**Chapter 26**

**Surveillance or Privacy?**

**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

**Every thing secret degenerates, even the administration of justice;**

**nothing is safe that does not show how**

**it can bear discussion and publicity.**

– Lord Acton

**The arguments of lawyers and engineers pass through one**

**another like angry ghosts.**

– Nick Bohm, Ian Brown and Brian Gladman

**26.1** **Introduction**

Governments have ever more interests online, ranging from surveillance to cen-  
 sorship, from privacy to safety, and from market competition to fair elections.  
 Their goals are often in tension with the reality of a globalised online world,  
 and with each other too. They crystallise around a number of speciﬁc pol-

icy concerns, from terrorism and counterinsurgency, through national strategic  
 and economic advantage, to the suppression of harmful or unpopular content  
 and the maintenance of human rights. In this chapter we explore the nexus of  
 surveillance, censorship, forensics and privacy.

The Internet has transformed the world in lots of complicated ways, like other

big technologies before it – electricity, the steam engine, writing, agriculture and  
 ﬁre. The relationship between the citizen and the state has changed everywhere,  
 with the state usually acquiring more power and control. In the early years, as  
 the PC replaced the mainframe and the Internet opened up to all, many pioneers

820

*26.1. INTRODUCTION*

were utopians: we believed that free access to information would be liberating  
 at the personal level, and would destabilise authoritarian governments too. Yet  
 governments and large companies learned in time to use the new tools. The  
 terrorist attacks of September 11, 2001, on New York and Washington had a real  
 impact, by creating the incentive for mass surveillance and weakening political  
 opposition to it. The move of business online created the tools, and a commercial  
 market for personal information to pay for them. While the pendulum swung  
 back during the 2010s towards surveillance capitalism, the COVID-19 pandemic  
 looks set to increase state surveillance once more, with the trade-off being not  
 privacy versus security but privacy versus health.

It’s been a boom time for surveillance. It’s not just the NSA capabilities

revealed in 2013 by Ed Snowden; nation-state competitors like Russia and China  
 also have serious capabilities; while there are more primitive but still effective  
 systems in less developed countries like Syria.

The 2010s also saw growing cyber conﬂict and disruption with states inter-

fering covertly in other states’ affairs. The USA and Israel used the Stuxnet  
 malware to damage and delay Iran’s push to acquire nuclear weapons, and this  
 caused a rush by other states to acquire cyber-weapons of various kinds. Since  
 the Russian interference in the 2016 US election, legislators in a number of coun-  
 tries want to regulate social media: a lot of politicians have stopped ignoring  
 technology once they realised their jobs were on the line.

There are many thorny issues. First, are open societies with democracy and

a free press more vulnerable, because we’re easier to exploit? And if so what  
 can we do about it? We face real challenges to our core values – expressed in the  
 USA as the Constitution, and in Europe as the Convention on Human Rights.  
 Since 9/11 we’ve seen one authoritarian measure after another, ranging from  
 large-scale surveillance of communications to detention without trial and even  
 torture. Many of these measures were not just illegal and immoral but ineffective  
 or even counterproductive: torturing Iraqi secret policemen alongside al-Qaida  
 terrorists in the Abu Ghraib prison was what forged them into the core of Islamic  
 State. Can’t we ﬁnd better ways to defend freedom? And how can we reassert  
 and defend our core values?

Second, there’s the political economy of security. President Eisenhower

warned in his valedictory speech that ‘we must guard against the acquisition  
 of unwarranted inﬂuence, whether sought or unsought, by the military indus-  
 trial complex. The potential for the disastrous rise of misplaced power exists  
 and will persist’. Since 9/11, we’ve seen a security-industrial complex capturing  
 policy in the same ways that the defence industry did at the start of the Cold  
 War. Politicians of left and right have stoked a culture of fear, abetted by se-  
 curity agencies and the press. This has been deepened since the ﬁnancial crisis  
 of 2008 by the rise of nationalism.

Security technology arguments are often used to bamboozle or intimidate

legislators. For example, all through the Irish republican terrorist campaign  
 from the 1970s through 1990s, 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. The real problem was police

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 821 | Ross Anderson |

*26.1. INTRODUCTION*

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 talk of decryption seems a good  
 way to turn legislators’ brains to mush. People who understand cryptography  
 have a duty to speak out.

The focus on terrorism starved the rest of law enforcement. About half of all

crime is now online, and yet the resources devoted to ﬁghting it are tiny. Many  
 scammers operate with impunity.

There are further problems around censorship. Concerns about online abuse

are real, but this is a difficult area. Abuses range in seriousness from videos of  
 murder and child rape at the top end, down through hate speech, rape threats  
 and cyber-bullying to news manipulation which, at scale, can be toxic. Countries  
 are starting to pass laws requiring ﬁrms like Facebook to do the censorship for  
 them, which causes many tensions. The companies don’t like the extra costs, and  
 thoughtful citizens don’t like the idea of censorship being in the hands of private  
 monopolies – or the idea that everything we upload, from pictures and videos  
 to private messages, is ﬁltered. So the ﬁrms have an incentive to redesign their  
 systems so that they’re harder to abuse; Facebook, for example, claims to be  
 rebuilding its systems to focus more on groups, which are harder for extremists to  
 game, and to make more use of end-to-end encryption, so it can claim ignorance.  
 Such arguments cut no ice in major incidents, such as when a shooter killed  
 people at two mosques in Christchurch, New Zealand, in March 2019 and used  
 Facebook to share live video of the crime. This forced the company to start  
 censoring white supremacist groups, a politically sensitive task it had previously  
 avoided [1913]. The COVID-19 pandemic led the company to rapidly do many  
 things that the industry had previously denounced as impossible, undesirable  
 or impractical: removing misinformation, banning exploitative ads and pushing  
 official advice [984]. The tensions between privacy and censorship may continue  
 to work out in unpredictable ways.

Privacy regulation is already complex. U.S. laws are fragmented, with federal

laws on speciﬁc topics such as health data and video rentals and the FTC pun-  
 ishing ﬁrms that violate their published privacy policies, while state laws drive  
 security-breach disclosure. Europe is very different: the General Data Protec-  
 tion Regulation provides a comprehensive framework, backed up by human-  
 rights law that has been used to strike down laws on surveillance. The over-  
 all effect, from the viewpoint of the IT industry, is that Europe is becoming  
 the world’s privacy regulator; Washington doesn’t care, and nobody else is big  
 enough to matter. (There are strong signs that this regulatory power will be  
 extended steadily to safety as well, although we’ll leave that to the chapter on  
 assurance.)

In this chapter, I’m going to discuss the evolution of surveillance, then look

at terrorism before discussing censorship and privacy regulation, and ﬁnally  
 trying to put the whole thing in context.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 822 | Ross Anderson |

*26.2. SURVEILLANCE*

**26.2** **Surveillance**

The 2010s saw a huge increase in technical surveillance, not just by governments  
 but also by commercial ﬁrms monitoring our clickstream and location history  
 in order to target ads better – described by Shoshana Zuboff as ‘Surveillance  
 Capitalism’ [2075]. The two interact in various ways. In some countries, like  
 the USA, law enforcement and intelligence agencies don’t just get information  
 from their own collection systems but use warrants to get it from ﬁrms like  
 Google and Facebook too. In others, like China, these ﬁrms are banned because  
 they refused to give complete access to the authorities; in others, like Iran and  
 Syria, the police agencies just beat people’s passwords out of them, or phish  
 their friends, or hack their phones.

This is a huge subject, and all I can reasonably provide is a helicopter tour:

to place surveillance in its historical context, sketch what’s going on, and provide  
 pointers to primary sources.

**26.2.1** **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, ‘The Codebreakers’ [1001].

When electronic communications came along, governments tried to keep con-

trol. In most of Europe, the telegraph service was set up as part of the post office  
 and owned by the government; in Britain, the telegraph industry was national-  
 ized by Gladstone in 1869. A profusion of national rules caused so much trouble  
 that the *International Telegraph Union* (ITU) was set up in 1865 to standardise  
 things [1818]. In the USA, Western Union was the ﬁrst nationwide industrial  
 monopoly and dominated the market through the nineteenth century. Union  
 and Confederate soldiers tapped each others’ telegraph lines, and the New York  
 Police Department started wiretapping operations in 1895.

The invention of the telephone led to tussles over privacy. 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; Justice Brandeis famously dissented. In  
 1967, the Court reversed itself in *Katz vs United States*, ruling that the amend-  
 ment 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 in-  
 vestigation into the Nixon administration’s abuses, Congress passed the Federal  
 Intelligence Surveillance Act (FISA), which controls wiretapping for national se-  
 curity. 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 wiretap, as did technical developments such as adaptive  
 echo cancellation in modems.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 823 | Ross Anderson |

*26.2. SURVEILLANCE*

So the 1994 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 [634, 1257]; by 2017 the number  
 of wiretap orders had almost tripled to 3,813, but 94% were against portable  
 devices such as cellphones [1927]1. A further 1,598 orders were granted in whole  
 or in part by the Foreign Intelligence Surveillance Court (FISC) while 26 were  
 denied.

Even before 9/11, some analysts believed that there were at least as many

unauthorized wiretaps as authorized ones [558]. First was phone company col-  
 lusion: while a phone company must give the police access if they present a  
 warrant, in many countries they are also allowed to help – and there have been  
 many reports over the years of phone companies being cosy with the government.  
 Second, there’s intelligence-agency arbitrage: 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 was said, for example, that Margaret Thatcher used the Cana-  
 dian intelligence services to wiretap ministers suspected of disloyalty [728]. Such  
 practices were denied by the agencies for years but the Snowden leaks showed  
 them to be reality; for example, the NSA got GCHQ to tap the links between  
 Google data centres, as I described in 2.1. Third, in some countries, wiretapping  
 is uncontrolled if one of the subscribers consents – so calls from phone boxes are  
 free to tap (the owner of the phone box is the legal subscriber). Companies may  
 wiretap their staff to detect fraud and voluntarily pass the product to the police  
 or security agencies; there was a scandal in the UK when it emerged that the  
 security services were involved in an unlawful, clandestine scheme to blacklist  
 construction industry staff who had tried to organise unions [658]. Finally, in  
 many countries, the police get hold of email and other stored communications  
 by subpoena rather than warrant. They did this in America too before a court  
 stopped the practice in 2007 [1161] – but the judgment didn’t stop private ac-  
 tors such as bounty hunters and bail agents buying phone location histories from  
 data aggregators [489].

But even if the official ﬁgures have to be doubled or tripled, democratic

regimes use wiretapping very much less than authoritarian ones. The surveil-  
 lance leader now is China, which uses pervasive technical monitoring in regions  
 with minority populations such as Xinjiang and Tibet, with surveillance cameras  
 mounted over street corners, mosques and schools hooked up via face-recognition  
 software to databases recording who was seen where and when. There are also  
 intrusive physical measures ranging from frequent street checkpoints, through  
 billeting party members in the homes of minority families, to mass incarceration  
 in labour camps [1110].

The incidence of wiretapping has also been highly variable within and be-

tween democracies. In the USA, for example, only about half the states use it,  
 and for much of the 20th century most taps were in the ‘Maﬁa’ states of New  
 York, New Jersey and Florida (though Nevada and California have now caught  
 up) [1927]. There is similar variation in Europe. Wiretaps are very common in  
 the Netherlands: they have up to 1,000 taps on the go at once with a tenth of

1The relevant law is 18 USC (US Code) 2510–2521, while FISA’s regulation of foreign

intelligence gathering is now codiﬁed in US law as 50 USC 1801–1811.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 824 | Ross Anderson |

*26.2. SURVEILLANCE*

America’s population [356]. In a Dutch homicide investigation, it’s routine to  
 tap everyone in the victim’s address book for a week to monitor how they react  
 to the death. The developed country with the most wiretaps is Italy, thanks to  
 its history of organised crime [1160]. In the UK, domestic wiretaps are supposed  
 to need a ministerial warrant, and cannot be used in evidence; so the police use  
 room bugs and computer exploits instead. If you can root a gangster’s phone  
 or laptop you can record, and mail home, everything said nearby, whether it’s  
 said to someone in the same room, or on a call. International calls have been  
 routinely recorded for decades and stored for some days to weeks in case they  
 turn out to be of interest, a model followed by many other countries; for exam-  
 ple, after the Mumbai massacre in 2008, India could dig out recordings of phone  
 calls the terrorists made to their controllers in Pakistan.

Automation is shifting the costs of wiretapping from per-call labour costs to

one-off capital costs. Before CALEA was introduced, in 1993, US police agencies  
 spent only $51.7 million on wiretaps – perhaps a good estimate of their value  
 before the issue became politicised [862]. The implementation of CALEA cost  
 over $500m, and that was before it was extended to VOIP in 2007. VOIP was  
 harder: “The paradigm of VoIP intercept difficulty is a call between two road  
 warriors who constantly change locations and who, for 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” [220]. During the 2010s things became  
 harder still as people moved from physical platforms, such as their cellphone,  
 to virtual platforms such as Facebook, Skype and Signal. So the trend for

policymakers has been to make capital investments that cut the marginal costs  
 of access. For example, ten years ago, if the UK police were investigating three  
 similar rapes, they might have had to pay the phone companies thousands of  
 pounds to assemble cellsite dumps so they could look for any mobile phones that  
 were present at all three locations. Now, after spending hundreds of millions  
 and getting several laws passed, they have access to databases of mobile phone  
 locations, and all it takes is a database query. This changes the nature of both  
 police and intelligence work.

The USA also changed its laws to facilitate bulk surveillance. 43 days after

the 9/11 attacks, Congress passed the Patriot Act, which 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.

