving from overseas. But the world headlines clearly caused pain, and an Internet closedown started on September 29th, the third day of the crackdown. This was the first time wholesale Internet blocking was used to stop news getting out [986]. Service was resumed patchily after October 4; from the 4th to the 12th there was a curfew, with connectivity available only from 10pm until 4am; and in the third phase, some Internet cafés were allowed to reopen on October 11th, but speeds were limited to 256 kbit/sec; others were closed down and had equipment confiscated. It seems that most Burmese had been using censorship-circumvention tools such as proxies. In fact the uprising was called 'the g-lite revolution' after a popular Gmail proxy, `http://glite.sayni.net`.

If the lesson to learn from this sad incident is that even 1% Internet use can destabilise a dictatorship, and that even dictatorships have a hard time getting by without the Internet, then that's rather encouraging.

24.4.2 Network Neutrality

A number of less developed countries block voice-over-IP (VOIP) services to make phone tapping easier, and to keep the state phone company profitable. LDC phone companies often get much of their revenue from their share of the charges paid by foreigners to call that country, and VOIP lets expats escape these charges.

However, most of the problems experienced by VOIP operators are in the developed world, and particularly in America. A number of ISPs are also phone companies, and use technical mechanisms to disrupt VOIP services — such as introducing jitter or short outages into the packet stream. This affects not just wireline providers but also mobile firms. As a result, a fierce debate has erupted in Washington about *network neutrality*. On one side, the VOIP industry argues in favour of a law that would compel ISPs to treat all traffic equally; on the other, the phone companies retort 'Don't regulate the Internet'.

The issue is wider than just VOIP. Phone companies always charged widely different rates for different types of traffic: given that they have high fixed costs and low marginal costs, they have every incentive to price discriminate. Ed Whitacre, the AT&T chairman, kicked off the debate in 2005 when he argued that for companies like Google, Yahoo or Vonage to use 'his' broadband pipes for free to make money for themselves was 'nuts' [1340]. This has split Congress broadly on party lines, with Democrats favouring net neutrality and Republicans favoring the phone companies.

In Europe, net neutrality is less of an issue, as we have more competition in the ISP market. Regulators tend to take the view that if some ISPs indulge in traffic shaping (as it's politely called), then that doesn't matter so long as customers can switch to other ISPs that don't. There are some residual issues to do with mobile operators, as international calls from mobiles are expensive, but regulators are trying to tackle high charges directly rather than worrying about whether people can use Skype over GPRS.

24.4.3 Peer-to-Peer, Hate Speech and Child Porn

The three horses being flogged by the advocates of Internet censorship in the developed countries are file sharing, hate speech and child pornography.

File-sharing systems raise some of the net neutrality issues; for example, Comcast has been disrupting BitTorrent, using the same forged-reset packet techniques observed in the Great Firewall of China [409]. In Comcast's case, being a cable operator, they want their customers watch TV on their cable channel, rather than as downloads, to maximise their ad revenue. Other ISPs have different incentives; many people sign up to broadband service specifically so they can download stuff. Whether this makes a profit for the ISP or not will depend on how much traffic new customers generate and whether the backhaul costs more than their subscriptions. In general, ISPs make money from P2P, though often they have to restrict bandwidth use.

The main players arguing for filtering of peer-to-peer traffic are the music companies. Many universities have been bullied by the threat of litigation into restricting such traffic on student LANs; others have cut it simply to save on bandwidth charges. And despite all the economic evidence I discussed in Chapter 22, about the modest effect that file-sharing has on music sales, the music industry believes its interests would be served by imposing this censorship more widely. ISPs resist cenorship citing the high costs of filtering. It's therefore going to be interesting to see whether countries introduce mandatory filtering for 'moral' purposes, which the music industry can then have used for its purposes too.