But this was not enough for the agencies. In December 2005, the New York

Times revealed that President Bush had signed a secret 2002 order mandat-  
 ing warrantless wiretapping of US residents suspected of terrorism, contrary to  
 law [1606]. In 2006, USA Today revealed that the NSA had covertly obtained  
 full call-data records (CDRs) for the 200m customers of AT&T, Verizon and  
 BellSouth, the nation’s three biggest phone companies. The CDR program had  
 been started by the DEA in 1992 under the older President Bush, and tar-  
 geted calls by Americans to and from certain countries; it was ramped up after  
 9/11, when his son authorised the collection of CDRs for all internal US calls  
 too [877]. Qwest did not cooperate, because its CEO at the time, Joe Nac-  
 chio, maintained that the NSA needed a court order. The NSA put pressure on

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 825 | Ross Anderson |

*26.2. SURVEILLANCE*

Qwest by threatening to withhold classiﬁed contracts, so Qwest’s lawyers asked  
 the NSA to take its proposal to the FISA court. They refused, saying the court  
 might not agree with them. It’s since emerged that they had put pressure on  
 Qwest to hand over data even before 9/11 [768]. In October 2007, Verizon ad-  
 mitted to senators that it had given the FBI second-generation call data on its  
 customers against national security letters on 720 occasions since 2005 [1376].  
 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 [1377]. After  
 two years of debate, Congress amended FISA to grant retroactive immunity to  
 phone companies who cooperated with unlawful wiretapping, and to change the  
 law so that 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-US person. (This split both  
 parties, with Senators Obama and Feinstein supporting the amendment while  
 Senators McCain, Biden, Reid, Leahy and Clinton opposed it.)

**26.2.2** **Call data records (CDRs)**

Historically, more police communications intelligence has come from the analysis  
 of telephone call data records and other metadata rather than wiretaps. We  
 discussed in the chapter on telecoms security how the police use such data to  
 trace networks of criminal contacts, and how criminals respond by burying their  
 signals in innocuous traffic using techniques such as pre-paid mobile phones and  
 PBX hacking.

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 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 [1818]. The First  
 World War taught the combatants how much intelligence could be gleaned from  
 measuring the volume of enemy radio traffic, even when it couldn’t conveniently  
 be deciphered [1001, 1380]. Later twentieth-century conﬂicts reinforced this.

When I wrote the ﬁrst edition of this book, I noted that the USA had

1,329 wiretap applications approved in 1998, while there were 4886 subpoenas  
 (plus 4621 extensions) for *pen registers* (devices which record all the numbers  
 dialed from a target 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). Law-enforcement agencies were also starting  
 to switch in the 1990s to using subpoenas for the call-detail records in the  
 phone companies’ databases. Bell Atlantic, for example, responded to 25,453  
 subpoenas or court orders for toll billing records of 213,821 of its customers  
 in 1989–92, while NYNEX processed 25,510 subpoenas covering an unrecorded  
 number of customers in 1992 alone [402]. Scaled up across the seven Baby Bells,  
 this suggests that perhaps half a million customers were having their records

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 826 | Ross Anderson |

*26.2. SURVEILLANCE*

seized every year in the 1990s, and that traffic data were collected on perhaps  
 a hundred times as many people as were subjected to wiretapping.

Statistics went dark after 9/11, during the period of unlawful collection,

although the NSA did reveal in 2006 that it wanted “to create a database of  
 every call ever made within the nation’s borders” so it could map the entire US  
 social network for the War on Terror [395]. After Snowden revealed in 2013  
 that it had built databases of pretty well all traffic data for all communications  
 worldwide, Congress passed the Freedom Act in 2015 and we started to get an  
 annual Statistical Transparency Report from the Director of National Intelli-  
 gence. The April 2018 report gives some ﬁgures for 2017; these relate only to  
 national-security matters, but give some feel for the balance between content  
 and traffic data. Wiretap warrants are stable at about 1,500 per year in the USA  
 (targeting about 300 US persons and 1000 others), as well as a rising number  
 of targets overseas – 106,469 in 2016 and 129,080 in 2017. In addition, there  
 were 7,512 US residents whose communications content was retrieved (e.g. sub-  
 poenas for email) while 16,924 residents had non-content (such as traffic data)  
 retrieved, along with 56,064 non-residents. There were also 87,834 collected

business records, which might include records of which subscriber was using  
 which IP address [1464].

Now the US intelligence community only considers a communication to be

‘intercepted’ when a human analyst looks at it; analysis by software doesn’t  
 count (UK law counts both). As I described in Section 23.3.1, the usual proce-  
 dure when hunting for suspects is contact chaining, also known as a ‘snowball  
 search’. If someone blows themselves up in a terror attack, analysts will use soft-  
 ware that looks at all the people they communicated with, and then everyone  
 these direct contacts communicated with, and exceptionally even out to a third  
 degree of separation. The standard depth-two search typically gives some tens  
 of thousands of indirect contacts. These contacts are then compared against  
 millions of names on various suspect lists – religious extremists, right-wing hate  
 groups, organised crime – and the analysts then home in on the links with any  
 known suspects. (The analogy is rolling a snowball downhill, then melting it  
 and seeing what dirt you ﬁnd in the bottom of the bucket.) So the analyst may  
 look at only half a dozen people who were in contact with the dead terrorist and  
 also with members of some religious group, but tens of thousands of innocent  
 people had their call data records looked at by the software. The DNI report  
 estimates that in 2017, 534,396,285 call data records (CDRs) were examined  
 automatically in this way – a large increase from 151,230,968 in 2016.

Yet there was a long debate in Congress about allowing Section 215 of the

Patriot Act (as amended by FISA) to lapse. This was the section that allows  
 the bulk collection of CDRs [416]; the NSA has said that it doesn’t want it. The  
 bulk collection of communications data was one of the matters highlighted by  
 Ed Snowden that sparked the most controversy. On June 8th 2013, the press  
 disclosed Boundless Informant, an NSA visualisation tool that shows a heat map  
 of where metadata are collected for both voice and computer communications;  
 in a 30-day period ending in March 2013, 3 billion records were collected from  
 504 sources (or SIGADs). Although the most intensive collection was in the  
 Middle East, Snowden said that more records were collected on Americans in  
 America than on Russians in Russia [756]. On another reading of the material,

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 827 | Ross Anderson |

*26.2. SURVEILLANCE*

Boundless Informant collected 3 billion phone records via US telecommunica-  
 tions providers, plus a further 97 billion emails and 124 billion phone calls round  
 the world [816, p. 92]; overall, 20 billion events a day are collected [816, p. 98].  
 However, a declassiﬁed report revealed that while the NSA call-data record pro-  
 gram in the USA cost over $100m, it produced only two leads and one signiﬁcant  
 investigation [1656]. In 2020, the clause was allowed to lapse in March but rein-  
 stated in May; the politics was messy. Susan Landau and Asaf Lubin explained  
 that with 4g mobile networks, traditional CDRs don’t identify both the caller  
 and the called party reliably any more [1126]. In any case, the action is shifting  
 from the plain old telephone system to messaging systems.

As for targeted collection in speciﬁc criminal investigations, under 18 USC

3123 [1925], the investigative officer merely has 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 misde-  
 meanour – and under either Federal or State law. Since CALEA, warrants are  
 still required for such communications data as the addresses to which a sub-  
 scriber has sent e-mail messages, but basic toll records can be obtained under  
 subpoena – the subscriber need not be notiﬁed, and there is no court supervision  
 once the order has been made. The US Department of Justice is required by  
 law to publish statistics for its non-national-security law-enforcement activities  
 but appears reluctant to do so; the American Civil Liberties Union (ACLU)  
 extracted ﬁgures for 2011–12 only after freedom-of-information (FOI) litigation,  
 which revealed that the combined number of original orders for pen registers and  
 trap and trace devices used to spy on phones increased by 60%, from 23,535 in  
 2009 to 37,616 in 2011 [765]. I’ve been unable to ﬁnd anything more recent.

Bulk access to traffic data has been also led to serious political tussles in

Europe. The UK pushed through a Data Retention Directive in the European  
 Union in 2006, under which member states had to store telecommunications  
 data – including IP address and timing of every email, phone call and text  
 message sent or received – for between 6 months and 24 months, and make  
 all this available to law enforcement and intelligence agencies. The Directive  
 was struck down in 2014 by the European Court of Justice after Digital Rights  
 Ireland brought a lawsuit arguing that blanket data collection violated the EU  
 Charter of Fundamental Rights.

In Britain, targeted access to 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. Following the Data Retention Directive, the Blair government wanted to  
 centralise things; it argued that the police needed a ‘communications database’  
 and pushed a law to establish it. Fate intervened when some wicked person  
 stole a copy of all the expenses claims ﬁled by members of parliament and sold  
 it to the Daily Telegraph. It turned out that numerous ministers and others had  
 been making embarrassing claims; several honourable members went to jail, and  
 most of the well-known politicians in Britain had to make repayments. (I told  
 the tragic tale of the Home Secretary, Jacqui Smith – who had been promoting  
 the communications database – in section 8.6.5 above.) We heard nothing more  
 of the communications database until Ed Snowden told us in 2013 that they’d  
 just built it anyway, even without parliamentary approval.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 828 | Ross Anderson |

*26.2. SURVEILLANCE*

After the European Court struck down data retention, and Snowden revealed

some highly objectionable activities by GCHQ, the UK passed the 2014 DRIP  
 Act to assert that what GCHQ had been doing was legal after all. It was clear  
 that the European Court would object eventually, but some breathing space was  
 needed and the Act gave this (it had a two-year sunset clause; Prime Minister  
 Cameron’s liberal coalition partners wouldn’t give him any more). Eventually,  
 in the wake of the Brexit vote, Parliament passed the Investigatory Powers Act,  
 which pretty well enables GCHQ to do as it pleases and compel any company  
 in the jurisdiction to assist it. The interesting action in the future will be, ﬁrst,  
 the extent to which the large US ﬁrms will help, and second, the line to be taken  
 by the European Court of Human Rights2. I’ll return to these issues later.

**26.2.3** **Search terms and location data**

It has become ever clearer over the past 20 years that the regulation of surveil-  
 lance that evolved in the phone-company era is not really ﬁt for purpose in  
 the era of the Internet. Back then, you got either a full wiretap and recorded  
 the content, or made do with traffic data from call data records. But as things  
 moved online, communications data and content got all mixed up, as what’s con-  
 tent at one level of abstraction is often communications data at the next. Some  
 people might think of a URL as 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. This became a live issue in 1999, when the UK government  
 modernised its surveillance law; academics, NGOs and industry managed to get  
 a ‘Big Browser Amendment’ into the resulting Regulation of Investigatory Pow-  
 ers Act of 2000 deﬁning traffic data as the information necessary to identify the  
 communicating machine; for URLs, this means everything up to the ﬁrst slash.

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 11.2.3 how when AOL released some search histories, a number of them  
 were easily identiﬁable to individuals.) AOL, Microsoft and Yahoo quietly com-  
 plied, but Google resisted. A judge ﬁnally ruled in 2006 that the Department  
 would get no search queries, and only a random sample of 50,000 of the URLs  
 it had originally sought [2035].

The next issue was mobile-phone location data, which ended up being treated

differently in different jurisdictions. In Britain, all information about the loca-  
 tion 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)

2Britain’s departure from the EU will let it escape the European Court of Justice, which is

an EU institution, but not the Court of Human Rights, as this is an institution of the Council  
 of Europe

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 829 | Ross Anderson |

*26.2. SURVEILLANCE*

would invade privacy [1926]. Also, even cell-granularity location information  
 would not be available under the lower standards applied to pen-register sub-  
 poenas. Yet despite these rules, there were massive leaks of information. It  
 emerged in 2019 that AT&T and Sprint had both been selling their customers’  
 location information to data brokers for years, including not just cellsite data  
 but GPS; and this had routinely been bought by bounty hunters and bail agents  
 to track defaulters [489]. Location data is now being collected by many govern-  
 ments with a view to tracing contacts of COVID-19 sufferers and epidemiology  
 more generally. It’s also collected by lots of apps: the Untappd beer-rating app  
 is run by millions of beer drinkers who record hundreds of time-stamped loca-  
 tions, which enabled journalists to track US military and intelligence personnel  
 around the world [1538].

**26.2.4** **Algorithmic processing**

The analysis of call data is only one aspect of a much wider issue: law-enforcement  
 matching of bulk datasets. The earliest serious use of multiple-source data ap-  
 pears 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 managing  
 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 subpoe-  
 naed from 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, and there’s little to stop them using commercially  
 available data such as feeds from credit reference agencies.

Since AlphaGo beat Lee Sedol in 2016, there’s been a host of machine-

learning startups, and quite a few aim to make law enforcement easier one way  
 or another. But it’s not as easy as it looks. Terrorists are so rare as a per-  
 centage of the population that any tests you use to ‘detect’ them would require  
 extraordinary speciﬁcity if you’re not to drown in false positives. Combining  
 multiple sensors is hard, and if you’re looking for a needle in a haystack, it’s  
 not always smart to build a bigger haystack. As Jeff Jonas, once the chief sci-  
 entist 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 accu-  
 racy that’s necessary that I see them as nothing but civil liberty infringement  
 engines” [757].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 830 | Ross Anderson |

*26.2. SURVEILLANCE*

**26.2.5** **ISPs and CSPs**

The 2000s saw rapid growth of intrusive surveillance at both Internet Service  
 Providers (ISPs) and Communications Service Providers (CSPs – ﬁrms like  
 Google and Yahoo). Tapping data traffic at an ISP 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. The  
 ISP simply became the natural control point.

Many countries now have laws requiring ISPs to help, and the usual way to

do it at a large ISP is to have equipment already installed that will send copies  
 of packets of interest (or NetFlow records) to a separate classiﬁed network. The  
 FBI’s system, DCSNet, is very slick – allowing agents point-and-click access  
 to traffic and content from participating phone companies [1761]. (Information  
 about which companies have been brought onboard is closely held, but smart  
 bad guys use small ISPs.) And things often go wrong because the police don’t  
 understand ISPs; they subpoena the wrong things, or provide inaccurate times-  
 tamps so that the wrong user is associated with an IP address. For an analysis  
 of failure modes, see Clayton [442].