There was a recent attempt in Europe to introduce a duty on ISPs to filter hate speech, and specifically jihadist websites. Europe has a history of such restrictions: France and Germany both prohibit the sale of Nazi memorabilia. (I recall one German justice minister telling a policy conference that her greatest achievement in office was to stop Amazon selling 'Mein Kampf' in Germany, and her greatest ambition was to stop them selling it in Arizona too.) I'm very sceptical about whether such a law would make Europe any safer; banning the writings of the militant Deobandi Muslim sect, to which perhaps a third of Britain's Muslims belong, is likely to aggravate community tensions more than anything else. Furthermore, research shows that most of the hate literature distributed inside and outside Britain's mosques is produced or funded by

religious institutions from Saudi Arabia [857]. The response of our government is not to stand up to King Abdullah, but to invite him for a state visit. Internet censorship here (as elsewhere) appears to be a displacement activity; it lets the government claim it's doing something. It's also likely to encourage all the third-world despots and Asian strongmen who denounce the freedom of speech on the Internet. Better, I'd think, to leave this material in the open, as America does, and let the police monitor the traffic to the worst of the sites, rather than driving Muslim youth to acquire the skills of the Chinese and Burmese at using proxies. In the end, the policy advice to the European Commission was along these lines: they should train the police to use the existing laws better [442]. And while they're at it, let law enforcement be technology-neutral: the cops should also monitor the young men who sell the hate tracts in the mosques (and if they ever pluck up the courage to prosecute them for breaking the existing laws on incitement to murder, so much the better).

The third horseman is child pornography. During the 1990s, as governments were looking for some handle on the Internet, a view arose that explicit images of child sex abuse were about the one thing that all states could agree should be banned. When arguing in favour of the latest repressive measure — such as key escrow — governments trotted out people from children's charities who would argue passionately that the Stalinism du jour was vital to save children from harm [272]. Needless to say, those of us on the liberal side of the argument would have preferred the charities to spend their money campaigning about more serious and potentially fixable child-protection problems, such as the abuse of children in local authority care homes, and under-age prostitution; and when a really serious problem arose at the boundary between IT policy and child protection — a proposal to construct a national child-welfare database that will expose the personal information of millions of children to hundreds of thousands of public-sector workers [66] — these worthy child-protectors remained silent.

The child-porn debate has subsided in most countries[4], as terrorism has taken the place of kiddieporn as the executive's ace of trumps –the argument that no-one's supposed to gainsay. But the hysteria did have some evil effects. They were severe in the UK where it was used to justify not only more pervasive online surveillance, but also a National High-Tech Crime Unit. This unit ran Operation Ore, in which some eight thousand UK citizens got raided by the police on suspicion of purchasing child pornography. It turned out that most of them were probably victims of card fraud. The porn squad didn't understand card fraud, and didn't want to know; they were fixated on getting porn convictions, and didn't ask their experts to even consider the possibility

[4]Russia's a notable exception; Putin uses kiddieporn as the leading excuse for censorship directed at political opponents, while his police take little action against the many pornographers and other online criminals in that country.

of fraud. Several thousand men had their lives disrupted for months or even years following wrongful arrest for highly stigmatised offences of which they were innocent, and at the time of writing (2007) there's a steady stream of acquittals, of civil lawsuits for compensation against police forces, and calls for public inquiries. The sad story of police bungling and cover-up is told by Duncan Campbell in [260, 261]. For some, the revelation that the police had screwed up came too late; over thirty men, faced with the prospect of a public prosecution that would probably destroy their families, killed themselves. At least one, Commodore David White, commander of British forces in Gibraltar, appears to have been innocent [594].

The cause of all this was that operators of illegal porn sites bought up lists of credit card numbers and then booked them through the portals that they used to collect payment — presumably in the belief that many people would not dare to report debits for such services to the police. And although the police justified their operations by claiming they would reduce harm to children, the child-porn purveyors in the Ore case escaped prosecution. (The operator of the main portal, Thomas Reedy, did get convicted and sentenced to over 1000 years in a Texas jail, but he was just the fall guy who collected the credit card payments. The gangsters in Indonesia and Brazil who organised and photographed the child abuse do not seem to have been seriously pursued.)