The smartphone revolution has changed the natural control point from the

ISP to the CSP. A modern criminal might get up, check his messages on Gmail  
 or WhatsApp using his home wiﬁ, then get on a bus into town and do the same  
 using his 3G or 4G data connection, then perhaps use wiﬁ at a Starbucks or  
 a public library ... and in none of these cases does a wiretap at the ISP tell  
 anything much beyond the fact that a particular service has been used. As

the traffic to that communications service is encrypted, the police have to serve  
 paperwork on the service to get anywhere. This is what led the FBI to set up  
 the Prism system, whereby intelligence agencies can get customer data from  
 Google, Yahoo, Apple, Microsoft, Facebook and others at the press of a button.  
 It is also what led the UK, in its 2016 Investigatory Powers Act, to grant itself  
 the power to order any company to do anything it physically can in order to  
 assist law-enforcement of intelligence investigations. More and more countries  
 are passing such laws, which put the service providers in conﬂict with other  
 countries’ laws.

One big ﬂashpoint is the tension between EU privacy and data-protection

law, which requires due process for privacy infringement, and US surveillance  
 law which demands that US ﬁrms hand over foreigners’ data on demand. But  
 there are many more. Google left China rather than give the police unfettered  
 access to all user data. And as a senior Google executive told me, ‘If a family  
 court in India orders you to hand over the Gmail of someone who lives in Canada  
 and imposes a lifelong secrecy order, how do you simultaneously employ people  
 in India, and give believable assurances of privacy to people in Canada?’

Finally, there are lots of issues around the much richer data available from

CSPs like Facebook, which not only collect highly sensitive data at scale but  
 enable sensitive facts to be deduced from traffic data in ways that were not pre-  
 viously possible. As I discussed in section 11.2.5, Michal Kosinski and colleagues

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 831 | Ross Anderson |

*26.2. SURVEILLANCE*

ﬁgured out that he could tell whether someone was straight or gay from four  
 Facebook likes [1086], after which some of his colleagues collected Facebook data  
 at industrial scale and weaponised it for political campaigning, leading to the  
 Cambridge Analytica scandal when it was discovered that social-network data  
 had been used in 2016 to intervene unlawfully and at scale in both the Brexit  
 referendum in the UK and the presidential election in the USA. What sort of  
 controls should there be on the use of social analysis methods by law-enforcement  
 and intelligence agencies, or for that matter by public-health agencies? (We’ll  
 return to the broader issues raised by these techniques later.)

**26.2.6** **The Five Eyes’ system of systems**

We discussed the technical meat of the Snowden revelations in 2.2.1. These did  
 not come entirely from the blue; there had been many previous disclosures about  
 signals intelligence collection. David Kahn’s inﬂuential history of cryptography  
 sets the scene by describing what happened up till the start of World War  
 2 [1001]. An anonymous former NSA analyst, later identiﬁed as Perry Fellwock,  
 then revealed the scale of NSA operations in 1972 [674]. “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 whistle-

blower 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 [2031], which led to many  
 further books on World War 2 signals intelligence (Sigint) [438, 1002, 2007].  
 Thereafter there was a slow drip of revelations by investigative journalists, quite  
 a few of whose sources were concerned about corruption or abuse of the fa-  
 cilities by officials monitoring targets they should not have, such as domestic  
 political groups. Whistleblower Peg Newsham revealed that the NSA had ille-  
 gally tapped a phone call made by Senator Strom Thurmond [373, 374]. James  
 Bamford pieced together a lot of information on the NSA from open sources  
 and by talking to former employees [160], while New Zealand journalist Nicky  
 Hager [849] dug up a lot of information following the New Zealand intelligence  
 community’s failure to obey an order from their Prime Minister to downgrade  
 intelligence cooperation with the USA.

The ﬁrst high-proﬁle expos´e of US economic espionage was made in a 1999

report to the European parliament [644], which was concerned that after the col-  
 lapse of the USSR, European Union member nations were becoming the NSA’s  
 main targets [377]. By then, people who paid attention were aware that data,  
 faxes and phone calls get collected at a large number of nodes ranging from  
 where international communications cables land in friendly countries (or are  
 tapped clandestinely underwater), through observation of traffic to and from  
 commercial communications satellites and special Sigint satellites that collect

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 832 | Ross Anderson |

*26.2. SURVEILLANCE*

traffic over hostile countries, to listening posts in member states’ embassies [644].

During the Cold War, much of the effort was military, aimed at understand-

ing Soviet radar and communications, and at gaining a decisive advantage in  
 location, jamming and deception. Without an ability to conduct electronic war-  
 fare, a modern state is not competitive in air or naval warfare or even in tank  
 battles. Most of the personnel at NSA were military, and its director has always  
 been a serving general or admiral. A lot of effort still goes into understanding  
 the signals of potential adversaries.

One might question whether this huge worldwide system of systems still

gives value for money. Politicians have justiﬁed its budgets since 9/11 in terms  
 of terrorism, and there have indeed been some successes against terrorists –  
 notably the arrest of an alleged 9/11 terrorism planner after he used a mobile  
 phone SIM from a batch bought by a known terrorist in Switzerland. But elec-  
 tronic warfare against insurgents in Iraq proved less productive, as I discussed  
 in Chapter 19. And it’s clear that 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” [758].  
 Nearly two decades after the start of the wars in Afghanistan, Iraq, Syria and  
 North Africa, we haven’t trained enough soldiers to carry a basic conversation  
 in Arabic, Dari or Pushtu.

Although other countries may complain about US Sigint collection, for them

to moralise about it is hypocritical. Other countries also run intelligence oper-  
 ations, and are often much more aggressive in conducting economic and other  
 non-military espionage. The real difference between the Five Eyes countries

and the others is that no-one else has built the ‘system-of-systems’. Indeed,  
 there are network effects in Sigint as elsewhere: while non-aligned countries like  
 India were happy to buy their warplanes from the old Soviet Union, they nowa-  
 days tend to share intelligence with the USA, as it has a much bigger network  
 than the Russians or the Chinese [84]. The Snowden documents reveal NSA  
 information sharing with over 60 other countries.

My own view is that, like the armed forces of which they are often a part,

signals intelligence agencies are both necessary but potentially dangerous. 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 US citizens [423]; this led to FISA. The Snowden  
 revelations in turn led to action by all three arms of the US government, albeit  
 of limited effect3.

The structural problems remain, though. The NSA is responsible for both

3President Obama set up the NSA review group and accepted most of its recommendations,

but his positive work was undone by President Trump. Congress passed the USA Freedom  
 Act which imposed some limits on the bulk collection of communications data on US residents  
 by US agencies. Chief Justice Roberts made some changes to the FISA court.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 833 | Ross Anderson |

*26.2. SURVEILLANCE*

attack and defence, and defence tends to play second ﬁddle. Imagine that you’re  
 the Director of the NSA, and one of your engineers comes to you with a cool new  
 zero-day exploit of Windows. Do you tell Microsoft, thereby protecting 300m  
 Americans, or do you keep it secret, so you can attack 1.2bn Chinese? Stated in  
 those terms, the answer is obvious. This *equities issue* is the one issue on which  
 President Obama declined to follow the advice of the NSA review group. The  
 group recommended that in almost all cases, vulnerabilities that come to the  
 attention of the NSA should be reported to vendors for ﬁxing; the NSA prefers  
 to stockpile them instead. Indeed it has a $100m a year budget for Bullrun,  
 a program to insert them into commercial products by means fair and foul, as  
 discussed in section 2.2.1.5. And when bugs occur naturally, the NSA uses them  
 where it can; it was reported in 2014, for example, that the hugely disruptive  
 Heartbleed bug in SSL had been exploited by the NSA for two years before it  
 was discovered independently and ﬁxed [2065].

In some countries things are cleaner: in both France and Germany, there are

separate agencies for attack and defence. But in most countries, the oversight  
 of intelligence isn’t even discussed. In the UK, it’s only the European courts  
 that forced the government to admit to the scale of surveillance, and to legislate  
 some controls on it. New cases continually highlight excessive collection, by  
 both electronic and human methods. In 2019, the European Court of Human  
 Rights ordered the UK police to delete from its ‘extremism’ database the records  
 of some 60 demonstrations attended by John Catt, a 94-year-old protester with  
 no criminal record – a verdict applauded even in the conservative press [2024].

That is the high-level picture of how surveillance has evolved over the past

few decades. Another aspect is scale. Cross-border bandwidth increased from  
 11Tbit/sec in 2007, when the systems described by Ed Snowden were being built,  
 to 704Tbit/sec in 2017; this ﬁrehose creates yet more pressure for the agencies  
 to collect traffic from CSPs or other edge systems rather than from ISPs or  
 the backbone, as they can target the collection much better. The resulting

pressure for government access to data is remarkably similar to the pressure for  
 government access to cryptographic keys in the 1990s, which was a formative  
 experience for many governments (as well as for industry and civil society) on  
 issues of surveillance and technology policy.

**26.2.7** **The crypto wars**

Technology policy during the 1990s was dominated by acrimonious debates  
 about *key escrow* – the Clinton administration doctrine that anyone who en-  
 crypted data should give the government a copy of the key, so that the civilian  
 use of cryptography would not interfere with intelligence gathering.

I was involved 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, a UK Internet-  
 policy think-tank, which wrestled with crypto policy, export policy, copyright  
 and related issues. In 2003 we set up European Digital Rights (EDRi) along  
 with other European NGOs to campaign on these issues in Brussels. In the next  
 few sections I’ll lay out a brief background to the crypto wars, and then discuss  
 how governments have failed to get to grips with the Internet.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 834 | Ross Anderson |

*26.2. SURVEILLANCE*

**26.2.7.1** **The back story to crypto policy**

Many countries made laws in the mid-19th century banning the use of cryp-  
 tography 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 [1818]. 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

signals intelligence, the UK and US governments agreed in 1946 to continue in-  
 telligence cooperation. This ‘BRUSA agreement’ was joined by Canada in 1948  
 and by Australia and New Zealand in 1956, giving the ‘Five Eyes’ partnership in  
 signals intelligence. They decided to prevent the proliferation of cryptographic  
 equipment and know-how. Until the 1980s, about the only vendors were com-  
 panies selling into government markets, who could mostly be trusted not to do  
 anything overseas which would upset their major customers at home. This was  
 reinforced by export controls that 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.” [206]

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 licenses and product approvals. The upshot was that most governments  
 used weak crypto, and the NSA could break it with ease. But this wasn’t the  
 whole story, as we learned in the B¨uhler case.

Hans B¨uhler worked as a salesman for the Swiss ﬁrm Crypto AG, a leading

supplier of cryptographic equipment to governments without the technical ca-  
 pability to build their own. He was arrested in 1992 in Iran when the authorities  
 ﬁgured out that the Iraqis had been reading their traffic during the Iran-Iraq  
 war; they accused him of selling them cipher machines which had been tampered  
 with so that the NSA could get at the plaintext. Crypto AG paid 1.44 billion  
 Rials – then about a million US dollars – to bail him, but ﬁred him once he  
 got back to Switzerland. B¨uhler 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 [335]. One story was that when the  
 founder of Crypto AG, Boris Hagelin, decided to retire, he contacted William  
 Friedman, the NSA’s chief scientist; Friedman was a friend, and the US govern-  
 ment had been a big customer, buying Hagelin machines during World War 2.  
 Hagelin sold his company secretly to the NSA, which had it secretly controlled  
 by German nominees. The equipment it sold was routinely red threaded [1205].  
 Crypto AG’s line was that these allegations were concocted by the NSA to

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 835 | Ross Anderson |

*26.2. SURVEILLANCE*

undermine the company, as it was one of the third world’s few sources of cryp-  
 tographic equipment. B¨uhler’s story was told in a book by Res Strehle [1837].  
 It is now known that Crypto AG was run by the German Bundesnachrichten-  
 dienst in collaboration with the agencies of Denmark, Sweden, the Netherlands  
 and France, and with the CIA. The backdoors in their equipment were used,  
 for example, by the UK to decipher Argentinian communications during the  
 Falklands war in 1982 – the outcome of which was “materially inﬂuenced, if not  
 decided” by this operation [970].

**26.2.7.2** **DES and crypto research**

Despite the poor 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 US but overseas, without this cipher being adopted by foreign  
 governments and driving up 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 gov-  
 ernments adopting it. The rotor machines continued in service, in many cases  
 reimplemented using microcontrollers; Crypto AG and other biddable vendors  
 continued to thrive; and the traffic continued to be harvested. Foreigners who  
 encrypted their important data with such ciphers merely marked that traffic as  
 worth collecting.

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 a subtler strategy. While the Pentagon funded research into  
 computer security, it tried to divert crypto research into theoretical channels  
 and claimed that more practical published research work was all old hat: ‘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 playbook. 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 sideline one and build up the other.

By the mid 1990s this line had become exhausted. Agency blunders in the

design of key escrow systems debunked their story that they were way ahead  
 of the rest of us in cryptology, and in any case the ﬁght moved to a different  
 battleﬁeld.

**26.2.7.3** **Crypto War 1 – the Clipper chip**

Crypto policy went mainstream in 1993 with the launch of the Clipper chip. Af-  
 ter AT&T proposed the introduction to the US domestic market of an encrypting

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 836 | Ross Anderson |

*26.2. SURVEILLANCE*

telephone that would have used Diffie-Hellman key exchange and triple-DES to  
 protect traffic, the NSA persuaded the Clinton administration to promote a dif-  
 ferent standard. This would use a classiﬁed block cipher, Skipjack, implemented  
 in a tamper-resistant chip and with a protocol that made a spare (‘escrowed’)  
 key available to the agencies to decrypt traffic. This ‘Escrowed Encryption Stan-  
 dard’ led to a public outcry; an AT&T computer scientist, Matt Blaze, found a  
 protocol vulnerability in Clipper that defeated the escrow mechanism [258] and  
 the proposal was withdrawn.

Several more attempts were made through the 1990s to promote the use

of cryptography with government access to keys. 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 [980], and this was used to try to get the private sector to  
 adopt it as well; but we found a number of vulnerabilities in it too [115].

The pro-escrow people said that as crypto provided conﬁdentiality, and con-

ﬁdentiality could help criminals, there needed to be some way to defeat it. The  
 anti-escrow lobby started out by arguing that since crypto was necessary for pri-  
 vacy, there must not be a way to defeat it. Reality was more complex [56]. Most  
 crypto applications are about authentication rather than conﬁdentiality, so help  
 the police rather than hindering them. As for criminals, they mainly require  
 unobtrusive communications – and back in the 1990s, encrypting a phone call  
 was a good way to bring attention to yourself. If you wanted to be unobtrusive,  
 it was better to just buy a prepaid phone. As for privacy, most violations result  
 from abuse of authorized access by insiders. Finally, a much more severe prob-  
 lem for policemen is to ﬁnd acceptable evidence, for which decent authentication  
 can also be helpful.

The debate got rapidly tangled up with export controls on weapons, the

means by which cryptography was traditionally controlled. US software ﬁrms  
 were not allowed to export products containing cryptography that was too hard  
 to break, and this was also used as a means of controlling cryptography at  
 home; Americans who put cryptography software on their websites were liable  
 to prosecution for making it available to foreigners. A US 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 became a folk  
 hero and made a fortune as his product grabbed market leadership. Others,  
 such as Bruce Schneier, printed cryptographic algorithms in books as a way of  
 exercising their constitutional right to free speech [1667]. The conﬂict became  
 international: the US State Department tried hard to persuade other countries  
 to control cryptography too (I’ll go into more detail in Section 26.2.9 on export  
 control below). Imposing American policy worldwide became one of the missions  
 of Vice-President Gore (a reason why many tech people contributed to the Bush  
 campaign in 2000).

The apparent resolution of Crypto War 1 came in two phases. In 1999, the

European Union’s Commissioner for the Single Market, Martin Bangemann,  
 pushed through the Electronic Signature Directive, a law that banned the com-  
 pulsory licensing of certiﬁcation authorities. This undermined the demand from

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 837 | Ross Anderson |

*26.2. SURVEILLANCE*

the NSA and GCHQ that all private signing keys should be escrowed – not just  
 decryption keys, but also signature veriﬁcation keys. The Germans objected  
 that escrowing signature keys would let the agencies not just read messages,  
 but forge them too, undermining trust in electronic commerce and authentica-  
 tion generally. When the EU followed the German line rather than the British  
 one, it followed that individuals could either use their signature keypairs for  
 encryption, or to authenticate Diffie-Hellman keys and use those for encryption.  
 European officials molliﬁed the US administration by passing an export control  
 regulation that extended EU export controls from physical goods to intangibles  
 such as software, so that European ﬁrms faced the same export controls on  
 cryptographic software as US ﬁrms [651].

Second, in 2000 when Al Gore was running for president and wanted to get

Silicon Valley onside, the administration decided to call a halt. Meetings were  
 held at the FBI offices in Quantico between the agencies and the tech majors,  
 leading to an agreement that the agencies would no longer push for vulnerabilites  
 to be inserted into products and systems. Instead, the agencies would exploit  
 the many naturally-occurring vulnerabilities, and the NSA inveigled itself into  
 the patching cycle. When a software vulnerability is reported to the CERT

ecosystem, it ﬁnds its way to the CERT at the Software Engineering Institute  
 in Pittsburgh, which is sponsored by the DoD. This shares it with the NSA and  
 also reports it to the vendor for ﬁxing. The patch cycle typically takes a month  
 or two – sometimes more, if coordinating vulnerability disclosure and product  
 testing is hard – giving the NSA a window to exploit the bug.

Those of us who were active in digital rights in Europe were generally pleased

at the e-signature directive but appalled at intangible export controls; we set  
 up European Digital Rights (EDRi) in 2003 to create a lobbying presence in  
 Brussels, backed by dozens of individual NGOs in European countries. We

thought that the surveillance issue had been largely settled and that future  
 ﬁght would be over issues like software copyright and data protection. In 2013,  
 Ed Snowden showed us how wrong we’d been. The NSA and the other agencies  
 had simply gone underground, and had been running a covert program called  
 Bullrun with a budget of $100m a year to undermine commercial cryptography,  
 interfering with standards, implementations, supply chains and much else. But  
 that came later.

One of the engineering lessons from Crypto War 1 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; I discussed this in a paper ‘The Risks  
 of Key Recovery, Key Escrow, and Trusted Third-Party Encryption’ that I wrote  
 with ten other cryptographers and that became the most highly-cited reference  
 on the subject [4]. Where escrow is required it’s usually better done with simple  
 local mechanisms. In one army, every officer must write down his passphrase  
 on a piece of paper, put it in 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. But trying  
 to automate this and scale it up leads to trouble. The UK government idea was  
 that everyone’s private key would be generated from their email address using a

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 838 | Ross Anderson |

*26.2. SURVEILLANCE*

super-secret master key generated by GCHQ and kept in equipment controlled  
 by their departmental security officer, so that both the department and GCHQ  
 could decrypt traffic if they had to. The result was a clunky system that couldn’t  
 easily deal with the frequent changes of name as government departments were  
 reorganised and renamed. The demand for customised central control leads to  
 vast IT projects that run years late and millions over budget, or just never work  
 at all. Problems providing officials with working email systems led to them

using private accounts instead, and eventually the Cameron government more  
 or less gave up; routine email in the Cabinet Office (the stuff below Top Secret)  
 started to use a branded version of G Suite, the paid-for version of Gmail. By  
 the coronavirus pandemic, the cabinet was using Zoom for meetings, despite  
 known insecurities; there did in fact exist a secure videoconferencing system,  
 but as it was classiﬁed, ministers weren’t allowed to take it home.

Crypto War 1 left a signiﬁcant legacy, with both technical and political as-

pects. On the technical front, the mandated use of weak cryptography made  
 DVDs easy to rip, made cars easier to steal, made Bluetooth easy to hack, and  
 made millions of building locks easy to defeat – including the building where I  
 work4. The business models of ﬁrms selling hotel door locks have been under-  
 mined as they can no longer lock in their customers to buying their proprietary  
 card stock. As for policy, authoritarian governments such as Russia’s passed  
 harsh crypto control laws; Britain went from a laissez-faire policy under John  
 Major in the mid 1990s to Tony Blair’s Regulation of Investigatory Powers  
 (RIP) Act of 2000 which 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 licence if I send any cryptographic software outside Europe that  
 uses keys longer than 56 bits5. I’ll return to export control later.

**26.2.8** **Crypto War 2 – Going spotty**

The 2013 disclosures by Edward Snowden have led to a resumption, after a  
 fashion, of the crypto wars. In fact, the NSA and its partners never stopped,  
 but just took their ‘crypto enabling’ activities underground. They were not only  
 harvesting everyone’s SMSes and email from the backbone, and getting content  
 from major service providers using warrants at much larger scale than we imag-  
 ined. They were hacking allies, as when GCHQ hacked Belgacom [734] – an  
 amazing story about how one EU member state attacked the critical infrastruc-  
 ture of another, and went on to wiretap the European Commission. Another  
 example was New Zealand’s contribution to the Five Eyes which includes spy-  
 ing on small neighbours such as Samoa, Tonga and French Polynesia [850]. The  
 NSA had lied to Congress, for example about collecting call data records on US  
 citizens. They were bypassing legal controls: GCHQ could get my gmail from  
 Google using Prism, as I’m not a US resident, and we’d always suspected this,  
 but it had always been denied. They were also getting it from major services by  
 covert means – by tapping the communications between Google’s data centres.

4See section 4.3.1 for car theft, section 5.7.2.2 for attacks on Bluetooth and section [**?**] for

attacks on door locks.

5Thankfully, the person who does the exporting is the person who clicks on the link – so

if you’re in Iran, you would be a very bad person if you clicked on the link on my website to  
 download the Serpent block cipher. You have been warned!

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 839 | Ross Anderson |

*26.2. SURVEILLANCE*

In 2015, a UK court ruled that for the UK to obtain mass surveillance data on  
 UK residents via the USA had been unlawful, as it contravened the European  
 Convention on Human Rights [304].

All this had a real effect on behaviour. First, the service providers cleaned

up their act; Google had been starting to encrypt its internal network but ac-  
 celerated the program to ensure that the only way to get their users’ data was  
 through the front door, by a warrant. Microsoft and Yahoo followed. Second,  
 most messaging systems offered end-to-end encryption to reassure users (and  
 also to save system operators the cost of complying with warrants). Third, the  
 policy conversation started tackling more realistic problems, such as jurisdic-  
 tion; given that most of the material of interest to the world’s police forces is  
 kept on servers belonging to US companies, who can get access to it, and on  
 what terms? While countries like the UK worked at getting faster access to  
 US data, others went for localisation. India had already insisted that all pri-  
 vate Blackberry users keep their messages on servers in India; China banned  
 Facebook and Google to ensure its residents used Chinese systems instead; and  
 many countries have passed data-localisation laws to ensure that some kinds  
 of personal data are kept within the jurisdiction. Most countries in Africa, for  
 example, require ﬁnancial data to be kept locally; I’ll discuss the European  
 Union’s data-protection regulation and its interaction with US ﬁrms later.

Although the agencies no longer ask for access to all keys, the escrow ar-

guments came back in new forms post-Snowden. GCHQ, along with the FBI,  
 started to argue that providers of messaging services such as WhatsApp and  
 FaceTime should be compelled to build in a facility whereby law enforcement  
 can be added as a silent conference-call party (so-called ‘ghost users’) when  
 they get a warrant. FBI Director James Comey led the charge along with

GCHQ Director Robert Hannigan, who accused Facebook in 2014 of helping  
 terrorism [1566] by requiring him to go through the procedures of the UK/USA  
 Mutual Legal Assistance Treaty to get information. Facebook’s response was  
 that they were just obeying US and EU privacy laws; the relevant service centre  
 was in Ireland, not the UK, so Hannigan couldn’t simply use UK law to force  
 them to help him. He and Comey were supported by UK Prime Minister David  
 Cameron.

My cryptographer colleagues and I reconvened to write an update of our

analysis, ‘Keys Under Doormats’, which explains how many of the problems  
 with 1990s key escrow proposals simply come back in a new form if you man-  
 date government access to data instead of to keys [5]. The effects if anything  
 are likely to be worse, as we are now much more dependent on the Internet than  
 in the 1990s. It would be a bad thing if governments were to force designers  
 to abandon security mechanisms such as forward secrecy, authenticated encryp-  
 tion and strict transport security that have become widespread in the meantime;  
 and because of the many interactions between systems that have been secured  
 in different ways, the risk of mandated vulnerabilities having serious and unan-  
 ticipated side-effects is now much greater. Building in exceptional access also  
 creates huge targets in the wiretapping systems themselves, and extra complex-  
 ity that can lead to further security failures. Indeed, the 2010 Chinese hack of  
 Google’s wiretapping system suggests that even the best-run companies cannot  
 keep out state actors all the time – and that hack was aimed at the systems

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 840 | Ross Anderson |

*26.2. SURVEILLANCE*

Google built to service wiretaps. The Chinese obviously wanted to know which  
 of their agents in the USA was under suspicion. There are huge problems around  
 jurisdiction. If Facebook carries a WhatsApp message from a user in France to  
 a user in Argentina, do only these two governments get access, or does the NSA  
 demand it too? Since Snowden, everyone knows they will, and nobody believes  
 they could keep such a capability under control. Any demand for such systems  
 raises a lot of questions of both law and engineering, some of which we spelled  
 out in our analysis [5].

The next move came in 2016 when the FBI tried to force Apple to produce

an operating system ‘upgrade’ for the iPhone that would unlock it, using as  
 their test case a locked iPhone that had been used in a terrorist attack in  
 San Bernardino. Apple’s Tim Cook had resisted pressure to install back doors  
 before, and saw the case as a serious threat to Apple users’ privacy and to the  
 Apple brand; he fought the FBI in court [1006]. Comey testiﬁed that the agency  
 would not be able to get at such vital information without assistance from Apple.  
 The case divided American opinion, with Republicans supporting the FBI (and  
 candidate Trump, as he then was, calling for a boycott of Apple) while most  
 Democrats, and the tech industry, supported Tim Cook. My colleague Sergei  
 Skorobogatov worked out how to defeat the iPhone PIN retry counter [1777], as  
 I discussed in 3.4.8.3. As for the FBI, they bought a commercial iPhone exploit  
 from an Israeli ﬁrm, Cellebrite, and dropped the case.

In the chaos following the Brexit referendum, the new UK Prime Minister

Theresa May (who as home secretary had been a surveillance hawk) pushed the  
 Investigatory Powers Act through UK parliament. This law grants ministers  
 the power to order any company to do anything physically possible to facilitate  
 signals intelligence collection, and to keep quiet about it forever. In 2018, two  
 senior GCHQ mathematicians, Ian Levy and Crispin Robinson, suggested how  
 government access to messaging services might work [1153]; their idea was that  
 when GCHQ presented Facebook with a warrant, they would add a GCHQ pub-  
 lic key quietly to the target’s keyring, so that they’d become a silent conference  
 party to all his calls. My colleague Bruce Schneier responded in detail [1678]:  
 the fact that such an approach would work with some systems (it would work  
 with WhatsApp but not with Signal) is actually a bug that’s being ﬁxed by  
 better transparency mechanisms, and mandating it would prevent the bugﬁx.  
 In any case, such an access power is excessive; intelligence agencies should not  
 have it because of their history of abusing such access, or simply losing it. In  
 section 2.2.3 I described how the NSA tool EternalBlue was stolen and used by  
 the Russians against Ukraine in the NotPetya worm, causing billions of dollars  
 of collateral damage to US ﬁrms in 2016; by 2019 it was being used in ran-  
 somware that shut down email and other services in the city of Baltimore, just  
 up the road from the NSA [1529].

In 2019, Mark Zuckerberg announced that Facebook will shift its emphasis

from public posts to emphemeral, end-to-end encrypted messaging by unifying  
 WhatsApp with Instagram and Messenger [1439]. Some cynics suggested that  
 this would make it easier to hide fake news and hate speech from both the media  
 and the law, and cut the costs of moderation as well as the PR damage from  
 scandals; others that it was to prevent either the EU or the US government  
 from ordering the breakup of the company [1911, 1931]. In October, the US

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 841 | Ross Anderson |

*26.2. SURVEILLANCE*

Attorney General joined the UK Home Secretary and the Australian Minister  
 for Home Affairs in asking Zuck to think again, highlighting the risk of ‘a single  
 platform that would combine inaccessible messaging services with open proﬁles,  
 providing unique routes for prospective offenders to identify and groom our  
 children’. Time will tell whether Zuck can do abuse detection using metadata  
 alone; we’ll consider moderation and other forms of censorship below.