America actually handled this case much better than Britain. Some 300,000 U.S. credit card numbers were found on Reedy's servers; the police used the names for intelligence rather than evidence, matching the names against their databases, identifying suspects of concern — such as people working with children — and quietly investigating them. Over a hundred convictions for actual child abuse followed, and no wrongful convictions of which I'm aware. As with jihadist websites, a pragmatic emphasis on good old-fashioned policing is much preferable to fearmongering and grand political gestures.

24.5 Forensics and Rules of Evidence

This leads us naturally to the last main topic in the justice space, namely how information can be recovered from computers, mobile phones and other electronic devices for use in evidence. The three big changes in recent years have been, first, the sheer volumes of data; second, the growth of search engines and other tools to find relevant material; and third, that courts are becoming gradually more relaxed and competent.

24.5.1 Forensics

When the police raid even a small-time drug dealer nowadays, they can get well over a Terabyte of data: several laptops, half-a-dozen mobile phones, a

couple of iPods and perhaps a box of memory sticks. The suspect may also have dozens of accounts online for webmail services, social-networking sites and other services. He may have interesting gadgets — such as navigators that hold his location history (much of which is also available, with less resolution, via his mobile phone records). Security researchers have found all sorts of clever ways of extracting information from the data — for example, you can identify which camera took a picture from the pattern noise of the CCD array [818], and the number of such tricks can only increase.

The use of all this material in evidence depends, in most countries, on following certain procedures. Material has to be lawfully collected, whether with a search warrant or equivalent powers; and the forensic officer has to maintain a *chain of custody*, which means being able to satisfy a court that evidence wasn't tampered with afterwards. The details can vary from one jurisdiction to another, and I'll describe them in the next section.

The basic procedure is to use tools that have been appropriately tested and evaluated to make trustworthy copies of data, which may mean computing a one-way hash of the data so as to establish its authenticity later; to document everything that's done; and to have means of dealing appropriately with any private material that's found (such as privileged attorney-client emails, or the trade secrets of the suspect's employer). The details can be found in standard forensics textbooks such as Sammes and Jenkinson [1105], and much of the technical complexity comes from the proliferation of mobile phones, organisers, iPods and other storage devices, which the practitioner should be able to deal with. Indeed, as time goes on, specialist firms are springing up that deal with phones and other less common types of kit.

Computer forensics pose increasingly complex engineering problems. A recent example is that many police forces adopted a rigid procedure of always turning PCs off, so that hard disks could be mirrored and multiple copies made for prosecution and defence lawyers. The Rockphish gang exploited this by making their phishing software memory-resident. The police would arrive at a house containing a phishing server, inform the startled householder that his PC was being used for wicked purposes, switch the machine off — and lose all the information that would have let them trace the real server for which the seized machine had been acting as a proxy.

A related problem is that Windows Vista ships with Bitlocker, a disc encryption utility that stores keys in the TPM chip on the motherboard, and thus makes files unusable after the machine's switched off unless you know the password. While the UK now has a law enabling courts to jail people for failing to supply a password, most countries don't; so thoughtful police forces now operate a rule whereby a decision on whether to switch the machine off is at the officer's discretion. It's a judgment call whether to risk losing data by turning the machine off, or to image it when it's running and risk the defence lawyers arguing that it was tampered with. Truth to tell, however, the forensic

folks are still not discovering any great technical sophistication among normal criminals.

Another issue is that it may be important to minimise the disruption caused by forensic copying, especially where the machine belongs to someone other than an arrested suspect. Even where a machine is confiscated from a suspect, it can be problematic if you take too long to examine it. For example, in the Operation Ore cases I mentioned in the last section, many people who later turned out to be innocent had their PCs taken away and stored for months or even years because the police didn't have the forensic capacity to cope. As a result they remained under a cloud of suspicion for much longer than was reasonable; this had an adverse effect of people in regulated professions, leading to litigation against the police.