**26.2.9** **Export control**

One spillover from the crypto wars was the imposition of more uniform export  
 controls than before, particularly in Europe; here’s a quick summary. Interna-  
 tional arms control agreements (COCOM and Wassenaar) bind most govern-  
 ments 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 software that just uses cryptography for protection falls under  
 dual-use.

National policy used to vary more, and during the 1990s European re-

searchers like me could write crypto software and publish it on our web pages,  
 while our US colleagues were prevented from doing that by the US Interna-  
 tional Trafficking in Arms Regulations (ITAR). US ﬁrms complained and in  
 1997, Vice-President Al Gore persuaded the incoming British Prime Minister  
 Tony Blair to extend export control to intangibles. He initially tried to sell this  
 to the UK parliament, but the relevant committees weren’t keen, so Blair had it  
 pushed through as an EU regulation and his ministers then happily told us“Our  
 hands are tied – we have to do this as it’s EU law”. (Such policy laundering,  
 as it’s called, has been endemic in Europe and is one of the factors that fuelled  
 the movement to get Britain to leave the EU.)

Tens of thousands of academics and small software companies are now break-

ing the law without knowing it by exporting products (or even by giving away  
 software) containing crypto with keys longer than 56 bits. There are open gen-  
 eral export licenses (OGELs) that you can use, but you have to understand  
 the mechanisms and ﬁle the paperwork. And it’s not just cryptography. For  
 example, in our hardware tamper-resistance research we use an ion beam work-  
 station, which is like an electron microscope only it ﬁres metal ions at the target  
 rather than electrons, so you can modify a chip by cutting tracks and adding  
 new ones. Like cryptography, this is on the dual-use list. In the old days, we  
 had to get an export licence when we bought one, and another seven years later  
 when we threw it in a skip. Now, we’re in theory supposed to get a licence  
 whenever we share a script we’ve written for the machine with someone who  
 isn’t an EU citizen or resident. The practical outcome is that tens of thousands  
 of scientists happily break the law – which can make them vulnerable to pres-  
 sure from the agencies. The number has surely shot up now that the pandemic  
 has led to many people working from home, often from overseas, and that the  
 UK has left the EU. How I deal with such issues personally is to be very careful  
 that all such software and scripts are on my website, which enables me to use  
 a public-domain exemption, and rely on the fact that it’s the person who clicks

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 842 | Ross Anderson |

*26.3. TERRORISM*

on the link who performs the export.

The civil war in Syria exposed the dark side of export control in 2012. People

from several digital rights NGOs lobbied the UK government, asking it to use  
 export control law to prevent a UK company selling bulk surveillance equipment  
 to the Assad government. UK NGOs argued that mass surveillance equipment  
 should not just be on the dual-use list but the military list, that the intelligence  
 community includes bulk collection in ‘cryptanalysis’ which is military; and its  
 sale to a government involved in wholesale abuses was against human-rights  
 law. The lady from GCHQ fought this tooth and nail; the sales were going  
 through an arms dealer in Dubai so how could the vendor be sure of the desti-  
 nation; they came from a German subsidiary so it was the Germans’ problem;  
 Wassennaar was a forum for military issues rather than human rights ones; and  
 even that mass surveillance is also used for marketing. The real issue was that  
 GCHQ feared that UK troops would end up in Syria and they were determined  
 that if President Assad was going to have black boxes on his network, they  
 should be British black boxes rather than Ukrainian ones. Eventually the Ger-  
 man chancellor Angela Merkel admitted in public that she had decided to allow  
 surveillance equipment to be sold to Syria, and that it was one of the hardest  
 decisions she’d taken. In August 2013, the UK Parliament voted against autho-  
 rising military action in Syria, and President Obama decided not to go it alone.  
 In due course, the export control issue was referred to European agencies and  
 quietly forgotten.

One unpleasant side-effect of this ﬁght lingers: a system of vetting foreign

students at UK universities. GCHQ was opposed to Chinese students studying  
 cryptography, and the security service briefed that an Iraqi woman who’d got a  
 PhD in Britain had gone on to direct part of Saddam Hussein’s alleged research  
 programme into weapons of mass destruction. Briefers raised a scare about

people from countries on the terrorist list, such as Sudan, being allowed to study  
 medicine. Tony Minson, a professor of virology and Cambridge colleague, argued  
 that nature can do much nastier things than people can, and if there were no  
 competent public-health people in Khartoum when something like Ebola came  
 down the Nile, we’d regret it. He was of course ignored. We got an ‘Academic  
 Technology Approval Scheme’, and graduate students coming to the UK have  
 to get an ‘ATAS clearance’ to get a visa.

**26.3** **Terrorism**

Talk about terrorism has driven a lot of policy around surveillance and privacy,  
 especially since 9/11. The tide is starting to recede, but it’s still a card that  
 politicians play when they want to scare us, and the media often play along.  
 There has been talk of cyber-terrorism; that basically hasn’t happened, but  
 there are real concerns about encrypted chat services and social media being  
 used to groom and recruit young people to criminal organisations ranging from  
 right-wing hate groups to Islamic State. So what can we say about terrorism?

Political violence is nothing new; anthropologists have found that tribal war-

fare was endemic among early humans, as indeed it is among chimpanzees [1132].  
 Terror has long been used to cow subject populations – by the Maya, by the

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 843 | Ross Anderson |

*26.3. TERRORISM*

Inca, by William the Conqueror. Terrorism of the ‘modern’ sort also 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 1969–97, some three thousand people died, and the  
 IRA even blew up a hotel where the Prime Minister, 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 jihadists ﬁghting  
 the Russians in Afghanistan. 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.

**26.3.1** **Causes of political violence**

The biggest piece of good news is that the trend in terrorist violence has been  
 steadily downward [1350]. 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 partly

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) [459]. The world has plenty of grievances, but the data show

that the incidence of rebellion was more 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 got signiﬁcant support from  
 the Soviet bloc and Libya; the Tamil revolt in Sri Lanka was sustained by funds  
 from ethnic Tamils in the USA and India; and Al-Qaida was ﬁnanced by rich  
 donors in the Gulf states. So we know one way to tackle an insurgency: cut off  
 their money supply. It’s not entirely that simple, of course; the loss of Soviet  
 support for the ANC (and Angola and Mozambique) reduced the pressure on  
 the last white government of South Africa but gave them the space to do a  
 historic peace deal with Nelson Mandela.

**26.3.2** **The psychology of political violence**

Less encouraging ﬁndings come from scholars of psychology, politics and the  
 media. Psychology gives a lot of insight into the underlying mechanisms. I

mentioned the affect heuristic in Section 3.2.5: where people rely on affect, or

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 844 | Ross Anderson |

*26.3. TERRORISM*

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 [1787]. Most of the Americans who died as a result of 9/11 probably did  
 so since then in car crashes, after deciding to drive rather than ﬂy: the shift  
 from ﬂying to driving led to about 1,000 extra fatalities in the following three  
 months, and about 500 a year since then [1677].

There are other effects 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 [1564]. 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. 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 been made 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 just become mean: they were  
 also prepared to give larger rewards to citizens who performed some public act.  
 It turns out that when you remind people of death, it makes them adhere more  
 strongly to their cultural norms and defend their worldview more vigorously.  
 This helps explain why cyber-terrorism just hasn’t happened. Hacking a couple  
 of substations and turning off a town’s electricity can be mighty inconvenient,  
 but it just doesn’t have the same emotional effect as a bleeding child. The

media analysis conﬁrms this; coverage is strongly correlated with fatalities, and  
 increases by 46% for each extra dead body [1026].

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 natu-  
 ral 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 Pres-  
 ident), and for some people bigotry too. It was natural that, as the memory of  
 the attacks receded, society would repolarise because of divergent core values.  
 Curiously, when they’re reminded that they’re mortal, 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 Constitu-  
 tion, in which case conservatives defend the student’s right to free speech even  
 more vigorously than liberals do [1564].

So a national leader trying to keep a country together following an attack

should constantly remind people what they’re ﬁghting for. This is what the best  
 leaders do, from Churchill’s radio broadcasts to Roosevelt’s ﬁreside chats. In  
 more recent years, some countries have taken a bipartisan approach to terrorism  
 – as when Germany faced the Baader-Meinhof Gang, and Britain the IRA. In  
 others, politicians have given in to the temptation to use fearmongering to get  
 re-elected.

A study by the University of Alabama of over 200,000 articles on the 136

different attacks in the USA between 2005 and 2016 showed that attacks by Mus-  
 lims get 357% more news coverage than other terrorist attacks [1026]. Islamic

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 845 | Ross Anderson |

*26.3. TERRORISM*

extremists were labelled terrorists 78.4% of the time, whereas far-right extrem-  
 ists were identiﬁed as terrorists only 23.6% of the time. Political leadership

does matter. Perhaps the best recent response was that of New Zealand Prime  
 Minister Jacinda Ardern to the Christchurch shooting; she not only described it  
 immediately as terrorism but refused to name the shooter. On the other hand,  
 the Pittsburgh synagogue shooting was simply described as a ‘wicked act of  
 mass murder’ by the US President. In each case, the media followed [1335].

What are the dynamics here, and which approaches work best?

**26.3.3** **The role of institutions**

There’s a whole academic subject – *public-choice economics* – devoted to ex-  
 plaining why governments act the way they do, and for which one of its founders  
 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 explained by the incentives  
 facing individual public-sector decision makers. It’s natural for officials to build  
 empires as they’re ranked by their span of control rather than 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 – analysis of the incentives facing individual pres-  
 idents, congressmen, generals, police chiefs and newspaper editors, rather than  
 the potential gains or losses of a nation. We know it’s prudent to design in-  
 stitutions 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. What’s the equivalent for presidents and prime ministers?  
 How is the national interest even 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 politi-  
 cal process in turn is thus prone to speciﬁc types of failure. Intergenerational  
 bargaining is hard: it’s easy for politicians to borrow money to buy votes now,  
 and leave the bill with the next generation, who can’t vote yet. 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 [1182]. Washington insiders remarked that a similar  
 dynamic was involved in the decision to invade Iraq: although the 2001 invasion

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 846 | Ross Anderson |

*26.3. TERRORISM*

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, or much of a payoff to the defense industry either. Indeed,  
 USAF Colonel Karen Kwiatkowski retired at the start of the Iraq war, described  
 how intelligence assessments were politically manipulated, and later ran for  
 Congress [1113]. Similar things were said in the aftermath of World War 1,  
 which was blamed on the ‘merchants of death’.

An institution of particular concern must be the media, whether the old-

fashioned press or the social media that are taking over some of their functions.  
 ‘If it bleeds, it leads’, as the saying goes; bad news sells more papers than good.  
 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. And the  
 recommender algorithms of many social media platforms learn to promote fear  
 and outrage, as they increase the time people spend on the platform and the  
 number of ads they click on.

**26.3.4** **The democratic response**

Yet people also learn over time. The worldwide reaction to 9/11 was sharp;  
 it was more muted four years later, in July 2005, when four suicide bombers  
 killed 52 people on London’s public transport and injured about 700. The initial  
 response of the public was gritty resignation: ‘Oh, well, we knew something like  
 this was going to happen – bad luck if you were there, but life goes on.’6

And as populations learn, so might political elites. John Mueller has written

a history of the attitudes to terrorism of successive US administrations [1350].  
 Presidents Kennedy, Johnson, Nixon and Ford ignored terrorism. President

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 Iranian ‘students’ who’d  
 kidnapped US 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. In America, people got fed up with President Bush’s  
 fear-based policies and elected President Obama whose line was “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”. Much the same happened in  
 the UK, where Margaret Thatcher was re-elected twice after treating terrorists  
 as common criminals. Later, Tony Blair played the fear game, and his departure  
 from office was met with a sigh of relief; his successor Gordon Brown forbade  
 ministers from using the phrase ‘war on terror’, and David Cameron’s govern-  
 ment continued that. Mature voters prefer politicians who stand up to terrorists

6The 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.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 847 | Ross Anderson |

*26.4. CENSORSHIP*

rather than using them as props in their re-election campaigns.

The harshest teacher may be the coronavirus. For years, a pandemic has

been at the top of Britain’s risk register, yet far less was spent preparing for one  
 than on anti-terrorist measures, many of which were ostentatious rather than  
 effective. This misallocation of resources looks set to cost far more of us our lives  
 than any terrorist could have dreamed of. The US and UK governments justiﬁed  
 torture in the 2000s by talking of an al-Qaida cell stealing a nuclear bomb and  
 detonating it in New York or London. Yet a 10 kT atomic demolition munition  
 set off in a major city might cost 50–100,000 lives, compared with the 50–100  
 million who died in the 1918–19 pandemic. The rhetoric of terror puffed up the  
 security agencies at the expense of public health, predisposing governments in  
 America, Europe, India and Africa to disregard the lesson of SARS in 2003 –  
 unlike the governments of China, Singapore, Taiwan and South Korea.

**26.4** **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.” By the second edition, I noted that “copyright law has largely  
 stabilised”, and it was during 2008 that power over content distribution shifted  
 from the music majors and Hollywood to tech ﬁrms like Apple and Amazon. I  
 also noted that “censorship has become a much bigger issue over the past few  
 years”. Now, a decade later, censorship is front and centre. It has two faces:  
 state censorship, and content ﬁltering by service companies.

Rulers have long censored books, although the invention of the printing press

made their job a whole lot harder. When John Wycliffe translated the Bible into  
 English in 1380–1, the Lollard movement he started was suppressed along with  
 the Peasants’ Revolt. But when William Tyndale had another go in 1524–5,  
 printing let him spread the word so widely that the princes and bishops could  
 not suppress it. They had him burned at the stake, but by then over 50,000  
 copies of the New Testament had been printed, and the Reformation was under  
 way. After that upset, printers were closely licensed and controlled; things only  
 eased up in the eighteenth century.