There's also the issue of loss of access to data, which for an individual or small business can be catastrophic. I reckon it's prudent practice nowadays for a student to have seizure-proof offsite backup, for example by getting a Gmail account and emailing copies of your thesis there regularly as you write it. Otherwise your house might be raided and both your PC and backups removed to the police forensic lab for months or even years. And it needn't be your fault; perhaps the guy on the second floor is smoking dope, or running a supernode in a music file-sharing system. You can just never tell.

Another forensic pitfall is relying on evidence extracted from the systems of one party to a dispute, without applying enough scepticism about claims made for its dependability Recall the Munden case I described in section 10.4.3. A man was falsely accused and wrongly convicted of attempted fraud after he complained of unauthorized withdrawals from his bank account. On appeal, his defence team got an order from the court that the bank open its systems to the defence expert as it had done to the prosecution. The bank refused, the bank statements were ruled inadmissible and the case collapsed. So it's worthwhile when relying on forensic evidence supplied by a disputant to think in advance about whether it will have to withstand examination by hostile experts.

In general, when designing a system you should stop and think about the forensic aspects. You may want it not to provide evidence; an example is the policy adopted by Microsoft after their antitrust battles with the U.S. government, at which embarrassing emails came out. The firm reacted with a policy that all emails should be discarded after a fixed period of time unless someone took positive action to save them. In other circumstances you may want your system to provide evidence. Then there's not just the matter of whether the relevant data are preserved, and for how long (if your local statute of limitations for civil claims is seven years, you'll probably want to keep business data for at least this long), but also how the data are to be extracted. In many jurisdictions, court rules admit evidence only if it passes certain tests, for example that it was generated in the normal course of business operations. So we need to look at such requirements next.

24.5.2 Admissibility of Evidence

When courts were first confronted with computer evidence in the 1960s there were many concerns about its reliability. There was not just the engineering issue of whether the data were accurate, but the legal issue of whether computer-generated data were inadmissible on the grounds that they were hearsay. Different legislatures tackled this differently. In the U.S. most of the law is found in the Federal Rules of Evidence where computer records are usually introduced as business records. We find at 803(6):

Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term 'business' as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

The UK is similar: the Civil Evidence Act 1995 covers civil litigation while the Police and Criminal Evidence Act 1984 deals with criminal matters[5]. The requirement that the machine be operated in the normal course of business can cause problems when machines have to be operated in abnormal ways to extract information. In one case in my own experience, a woman was accused of stealing a debit card from the mail and the police wished to ascertain whether a torn-off corner of a PIN mailer found in her purse would activate the stolen card. So they got the branch manager to put the card into a statement printer in the branch, entered the PIN, and the card was confiscated. The manager testified that the way the card was confiscated showed that it was because the account had been closed rather than because the PIN was wrong. However, the court ruled this evidence to be inadmissible. The rules of electronic evidence in the common-law countries (England, the USA, Canada, Australia, South Africa and Singapore) are analysed in detail by Stephen Mason [838]; for a summary of relevant U.S. cases, read Orin Kerr [714].

There are some special legal provisions for particular technologies, many of them enacted during or shortly after the dotcom boom as legislators sought to smooth the path for e-commerce without really understanding the problems. Many industry lobbyists claimed that e-commerce was held up by uncertainty

[5]The latter used to require a certificate from the machine operator to the effect that the equipment was working normally, but this was dropped as it caused problems with evidence from hacked machines.

about whether electronic documents would be accepted as 'writing' for those laws that required certain transactions to be written (typical examples are real-estate transfers and patent licenses). Legislatures, starting with Utah's, therefore introduced laws granting special status to digital signatures. In most cases these had no effect, as courts took the sensible view that an email is writing just as a letter is: the essence of a signature is the signer's intent, and courts had long decided cases this way. For example, a farm worker who was crushed to death by a tractor and had managed to scrawl 'all to mum' on the tyre was held to have made a legal will [1358, 1359]. For surveys of digital signature laws, see [109, 524].

However there's one case in which eager legislators got it completely wrong, and that's Europe. The Electronic Signature Directive, which came into force in 2000, compels all Member States to give special force to an *advanced electronic signature*, which basically means a digital signature generated with a smartcard. Europe's smartcard industry thought this would earn them lots of money. However, it had the opposite effect. At present, the risk that a paper check will be forged is borne by the relying party: if someone forges a check on my account, then it's not my signature, and I have not given the bank my mandate to debit my account; so if they negligently rely on a forged signature and do so, that's their lookout[6]. However, if I were foolish enough to ever accept an advanced electronic signature device, then there would be a presumption of the validity of any signature that appeared to have been made with it. All of a sudden, the risk shifts from the bank to me. I become liable to anyone in the world for any signature that appears to have been made by this infernal device, regardless of whether or not I actually made it! This, coupled with the facts that smartcards don't have a trusted user interface and that the PCs which most people would use to provide this interface are easily and frequently subverted, made electronic signatures instantly unattractive.

Finally, a word on click-wrap. In 2000, the U.S. Congress enacted the Electronic Signatures in Global and National Commerce ('ESIGN') Act, which gives legal force to any 'sound, symbol, or process' by which a consumer assents to something. So pressing a telephone keypad ('press 0 to agree or 9 to terminate this transaction'), clicking a hyper-link to enter a web site, or clicking 'continue' on a software installer, the consumer consents to be bound to a contract [457]. This makes click-wrap licenses work in America. The general view of lawyers in Europe is that they probably don't work here, but no-one's eager to bring the first case.

[6]Some countries, like Switzerland, let their banks shift the fraud risk to the account holder using their terms and conditions, but Britain always prohibited this, first by common law and then by the Bills of Exchange Act 1886.

24.6 Privacy and Data Protection

Data protection is a term used in Europe to mean the protection of personal information from inappropriate use. Personal information generally means any data kept on an identifiable human being, or *data subject*, such as bank account details and credit card purchasing patterns. It corresponds roughly to the U.S. term *computer privacy*. The difference in terminology is accompanied by a huge difference in law and in attitudes. This is likely to remain a problem for global business, and may get worse.

European law gives data subjects the right to inspect personal data held on them, have them changed if inaccurate, understand how they're processed, and in many cases prevent them being passed on to other organizations without their consent. There are exemptions for national security, but they are not as complete as the spooks would like: there was a big row when it turned out that data from SWIFT, which processes interbank payments, were being copied to the Department of Homeland Security without the knowledge of data subjects. European privacy authorities ruled that SWIFT had broken European, Belgian and Swiss privacy law, and it agreed to stop processing European data in the USA by the end of 2009 [995, 996].

Almost all commercial data are covered, and there are particularly stringent controls on data relating to intimate matters such as health, religion, race, sexual life and political affiliations. Finally, recent law prescribes that personal data may not be sent to organizations in countries whose laws do not provide comparable protection. In practice that means America and India, where legal protections on privacy are fragmentary. The resolution so far is the *safe harbour agreement* whereby a data processor in America or India promises to their European customer to abide by European law. Many firms do this, pioneered by Citibank which set up such an arrangement to process German cardholder data in South Dakota. But this creates practical enforcement problems for EU citizens who feel that their rights have been violated; they aren't privy to the contract, and may have a hard time persuading the U.S. Department of Commerce to take action against a U.S. firm that is quite possibly obeying local laws perfectly well. So the safe harbour provisions may well fail when tested in court. For a discussion, see [1339]. We'll have to wait until test cases find their way to the European Court.

If safe harbour fails, the cynical fix may be to put the servers in a European country with very lax enforcement, such as Britain, but even so there are problems: the UK is currently in dispute with the European Commission, which claims that British law falls short of European requirements on eleven separate points [406]. Another is to insist that customers agree to their personal data being shared before you do business with them. This works to some

extent at present (it's how U.S. medical insurers get away with their abuses), but it doesn't work for data protection as coercive consent is specifically disallowed [66].

European privacy law didn't spring full-formed from the brow of Zeus though, and it may be helpful to look at its origins.