Censorship nowadays is done for a variety of motives. Most countries block

images of child sex abuse; during the 1990s, as the dotcom boom got underway,  
 governments started looking for some handle on the Internet, and a view arose  
 that images of child sex abuse were about the one thing that all states could  
 agree should be banned. In due course the 2004 Cybercrime Convention obliged  
 signatory states to ban sexual images of under-18s. Most governments go further  
 and block some kinds of hate speech. Britain bans websites that ‘radicalise’  
 young people by glorifying terrorism. Finally, censorship is sometimes imposed  
 by the courts.

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. Changing the histor-

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 848 | Ross Anderson |

*26.4. CENSORSHIP*

ical record wasn’t possible when it consisted of physical copies in libraries, and  
 the centralisation of human knowledge in the servers of a small number of ﬁrms  
 – from Amazon’s e-book system to the servers of the major news organisations –  
 takes us, in some sense, back to the 15th century. It’s also easier for the author-  
 ities to observe the transmission of disapproved material, as they can monitor  
 electronic communications more easily than physical packages. On the other  
 hand, nowadays everyone can be a publisher; much of the really unpleasant  
 material online comes from millions of individuals posting sort-of anonymously  
 to social media, to the comment pages of newspapers, and to individuals whom  
 they wish to harass and intimidate. Censors have learned to harness this. While  
 a decade ago China had tens of thousands of people who took down dissident  
 speech, now they have millions of citizen volunteers who drown it out. Once,  
 speech was scarce, and the censors tried to silence the speaker; now it’s the  
 listener’s attention that’s scarce, and so different tactics work.

To tease out the issues, let’s look at some contexts.

**26.4.1** **Censorship by authoritarian regimes**

When I wrote the second edition of this book, I was cautiously optimistic that  
 the government of China would fail in its attempts to censor all online content.  
 However the authorities there have become steadily more effective at suppressing  
 any forms of organisation and human solidarity outside of party control.

By 2006, observers noted that online discussion of local news events had led

to the emergence of ‘public opinion’ that for the ﬁrst time was not in thrall to  
 media managers [1470]. China had 137 million Internet users then, including a  
 quarter of the population in the big cities, and ‘the Great Firewall of China’ was  
 already a complex system of controls giving defence in depth against a range of  
 material, from pornography to religious material to political dissent [1469]. The  
 defences work at three levels.

First, there are the perimeter defences. China’s border routers 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. Deep packet inspection at the  
 TCP level is used to identify emails and web pages containing forbidden words  
 such as ‘Falun Gong’; such connections are torn down. Ten years ago, much  
 of the work was done at this level. Nowadays, since most traffic is encrypted,  
 that’s not so easy. In 2020, the ﬁrewall started dropping TLS 1.3 traffic using  
 *Encrypted Server Name Indication* (ESNI) as this stops the censor telling which  
 subdomain the traffic’s going to; this amounted to over 30% of traffic by the  
 beginning of July [433].

Second, there are application-level defences, which now do much of the work.

Nowadays some services are blocked and some aren’t, depending on whether  
 the service provider is prepared to help the regime with both surveillance and  
 censorship. Google and Facebook are largely blocked; China has promoted

Tencent, Alibaba and Baidu instead. Now that the borders that matter most  
 are those of ﬁrms rather than of nations, the Chinese government has aligned  
 its industrial policy with its politics. This is the big change; we never believed  
 ten years ago that China would build an entire ecosystem of Chinese-owned

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 849 | Ross Anderson |

*26.4. CENSORSHIP*

online service providers to keep western inﬂuence at bay. Language provides  
 one barrier, but there are strong technical barriers too: the perimeter defences  
 now focus on blocking Tor and VPNs that could be used by Chinese residents  
 to use non-approved services.

Third, there are social defences. There were already 30,000 online police

a decade ago; now many more citizens have been engaged in the process, and  
 rather than trying to block all dissident speech the strategy is to swamp it. Loyal  
 citizens are expected to post lots of pro-regime comments and to ﬂame anybody  
 who criticises authority, whether local or national. A social credit system gives  
 people positive points for such pro-social behaviour, while they can lose points  
 for anything considered antisocial. Online monitoring is being integrated with  
 the monitoring of physical space, such as by CCTV cameras with face recog-  
 nition and emotion recognition – which is particularly aggressive in areas with  
 rebellious minority populations, such as the Tibetans and Uighurs. Since 2014,  
 a system in Sinkiang for ‘re-education’ has pioneered a fusion of techniques from  
 the western ‘war on terror’ and Maoist social control, leading to the internment  
 of hundreds of thousands of Muslims on the basis of a scoring system whose  
 inputs include whether a suspect prays regularly or has a VPN on their phone.  
 The U.S. Congress has denounced this regime for ‘crimes against humanity’:  
 dozens of the contractor companies have been placed on the sanctions list [359].

So China appears to be winning the censorship battle, using populist but

authoritarian techniques. Russia’s Internet is fairly open, and although the

government had an ally take over the main social network, and has organised  
 armies of trolls to shout down its opponents, the opposition politician Alexei  
 Navalny has his own YouTube channel with millions of viewers, and attempts  
 to censor Telegram have been met with street protests. Putin has fought back  
 with a ‘digital sovereignty’ law enabling him to order ISPs to install surveillance  
 and censorship equipment.

The Arab Spring has also been signiﬁcant. This series of uprisings started in

Tunisia in December 2010 after a street vendor, Mohamed Bouazizi, set himself  
 on ﬁre after an official conﬁscated his wares and humiliated him. Protests were  
 organised using Facebook and other social media, leading to the downfall of the  
 government, and spreading to neighbouring countries too. The government of  
 Egypt also fell, along with those of Libya and the Yemen; in Egypt’s case a  
 Google employee, Wael Ghonim, turned Internet activist after the police beat  
 a man to death in Alexandria on suspicion that he had video evidence of their  
 involvement in a drug deal. The government of Syria almost fell, but fought  
 back in a civil war that killed hundreds of thousands and displaced millions.  
 A number of other Arab countries, such as Bahrain, suffered signiﬁcant unrest  
 and cracked down. As I write in 2020, only Tunisia has managed the transition  
 to democracy. In Egypt, one military dictator has been replaced by another;  
 Libya is in chaos, and Yemen, like Syria, is racked by war. The lesson drawn by  
 the world’s autocrats is that, to stay in power, they’d better study the methods  
 used by China. Arab countries do censor the Internet (as do most of the less-  
 developed countries) but their infrastructure is still fairly easily defeated using  
 VPNs or Tor. They also buy in kit for both bulk surveillance and targeted work;  
 for a description of how the UAE hired US mercenaries to set up an equivalent  
 of the NSA, see Bing and Schectman [247].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 850 | Ross Anderson |

*26.4. CENSORSHIP*

To what extent was the Arab Spring a function of technology, and to what

extent was this just marketing hype put out in 2011 by companies like Facebook  
 and Google while things seemed to be going well? It’s unclear. Some of the  
 populations that rose up made little use of the Internet, particularly those of  
 Libya and the Yemen; on the other hand, a revolt in Burma in 2007 was catalysed  
 by the Internet, even though only 1% of the population had access [1471]. In  
 the Arab world, the Qatari TV station Al-Jazeera may have done more work  
 than the Internet, by showing news videos of uprisings elsewhere in the region.

**26.4.2** **Filtering, hate speech and radicalisation**

Democracies’ laws on hate speech vary widely. At one end, the USA has con-  
 stitutional protection for free speech; so do France and Germany. But inter-  
 pretations differ. France and Germany both prohibit the sale of Nazi memo-  
 rabilia, and hate speech (‘Volksverhetzung’) has been a crime in Germany for  
 decades. In January 2018 the authorities started enforcing it against online ser-  
 vice providers, with the threat of a ﬁne of e50m if any service provider with  
 more than 2m customers doesn’t take down any such material within 24 hours.  
 Whatever the service companies say about the cost of taking down bad stuff,  
 the German example shows they can do it when they have to. Many countries  
 now ban terrorist material and extreme violence, the deﬁnition of which is never  
 straightforward. It might seem a good thing to ban not just beheading videos  
 but all videos of murder, such as drug gangs shooting a customer who didn’t  
 pay his debts. But it gets complex quickly. Platforms that enforce such a policy  
 end up deleting evidence, both of local killings and of human-rights violations  
 overseas.

Already much of the material you put online gets ﬁltered automatically to

look for material that’s forbidden by local laws, or by a platform’s terms of  
 service. Facebook’s former CISO Alex Stamos described the tension between  
 privacy and censorship as a spectrum: people expect end-to-end encrypted chat  
 such as WhatsApp to be private rather than censored, and broadcast media to be  
 censored rather than private, with the difficult stuff in the middle, like Facebook  
 groups. By now, most social media are censored. The platforms vary widely;  
 Facebook is perhaps the tightest, and bans even nudity7; though it is much  
 more forgiving of hate speech from President Trump than from others, and in  
 return appears to receive much less attention on the antitrust front [1790]. Au-  
 thoritarian countries are becoming more aggressive about forcing service ﬁrms  
 to block content they deem to be illegal; for example, Facebook’s service was  
 slowed to a crawl in Vietnam in early 2020 until the company agreed to suppress  
 dissent [1506].

Behind the AI systems that try to spot forbidden content are thousands of

content moderators. Filtering is expensive, and the costs are not just ﬁnan-  
 cial, but human; we’ve seen an increasing number of news articles about the  
 psychological toll on staff who have to spend all day looking at videos of gang  
 murders and terrorist beheadings, animal cruelty, child abuse, and other un-

7Facebook bans photos of female nipples but not male ones, so dozens of naked women

demonstrated in 2019 in New York holding pictures of men’s nipples over their own; men and  
 women demonstrated with pictures of female nipples [616].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 851 | Ross Anderson |

*26.4. CENSORSHIP*

pleasantness [1438]. Many moderators are in less developed countries; just as  
 we dump a lot of unpleasant refuse there, we also dump a lot of the Internet’s  
 nastiest trash [414]. It’s also problematic to outsource censorship to large ser-  
 vice monopolies. They act in a quasi-judicial manner, regulating the speech  
 of billions of people but without the transparency and due process we expect  
 of government decisions. The world sees them allowing abuse by the rich and  
 powerful while ignoring the weak. Perhaps it was inevitable that ﬁrms would  
 snuggle up to power and then try to direct political speech; this has become a  
 factor in the backlash against the whole tech sector.

One focus of debate is section 230 of the US Communications Decency Act

of 1996 (CDA) which states that ‘No provider or user of an interactive computer  
 service shall be treated as the publisher or speaker of any information provided  
 by another information content provider’ so platforms cannot be held liable  
 for bad stuff provided by users; it also left platforms free to remove anything  
 ‘obscene, lewd, lascivious, ﬁlthy, excessively violent, harassing, or otherwise  
 objectionable.’ When it passed the CDA, Congress was concerned that ﬁrms  
 that moderated content could be treated as publishers and held liable for all of  
 it (including copyright infringement and libel) while ﬁrms that didn’t would be  
 treated as distributors and escape liability. How could we get a civil internet  
 without killing innovation? Section 230 made ﬁrms like YouTube and Facebook  
 possible, but protected sites whose business model is based on revenge porn,  
 defamation, or getting a cut of illegal gun sales [1419]. It also enabled service  
 ﬁrms to acquire some of the powers of states. Back then, the Internet had

10-20m users, mostly geeks; now most human activity is online, and it’s not  
 sustainable for a handful of American ﬁrms to act as censor, prosecutor and  
 judge for 200-odd countries. As a result the CDA, and similar laws elsewhere,  
 are starting to be trimmed: in the USA in 2018 with laws on sex trafficking and  
 in Europe with a 2019 law on copyright [1598]. The tensions can only get worse.

When making laws to restrict speech, it’s a good idea to stop and look at the

historical context. Tim Wu’s ‘The attention merchants’ [2050] is a history of  
 propaganda since the 1830s when the ﬁrst mass-market newspapers appeared,  
 stuffed with grisly crime reports and adverts for patent medicines; this gave  
 politicians their ﬁrst industrial mass-market channel. Radio followed, and was  
 used skilfully by Hitler. TV was next, and its nature was shaped by advertising;  
 people invented quiz shows, soaps and much else to grab eyeballs. A second  
 useful perspective is Yochai Benkler’s ‘Network propaganda’ which analyses the  
 2016 US election campaign. He traces the history of political polarisation and  
 argues that the root cause of the outcome wasn’t technology or Russian inter-  
 ference so much as the asymmetric media systems of right and left that have  
 developed over the past 20 years; the left and centre-right are fact-based while  
 the right is a propaganda feedback loop [227]. A third perspective is the cri-  
 tique of recommender systems by former Googler Tristan Harris: the platforms’  
 algorithms learn that to maximise the time people spend on site, they should  
 be fed articles that stoke fear, anxiety and outrage.

The reactions of governments to fake news are mostly ineffective. The most

capable may be Finland, which has been a target of Russian propaganda since  
 Tsarist times. Its government has been promoting critical thinking and me-  
 dia literacy in schools and elsewhere since 2014, making it every citizen’s job

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 852 | Ross Anderson |

*26.4. CENSORSHIP*

to spot and counter information that’s designed to sow division. In Britain

we have laws designed to please tabloid newspapers rather than to push back  
 against them. Schoolteachers and university professors are supposed to report  
 students who seem at risk of being radicalised, and have procedures to ﬁgure  
 out whether seminars or other talks could radicalise them; there are also laws  
 against online material that might lead them astray. If such an approach were  
 applied consistently it might lead to banning much of the literature produced  
 or funded by religious institutions from Saudi Arabia [1263], but action against  
 our largest arms export customer isn’t going to happen anytime soon. White  
 supremacists are at least as much of a threat, having murdered a member of the  
 UK parliament during the Brexit campaign; but our government is much less  
 keen on cracking down on them, and the people who broke the law by spend-  
 ing too much money on that campaign (including Russian money) did not end  
 up in jail, but at the heart of government. In general, Internet censorship lets  
 the government claim it’s doing something, but doesn’t really work well, and  
 undermines whatever our diplomats might say about freedom of speech to the  
 world’s despots. I’d prefer to enforce existing laws on incitement to murder (and  
 campaign ﬁnance, leave other political material in the open, let the police mon-  
 itor the traffic to the worst of the sites, and train them to use the existing laws  
 better [642]. In the longer term, the key is education, as Finland has shown.