24.6.1 European Data Protection

Technofear isn't a late twentieth century invention. As early as 1890, Justices Warren and Brandeis warned of the threat to privacy posed by 'recent inventions and business methods' — specifically photography and investigative journalism [1321]. Years later, after large retail businesses started using computers in the 1950s and banks followed in the early 1960s, people started to worry about the social implications if all a citizen's transactions could be collected, consolidated and analyzed. In Europe, big business escaped censure by making the case that only government could afford enough computers to be a serious privacy threat. Once people realised it was both economic and rational for government to extend its grasp by using the personal data of all citizens as a basis for prognosis, this became a human rights issue — given the recent memory of the Gestapo in most European countries.

A patchwork of data protection laws started to appear starting with the German state of Hesse in 1969. Because of the rate at which technology changes, the successful laws have been technology neutral. Their common theme was a regulator (whether at national or state level) to whom users of personal data had to report and who could instruct them to cease and desist from inappropriate processing. The practical effect was usually that the general law became expressed through a plethora of domain-specific codes of practice.

Over time, processing by multinational businesses became an issue too, and people realised that purely local or national initiatives were likely to be ineffective against them. Following a voluntary code of conduct promulgated by the OECD in 1980 [991], data protection was entrenched by a Council of Europe convention in January 1981, which entered into force in October 1985 [327]. Although strictly speaking this convention was voluntary, many states signed up to it for fear of losing access to data processing markets. It required signatory states to pass domestic legislation to implement at least certain minimum safeguards. Data had to be obtained lawfully and processed fairly, and states had to ensure that legal remedies were available when breaches occurred.

The quality of implementation varied widely. In the UK, for example, Margaret Thatcher unashamedly did the least possible to comply with European

law; a data protection body was established but starved of funds and technical expertise, and many exemptions were provided for favored constituencies[7]. In hard-line privacy countries, such as Germany, the data protection bodies became serious law-enforcement agencies. Many other countries, such as Australia, Canada, New Zealand and Switzerland passed comparable privacy laws in the 1980s and early 1990s: some, like Switzerland, went for the German model while others, like Iceland, followed the British one.

By the early 1990s it was clear that the difference between national laws was creating barriers to trade. Many businesses avoided controls altogether by moving their data processing to the USA. So data protection was finally elevated to the status of full-blown European law in 1995 with a Data Protection Directive [444]. This sets higher minimum standards than most countries had required before, with particularly stringent controls on highly sensitive data such as health, religion, race and political affiliation. It also prevents personal information being shipped to 'data havens' such as the USA unless there are comparable controls enforced by contract.

24.6.2 Differences between Europe and the USA

The history in the USA is surveyed in [933]; basically business managed to persuade government to leave privacy largely to 'self-regulation'. Although there is a patchwork of state and federal laws, they are application-specific and highly fragmented. In general, privacy in federal government records and in communications is fairly heavily regulated, while business data are largely uncontrolled. There are a few islands of regulation, such as the Fair Credit Reporting Act of 1970, which governs disclosure of credit information and is broadly similar to European rules; the Video Privacy Protection Act or 'Bork Bill', enacted after a Washington newspaper published Judge Robert Bork's video rental history following his nomination to the U.S. Supreme Court; the Drivers' Privacy Protection Act, enacted to protect privacy of DMV records after the actress Rebecca Schaeffer was murdered by an obsessed fan who hired a private eye to find her address; and the Health Insurance Portability and Accountability Act which protects medical records and which I discussed in Chapter 9. However U.S. privacy law also includes several torts that provide a basis for civil action, and they cover a surprising number of circumstances; for a survey, see Daniel Solove [1200]. There was also a landmark case in 2006, when Choicepoint paid $10 m to settle a lawsuit brought by the FTC after it failed to vet subscribers properly and let crooks buy the personal information of over 160,000 Americans, leading to at least 800 cases of 'identity theft' [459].

[7] In one case where you'd expect there to be an exemption, there wasn't; journalists who kept notes on their laptops or PCs which identified people were formally liable to give copies of this information to the data subjects on demand.

That may have started to put privacy on CEOs' radar. Yet, overall, privacy regulation in the USA is slack compared with Europe.

Attitudes also differ. Some researchers report a growing feeling in the USA that people have lost control of the uses to which their personal information is put, while in some European countries privacy is seen as a fundamental human right that requires vigorous legislative support; in Germany, it's entrenched in the constitution [1339]. But it must be said that there's a persistent problem here. As I discussed in section 7.5.4, people say that they value privacy, yet act otherwise. The great majority of people, whether in the USA or Europe, will trade their privacy for very small advantages. Privacy-enhancing technologies have been offered for sale, yet most have failed in the marketplace.

There's simply no telling how the gulf between the USA and Europe on privacy laws will evolve over time. In recent years, Europe has been getting less coherent: the UK in particular has been drifting towards the U.S. model, with ever more relaxed enforcement; and the new Member States that used to be part of the Soviet Union or Yugoslavia are not rocking the boat. Commerce is certainly pulling in the U.S. direction. As I discussed in section 7.5.4, technology simultaneously creates the incentive for greater price discrimination and the means to do it by collecting ever more personal data. Yet in other countries, courts have become more protective of citizens' rights post-9/11. In Germany, which generally takes the hardest line, privacy trumps even the 'war on terror': the highest court found unconstitutional a 2001 police action to create a file on over 30,000 male students or former students aged 18 to 40 from Muslim-majority countries — even though no-one was arrested as a result. It decided that such exercises could be performed only in response to concrete threats, not as a precautionary measure [244].

The flip side of the privacy-law coin is freedom-of-information law. A radical version of this is proposed by David Brin [227]. He reasons that the falling costs of data acquisition, transmission and storage will make pervasive surveillance technologies available to the authorities, so the only real question is whether they are available to the rest of us too. He paints a choice between two futures — one in which the citizens live in fear of an East German–style police force and one in which officials are held to account by public scrutiny. The cameras will exist: will they be surveillance cams or webcams? He argues that essentially all information should be open — including, for example, all our bank accounts. Weaker versions of this have been tried: tax returns are published in Iceland and in some Swiss cantons, and the practice cuts evasion, as rich men fear the loss of social status that an artificially low declared income would bring. Still weaker versions, such as the U.S. and U.K. Freedom of Information Acts, still give some useful benefit in ensuring that the flow of information between the citizen and the state isn't all one-way. As technology continues to develop, the privacy and freedom-of-information boundaries will no doubt involve a lot of pushing and shoving.

There are some interesting engineering questions. For example, while U.S. felony convictions remain on the record for ever, many European countries have offender-rehabilitation laws, under which most convictions disappear after a period of time that depends on the severity of the offence. But how can such laws be enforced now that web search engines exist? The German response is that if you want to cite a criminal case, you're supposed to get an officially de-identified transcript from the court. In Italy, a convicted business person got a court to order the removal from a government website of a record of his conviction, after the conviction had expired. But if electronic newspaper archives are searchable online, what good will this do — unless the identities of all offenders are blocked from electronic reporting? There has recently, for example, been much debate over the monitoring of former child sex offenders, with laws in some states requiring that offenders of registers be publicly available, and riots in the UK following the naming of some former offenders by a Sunday newspaper. How can you rehabilitate offenders in a world with Google? For example, do you tag the names of offenders in newspaper accounts of trials with an expiration date, and pass laws compelling search and archive services to respect them?

The upshot is that even if data is public, its use can still cause offences under European privacy law. This causes peculiar difficulties in the USA, where courts have consistently interpreted the First Amendment to mean that you can't stop the repetition of true statements in peacetime except in a small number of cases[8]. So it's hardly surprising that the current flashpoint between Europe and America over privacy concerns Google. The immediate casus belli is that EU law requires personal data to be deleted once it's no longer needed, while Google built its systems to keep data such as clickstreams indefinitely. During 2007, the European data-protection folks brought this to Google's attention; the search engine has offered to de-identify clickstreams after 18 months. Given the difficulty of doing inference control properly — as I discussed in Chapter 9 — this claim will no doubt be examined closely by the European authorities. No doubt this saga will run and run. Even in America, there's been a call from CDT and EFF for a 'Do Not Track' list, similar to the Do Not Call list, so that people could opt out; other activists disagree, saying this would undermine the paid-by-ads model of useful web services [1333]. In any case, less than a percent of people bother to use ad-blocking software. We'll have to wait and see.