As for targeting Muslim students, this runs directly against the criminologi-

cal evidence. The few UK students who’ve signed up to extremist organisations  
 have been those who experienced lack of respect socially, perhaps being rejected  
 by their peers, were searching for identity but couldn’t ﬁnd it in the religion of  
 their parents – then fell in with small groups of other disaffected youngsters.  
 They came under the inﬂuence of radical preachers, who offered ideals, com-  
 munity, kinship, caring and brotherhood. The radicalisation of white boys into  
 white supremacist groups is not hugely different. Research by Max Abrahms  
 also shows that terrorists mostly joined their movement in a search for social sol-  
 idarity; that’s why they recruit from lonely young men rather than from among  
 political activists. Their groups become institutions to which members cleave,  
 rather than agents of change; that’s why they can respond to sensible peace  
 offers with increased violence, and indulge in fratricidal conﬂict with similar  
 groups [6]. In fact, as Lydia Wilson pointed out after interviewing large num-  
 bers of young people who’d gone to Syria to join Daesh and ended up in Kurdish  
 jails, the process whereby young men (and occasionally women) ﬁnd their iden-  
 tity by joining terror groups or crime gangs is no different from ﬁnding identity  
 by joining religions, sports clubs or dance bands [2022]. Zo¨e Quinn’s more re-  
 cent experience of angry online mobs during the Gamergate drama, which we  
 discussed in section 2.5.1, draws much the same conclusion [1567]. The people  
 who join extreme organisations in search of social solidarity need to think of  
 themselves as the good guys; you need to undermine that, and you can’t do it  
 by excluding them.

For all these reasons, it is unwise to model terrorist groups as rational eco-

nomic actors, and just as unwise to try to prevent radicalisation on similar as-  
 sumptions. The best approach is to have an environment that doesn’t exclude  
 people – one in which students get to know others from different backgrounds on  
 the staircase in their residence, in small teaching groups, and in project groups  
 – and with hundreds of sports and student societies to choose from, so everyone

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 853 | Ross Anderson |

*26.5. FORENSICS AND RULES OF EVIDENCE*

can ﬁnd a gang to belong to. That’s how great universities have always worked  
 anyway.

**26.5** **Forensics and Rules of Evidence**

Our last main policing topic is how information can be recovered from comput-  
 ers, mobile phones and other electronic devices for use in evidence. This has  
 been getting more problematic over the past twenty years because of ﬁrst, the  
 sheer volumes of data; and second, the fact that while much of it is seized from  
 platforms such as mobile phones and laptops, more and more of it is held on  
 cloud services that require paperwork and often quite substantial delays. The  
 rising costs and operational difficulties lead to more selective law enforcement,  
 with whole categories of online harms where states rarely intervene. As a result,  
 many bad people, from cybercriminals to creeps, bullies and extremists, operate  
 online with near-total impunity.

**26.5.1** **Forensics**

Computer forensics has been a growing problem for the police since at least the  
 1980s; by the early 2000s both the facilities and the staff training were hopelessly  
 behind. The move of everything online during the 2010s has made matters still  
 worse. When the police raid even a small-time drug dealer nowadays, they can  
 get half-a-dozen mobile phones, several laptops, and gadgets such as a navigator  
 or a Fitbit that hold his location history. The suspect may also have dozens of  
 accounts for webmail, social-networking sites and other services. We have 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 [1192], and even use this to ﬁgure out which parts of a photo might have  
 been tampered with.

The use of digital material in evidence depends, however, on both law and

economics. 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. That means using trustworthy tools to make evidential copies of  
 data; to document everything that’s done; and to have means of dealing appro-  
 priately with any private material that’s found (such as privileged lawyer-client  
 emails, or the trade secrets of a suspect’s employer). The traditional approach  
 to computer forensics is described in standard textbooks such as Sammes and  
 Jenkinson [1644].

Since the world moved to smartphones and cloud services, the centre of

gravity has shifted to a handful of companies that sell mobile forensics tools to  
 police and intelligence agencies. They supply kiosks to police forces that enable  
 unskilled officers to download mobile-phone contents, and to use the tokens on  
 them to download data from suspects’ accounts in the cloud. Some police forces  
 are working hard to get the legal issues sorted out (such as Police Scotland, who  
 don’t use ‘cloud forensics’ without a warrant) but many just grab and keep all  
 the data.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 854 | Ross Anderson |

*26.5. FORENSICS AND RULES OF EVIDENCE*

At the more sophisticated end of the trade, there’s an arms race between

forensics and countermeasures. Police forces used to always turn PCs off, so  
 that hard disks could be copied for prosecution and defence lawyers. Phishing  
 gangs exploited this by making their phishing software memory-resident, so that  
 the evidence would self-destruct. And since laptops started to ship with decent  
 encryption, the risk is multiplied. By 2013, when the FBI arrested Ross Ulbricht  
 – the creator of the Silk Road underground drugs market – one agent’s mission  
 was to put his hand in the laptop to stop Ulbricht closing it, and he already had  
 the right kind of power cord to plug it in [482].

In the old days, people – and small businesses – who got caught up in a

police investigation and had their computers seized could wait years to get them  
 back, even if they were just a bystander, or if they were charged but eventually  
 acquitted. Nowadays, people have seizure-proof offsite backup thanks to cloud  
 services. These services also make life harder for the police where suspects’

material sits on servers overseas. The ﬁght between Facebook and GCHQ I  
 referred to in Section 26.2.8 arose when two terrorists murdered a British soldier,  
 Lee Rigby, near Woolwich barracks in March 2013 by running him over with  
 a car and then stabbing him. While they were at the crime scene, facing off  
 against the police, Facebook fed the police and security services data instantly,  
 but once the two had been shot and were in custody in hospital, requests had to  
 go through the UK/US mutual legal assistance treaty. This involves the police  
 ﬁling forms at the US Embassy in London that are then considered at length in  
 the Department of Justice in Washington. The forms are often sent back as UK  
 police staff don’t understand US law and complete them incorrectly. Even where  
 everything goes right, it can take six weeks for the FBI to serve the paperwork  
 on Facebook in Menlo Park, California, and collect the data. So we found we’d  
 gone from a world in which, after a raid, the police would have your data and  
 you wouldn’t, to one in which you still have your data but the police don’t –  
 unless you cooperate, or unless you’re a serious enough bad guy to be worth the  
 time and attention of diplomats.

Since about 2017, there’s been a third option: cloud forensics. What this

means in practice is that your phone is hacked by the police’s forensic kiosk  
 and gives up access tokens to your email, your photos, your Facebook and your  
 other cloud services. Some UK police forces think this is wonderful; they treat  
 the downloaded data as ‘data at rest’ as if it had been found on the phone itself  
 and keep it forever. Others consider that it can only be obtained by consent or  
 with a further warrant. The incentives to grab cloud data are strong, but the  
 mechanisms involved (phone hacking followed by impersonation of the user) are  
 likely to strike most citizens as unfair. And ever more devices are now acquiring  
 an attached cloud service and an app. Will the police investigate traffic offences  
 in future by seizing the driver’s phone and using it to download the car’s logs  
 from the manufacturer’s server? This is a current policy topic in 2020: for

example, the UK privacy regulator called for a statutory code of practice to  
 be developed [958]. As it happens, courts already have some rules about what  
 evidence can be used.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 855 | Ross Anderson |

*26.5. FORENSICS AND RULES OF EVIDENCE*

**26.5.2** **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 as hearsay. Different legislatures tackled this  
 differently. In the US, most of the law is found in the Federal Rules of Evidence  
 where 803(6) allows computer data to be introduced as records ‘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... unless the

source of information or the method or circumstances of preparation indicate  
 lack of trustworthiness.’ The UK is similar, and the rules of electronic evidence  
 in the common-law countries (including Canada, Australia, South Africa and  
 Singapore) are analysed by Stephen Mason [1236].

The deﬁnition of ‘writing’ and ‘signature’ is of interest, and varies by juris-

diction. In Britain, courts took the view that an email is writing just as a letter  
 is: the essence of a signature is the signer’s intent [2042, 2043]. The US approach  
 was similarly pragmatic. In 2000, 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 press-  
 ing 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 [669]. This makes  
 click-wrap licenses perfectly valid in America. Nonetheless, Docusign has built  
 a business offering digital signatures as a service for ﬁrms who want something  
 a bit more showy.

In Europe the Electronic Signature Directive, which came into force in 2000,

gave special force to an *advanced electronic signature*, which basically means  
 a digital signature generated with a smartcard or hardware security module.  
 Europe’s smartcard industry thought this would earn them lots of money, but  
 it languished for years. In many countries, 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. However, if I ever accept an advanced electronic signature device,  
 then I become liable to anyone in the world for any signature that appears to  
 have been made by this device, regardless of whether or not I actually made it!  
 This, coupled with the facts that smartcards don’t have a trusted user inter-  
 face and that the PCs which most people would use as an interface are easily  
 subverted, made such electronic signatures unattractive. Following further lob-  
 bying, Europe updated the law with the eIDAS Regulation (910/2014) which  
 tries to improve the incentives for adoption, by requiring all organisations deliv-  
 ering public services to accept electronic signatures since 2018. A number of EU  
 countries now insist that you use such a signature to ﬁle your taxes, rather than  
 permitting it. There’s a hierarchy whereby a signature can be ‘advanced’ or  
 ‘qualiﬁed’ depending on the certiﬁcation of the technology used, and a qualiﬁed  
 electronic signature must be accepted for any purpose for which a handwrit-  
 ten signature was previously required. Dozens of signature creation products  
 were duly certiﬁed and brought to market. The assurance mechanisms used

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 856 | Ross Anderson |

*26.5. FORENSICS AND RULES OF EVIDENCE*

to certify such products are defective in many ways, as I will discuss later in  
 section 28.2.7.2. The European Commission duly made a reference implementa-  
 tion available to help governments get started with verifying all the signatures;  
 in 2019 bugs were discovered in it that would let any citizen impersonate any  
 other [429].

**26.5.3** **What goes wrong**

Many things can go wrong with police investigations, and the computerised kind  
 are no different. An old pitfall is relying on evidence extracted from the sys-  
 tems of one party to a dispute, without applying enough scepticism about its  
 dependability. Recall the Munden case described in Section 12.4.3. 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 state-  
 ments were ruled inadmissible and the case collapsed. The same has happened  
 multiple times since then, including two terror cases involving curfew tags which  
 I discussed in section 14.4.

The worst failure of computer evidence of which I’m aware was Operation

Ore. After the US Postal Service raided a porn site in Texas, they discovered  
 hundreds of thousands of credit card numbers that they thought had been used  
 to buy child sex abuse images, and some eight thousand of these were from  
 UK cardholders. Some 3,000 homes got raided in the early 2000s, until the

police ﬁnally realised that most of the cardholders were probably victims of  
 card fraud. The vice squad used unskilled staff in their initial analysis of the  
 seized material, and were slow to learn – because they were ﬁxated on getting  
 porn convictions, because they didn’t have the forensic capacity to process all  
 the seized computers quickly, because they didn’t understand card fraud (they  
 preferred to leave that to the banks) and because of politics (Prime Minister  
 Tony Blair himself had ordered the raids). So several thousand men had their  
 lives disrupted for months or even years, and the sad story of police bungling and  
 cover-up is told by Duncan Campbell in [375, 376]. For some, the revelation  
 that the police had screwed up came too late; over thirty men, faced with  
 prosecution, killed themselves. At least one of them, Commodore David White,  
 commander of British forces in Gibraltar, appears to have been innocent [886].  
 The gangsters in Indonesia and Brazil who organised and photographed the  
 child abuse do not seem to have been seriously pursued. America handled this  
 case much better. Some 300,000 US credit card numbers were found on the  
 same servers, but US police forces used the data for intelligence rather than  
 evidence, identifying suspects of concern – such as people working with children  
 – and quietly investigating them. Over a hundred convictions for actual child  
 abuse followed.

Sometimes systems are deliberately designed to not provide evidence; an

example is the policy adopted by Microsoft after embarrassing emails came out  
 during their antitrust battles with the US government in the 1990s. The ﬁrm  
 reacted with a policy that all emails are discarded after a ﬁxed period of time  
 unless someone takes positive action to save them, and many other ﬁrms followed

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 857 | Ross Anderson |

*26.6. PRIVACY AND DATA PROTECTION*

suit. Another example is the move by service ﬁrms in the mid-2010s to adopt  
 end-to-end encryption, so they don’t have access to customer message traffic  
 and don’t have to employ hundreds of lawyers to deal with requests for it.

The biggest problem with computer forensics, though, has always been sheer

lack of money. Despite all the cool tricks that intelligence agencies can use to  
 extract information from computer systems, a county drugs squad often won’t  
 have the budget to do even basic computer forensics except for occasional big  
 cases. They can’t even afford to send every wrap of white powder off to the  
 lab to see if it’s illegal or not. In normal cases, they were only able to use

digital material that was easily available, such as copies of messages on the  
 phones of cooperative witnesses, until mobile-phone forensic kiosks came along  
 around 2016–8 and made masses of data available from seized handsets at low  
 marginal costs. Hence the huge pressure to use the kiosks, even before robust  
 legal procedures could be developed. And, of course, the use of forensic tools  
 by regular police officers with no specialist training raises the risk of future  
 miscarriages of justice. Judicial education is also an issue; few judges understand  
 probability theory, and indeed the UK Court of Appeal has refused to accept  
 analysis of evidence based on Bayes’ theorem. Quite apart from the injustice of a  
 court system that denies mathematics, there’s the practical issue that defendants  
 faced with computer evidence that’s the result of bugs, or simply misrepresented,  
 may have no practical way to prove their innocence.