24.7 Summary

Governments and public policy are entangled more and more with the work of the security engineer. The 'crypto wars' were a harbinger of this, as were the

[8]The classic example is a regulated profession such as securities trading.

struggles over copyright, DRM and Trusted Computing. Current problems also include surveillance, privacy, the admissibility and quality of evidence, and the strains between U.S. and European ways of dealing with these problems. In less developed countries, censorship is a big issue, although from the data we have to date the Internet still works as a definite force for good there.

Perhaps the biggest set of issues, though, hinge on the climate of fear whipped up since the 9/11 attacks. This has led to the growth of a security-industrial complex which makes billions selling counterproductive measures that erode our liberty, our quality of life and even our security. Understanding and pushing back on this folly is the highest priority for security engineers who have the ability to get involved in public life — whether directly, or via our writing and teaching. And research also helps. Individual academics can't hope to compete with national leaders in the mass media, but the slow, careful accumulation of knowledge over the years can and will undermine their excuses. I don't mean just knowledge about why extreme airport screening measures are a waste of money; we also must disseminate knowledge about the economics and psychology that underlie maladaptive government behaviour. The more people understand 'what's going on', the sooner it will stop.

Research Problems

Technopolicy involves a complex interplay between science, engineering, psychology, law and economics. There is altogether too little serious cross-disciplinary research, and initiatives which speed up this process are almost certainly a good thing. Bringing in psychologists, anthropologists and historians would also be positive. Since 2002 I've helped to build up the security-economics research community; we now have to broaden this.

Further Reading

It's extraordinarily easy for technopolicy arguments to get detached at one or more corners from reality, and many of the nightmares conjured up to get attention and money (such as 'credit card transactions being intercepted on the Internet') are really the modern equivalent of the monsters that appeared on medieval maps to cover up the cartographer's ignorance. An engineer who wants to build things that work and last has a duty not to get carried away. For this reason, it's particularly important to dig out primary sources — material written by experienced insiders such as R.V. Jones [671] and Gerard Walsh [1311].

There's a good book on the history of wiretapping and crypto policy by Whit Diffie and Susan Landau, who had a long involvement in the policy

process [387], an NRC study on cryptography policy was also influential [950]; and there's a compilations of primary materials at [1135]. There's also useful stuff at the web sites of organizations such as EPIC [432], EFF [422], FIPR [484], CDT [278], the Privacy Exchange [1048] and on mailing lists such as politech [1031] and ukcrypto [1267].

There are many resources on online censorship, starting perhaps with the OpenNet Initiative; and Reports without Borders publish a 'Handbook for bloggers and cyber-dissidents' that not only contains guides on how to circumvent censorship, but a number of case histories of how blogging has helped ipen up the media in less liberal countries [1069].

The standard work on computer forensics is by Tony Sammes and Brian Jenkinson [1105], and there's a nice article by Peter Sommer on the forensics and evidential issues that arose when prosecuting some UK youngsters who hacked the USAF Rome airbase [1202]. The Department of Justice's 'Guidelines for Searching and Seizing Computers' also bear some attention [381]. For collections of computer crime case histories, see Peter Neumann [962], Dorothy Denning [370] and Donn Parker [1005]. The standard work on computer evidence in the common law countries is by Stephen Mason [838].

On the topic of data protection, there is a huge literature but no concise guide that I know of. [1339] provides a good historical overview, with a perspective on the coming collision between Europe and the USA. Simson Garfinkel [515] and Michael Froomkin [504] survey privacy and surveillance issues with special relevance to the USA.