**26.6** **Privacy and Data Protection**

Privacy and data protection are one subject on which the USA and Europe have  
 taken separate paths. A concentrated interest (such as business wanting to use  
 our personal information to exploit us) usually prevails over a diffuse interest  
 (such as the desire of individuals to keep control of our personal information),  
 and the usual remedy is law. The remedy is imperfect because the concentrated  
 interest lobbies the lawmakers and will attempt to capture any regulator they  
 set up. And Europe, for historical reasons regulates more than America does.  
 The resulting gulf was highlighted powerfully in May 2014 when, in the USA, the  
 Presidential Council of Advisers on Science and Technology (PCAST) published  
 “Big Data: A Technological Perspective” [1546]. This report, whose authors  
 included Google’s Eric Schmidt and Microsoft’s Craig Mundie, painted a picture  
 of a world full of smart objects connected to cloud servers, with an ecology in  
 which sensors reported to cloud analytics which in turn provided information to  
 users, such as advertisers. PCAST warned that the spread of voice and gesture  
 interfaces meant that pretty soon, every inhabited space on the planet would  
 have microphones and cameras in it, whose output would be processed centrally  
 for energy efficiency. They argued that privacy controls could not be imposed  
 on the sensors, as they’ll be too numerous; that they should not be imposed on  
 the central service aggregators; and that the controls would therefore have to  
 fall on how the information was used.

Less than two weeks later, the European Court of Justice disagreed. A

Spanish lawyer, Mario Costeja Gonz`alez, had complained that searches for his  
 name brought up two ancient press reports of an auction sale of his repossessed

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 858 | Ross Anderson |

*26.6. PRIVACY AND DATA PROTECTION*

house. He asked the Spanish data protection authorities to order Google to stop  
 serving these results as they were out of date and no longer relevant. Google  
 argued that it was just reporting the contents of a newspaper. The case went  
 to the ECJ, which found in Gonz`alez’ favour, creating what the media colour-  
 fully if inaccurately called a ‘right to be forgotten’, later codiﬁed into Europe’s  
 General Data Protection Regulation from 2018. Google and other online ser-  
 vice providers had to set up mechanisms whereby people could complain about  
 search results that are ‘inadequate, irrelevant or no longer relevant, or excessive  
 in relation to the purposes for which they were processed’ and have them re-  
 moved. The mechanisms are contentious: Gonz`alez’ results are removed from  
 Google searches in Spain, but European regulators want them removed globally.  
 Google’s supporters claim that this would interfere with its right to free speech  
 in the USA.

How did this rift come about?

**26.6.1** **European data protection**

Fear of technology undermining privacy isn’t a recent development. As early  
 as 1890, Justices Warren and Brandeis warned of the threat to privacy posed  
 by ‘recent inventions and business methods’ – speciﬁcally photography and in-  
 vestigative journalism [1988]. After banks, tax collectors and welfare agencies  
 started using computers in the early 1960s, people started to worry about the  
 privacy implications if all our transactions could be collated and analyzed. In  
 Europe, business argued that only government could afford enough computers  
 to be a serious privacy threat. This became a human-rights issue, given living  
 memory of the Gestapo in most European countries and of communist secret  
 police forces in the East8.

A patchwork of data protection laws started to appear starting with the Ger-

man 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 inappro-  
 priate 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 ineffec-  
 tive against them. Following a voluntary code of conduct promulgated by the  
 OECD in 1980 [1476], data protection was entrenched by a Council of Europe  
 convention in January 1981, which entered into force in October 1985 [475].  
 Although strictly speaking this convention was voluntary, many states signed  
 up to it for fear of losing access to data-processing markets. It required cer-  
 tain minimum safeguards for *personal information*, which generally means any  
 data kept on an identiﬁable human being, or *data subject*, such as bank account

8In Germany, privacy is now entrenched in the constitution, and 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 from Muslim-majority countries – even though no-one  
 was arrested as a result. It ruled that such exercises could be performed only in response to  
 concrete threats, not as a precautionary measure [344].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 859 | Ross Anderson |

*26.6. PRIVACY AND DATA PROTECTION*

details and credit card purchasing patterns. Data subjects have the right to  
 inspect personal data held on them, have records changed if inaccurate, un-  
 derstand how they’re processed, and in many cases prevent them being passed  
 on to other organizations without their consent. Almost all commercial data  
 are covered. 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 payment instructions, were being  
 copied to the Department of Homeland Security without the knowledge of data  
 subjects; SWIFT eventually agreed to stop processing European data in the  
 USA [1485, 1486].

The quality of implementation varied widely. In the UK, for example, Mar-

garet Thatcher unashamedly did as little as possible to comply; a data protection  
 body was established but starved of funds and technical expertise, and many ex-  
 emptions were provided for both government and industry9. In Germany, which  
 had written a right to privacy into its post-war constitution, the data protection  
 bodies became proper 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 and Ireland, followed the British one.

By the early 1990s the difference between national laws was creating barriers

to trade. Some businesses avoided controls altogether by moving their data

processing to the USA. So data protection was ﬁnally elevated to the status of  
 European Union law in 1995 with a Data Protection Directive [647]. This set  
 higher minimum standards than before, with particularly stringent controls on  
 highly sensitive data such as health, religion, race and political affiliation. It  
 also set out to prevent personal information being shipped to ‘data havens’ such  
 as the USA in the absence of comparable controls enforced by contract or treaty.

The British implementation was again minimal, falling far short of European

requirements [597]. For example, data controllers could pretend that lightly-  
 anonymised information was no longer personal information, just so long as  
 they themselves did not possess the auxiliary data needed to re-identify it. The  
 Information Commissioner’s Office was overwhelmed, and severely conﬂicted  
 as a result of being simultaneously the public sector’s adviser on privacy and  
 the privacy enforcer; the enforcement arm was reluctant to take action against  
 systems blessed by their colleagues in the advisory arm. Ireland’s enforcement  
 was even weaker – its industrial strategy for the past 50 years has been to attract  
 US ﬁrms’ European headquarters. So in addition to having low corporate taxes,  
 the Dublin government located its data protection office in Portarlington, a town  
 of less than 10,000 people, gave it only 30 staff, and did not allow it to publicise  
 the results of investigations.

This so annoyed countries with tighter privacy laws such as France and Ger-

many that they pushed for the General Data Protection Regulation (GDPR),  
 which passed in 2016 and came into force in May 2018. This was the most heav-  
 ily lobbied piece of European legislation ever, with over 3,000 amendments dis-  
 cussed in committee in the European Parliament [82]; it was helped over the line

9In 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.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 860 | Ross Anderson |

*26.6. PRIVACY AND DATA PROTECTION*

by the Snowden disclosures, although it had been cooking for some time before  
 that10. GDPR took direct effect in all EU member states, removing the wriggle  
 room for Britain or Ireland to introduce loopholes; but lobbyists got quite a  
 few of those in the Regulation already (particularly for ‘research’, whether of  
 the scientiﬁc or marketing kind). The main effect on normal businesses is to  
 force them to document all their uses of personal information and write down,  
 in advance, what the legal basis is for each of them; it’s not enough to try and  
 ﬁgure things out once challenged. For information-intensive businesses, the im-  
 plications could be more signiﬁcant, and there have been fascinating disclosures  
 of how Facebook executives lobbied to amend the regulation – effectively using  
 the Irish prime minister, Enda Kenny, as their advocate in Brussels [1418].

Despite the many carve-outs inserted by the lobbyists, GDPR is still pro-

viding regulators with tools to push back. France ﬁned Google e50m for failing  
 to tell users enough about its data consent policies or give them enough control  
 over how their information is used [1534]. The fact that consent can no longer  
 be coerced or presumed may become a big deal, and there are many further  
 cases in the pipeline.

**26.6.2** **Privacy regulation in the USA**

In the USA, business has mostly managed to persuade government to leave  
 privacy largely to ‘self-regulation’. Although there’s a patchwork of state and  
 federal laws, they are application-speciﬁc and fragmented. In general, privacy in  
 federal government records and in communications is regulated, while business  
 data are largely uncontrolled. The few islands of regulation include 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 US 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. Most states also have a breach disclosure law, which requires ﬁrms  
 suffering any security failure that compromises residents’ personal information  
 to inform them about it. Several torts also provide a basis for civil action in a  
 surprising number of circumstances; for a survey, see Daniel Solove [1801].

The ﬁrst case that started to put privacy on CEOs’ radar came in 2006,

when Choicepoint paid $10m 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’ [671]. In  
 2007, it came out that the store chain TJ Maxx had had 45.7 million customers’  
 credit card details stolen [1159]; Albert Gonzales got 20 years in prison for this  
 in 2010, and it’s reckoned that the breach cost the company $800m. The FTC  
 sued Facebook over deceptive changes to privacy settings and settled in 2011,  
 just before its IPO, requiring it to get user consent for certain changes and

10Snowden revealed some egregious abuses such as the large-scale collection of by GCHQ

of Yahoo video chats in Operation Optic Nerve, including intimate video chats [14].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 861 | Ross Anderson |

*26.6. PRIVACY AND DATA PROTECTION*

|  |
| --- |
| subjecting it to 20 years of audits [181]. The real shock to CEO-land came  when Target’s CEO, Gregg Steinhafel, was ﬁred in May 2014 following a hack  of more than 100m credit card numbers the previous December; the CIO wasalso replaced [702]. The C-suite carnage has continued, both in the USA11 andelsewhere12 moving cybersecurity steadily up the corporate agenda. |

In 2018, California passed a consumer privacy law, the California Consumer

Privacy Act (CCPA). This followed a privacy ballot initiative which, if it had  
 gone to a ballot and passed, would have entrenched an even tougher privacy  
 law. The ballot in turn followed the Cambridge Analytica scandal where the  
 Facebook data of 87 million users was harvested without their knowledge or  
 consent and used to target behavioural advertising during the 2016 election  
 campaign. The big tech companies’ defence was to negotiate the new law instead  
 of the ballot initiative, so they could have it amended later, or even trumped  
 by a Federal law. CCPA is somewhat similar to European data-protection law:  
 it empowers consumers to request the deletion of personal information, opt out  
 of its sale, and access it in a format that enables its transfer to third parties.  
 The European right to be forgotten is a non-starter thanks to the US First  
 Amendment. CCPA can be enforced by the state attorney general but also by  
 private action. A really important policy question now is whether this law is  
 progressively copied by other states, or whether Big Tech manages to emasculate  
 it13. But the USA is not the only serious player here.

**26.6.3** **Fragmentation?**

Since 1998, European law has forbidden companies from sending personal data  
 to organizations in countries where the law does not provide comparable pro-  
 tection or other safeguards – in practice, that means America and India. The  
 ﬁrst attempt to resolve this was the *Safe Harbour Agreement* whereby a data  
 processor in America or India would promise their European customer to abide  
 by European law. In 2000, the European Commission adopted an executive  
 decision to the effect that this would give ‘adequate protection’. However, it left  
 no practical recourse for EU citizens who felt their rights had been violated.

The case that killed Safe Harbour was brought by Max Schrems, an Austrian

lawyer, against Facebook. Following the Snowden revelations, he argued that  
 for Facebook in Ireland (its EU headquarters) to pass his data to the USA for  
 processing was unlawful, as the law and practice of the United States offer no  
 protection against surveillance by the public authorities, speciﬁcally the NSA,  
 which can collect it all via Prism. The European Court of Justice agreed and  
 in 2015 it struck down the Safe Harbour principles. The USA and the EU then  
 agreed to replace them with a fresh arrangement, called Privacy Shield, which

11Amy Pascal of Sony in 2014, Walter Stephan of FACC in 2016, Richard Smith of Equifax

in 2017; and maybe we can note Marissa Meyer of Yahoo who forfeited her bonus and stock  
 in 2017, and perhaps even Travis Kavalnick of Uber whose successor publicised a hack that  
 had been covered up.

12Dido Harding of TalkTalk, UK, in 2017; Bruce Liang of Integrated Health Information

Systems, Singapore, in 2019; and maybe we can count Martin Winterkorn of VW and Rupert  
 Stadler of Audi too, who presided over the company hacking its car emissions.

13Their lobbyists are already attacking it, but as I write in 2020, there’s a ballot initiative

that would entrench it in California law and put it beyond the grasp of state legislators.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 862 | Ross Anderson |

*26.6. PRIVACY AND DATA PROTECTION*

adds and ombudsperson to whom an EU citizen can complain if they think the  
 NSA might have spied on them [1474]; Max too this to the European Court  
 of Justice, which duly struck it down in July 2020[1683]. The defendant was  
 the Irish Data Protection Commissioner, who spent almost e3M defending the  
 position that she had the right to look the other way as US tech ﬁrms with  
 their EU headquarters in Ireland ride roughshod over privacy law. The court  
 also ruled that privacy authorities have a duty to take action when they receive  
 a complaint. It also made clear that the NSA’s right under US law to get free  
 access to the data of people who are not US persons is not consistent with US  
 ﬁrms keeping data on EU citizens under US custody and control14.

Many companies that process data in the USA had in the meantime fallen

back on contract, forcing customers to agree to their personal data being shared  
 before they do business with them. This has a long and sordid history (it’s how  
 medical insurers get away with selling your data to drug companies), and the  
 ECJ allowed the continued use of *standard contractual clauses* (SCCs) to protect  
 data. But this isn’t straightforward. First, the data controller has to establish  
 that there’s an adequate level of protection in the country where the data will  
 be held, and second, you can’t simply impose such terms on consumers in the  
 world of the GDPR as coercive consent is speciﬁcally disallowed. It is hard

to see how US ﬁrms can establish adequacy when US law provides unfettered  
 access to foreigners’ data on US soil and the Snowden disclosures document the  
 systematic use (and, from the EU law viewpoint, abuse) of this access.

So this is developing into a real ﬁght, with real consequences for how and

where the world’s server farms are located and controlled. Some of the better-  
 informed ﬁrms assume that they will eventually have to process European data  
 in Europe and under European law; Microsoft put a data centre in Germany  
 under the control of a German trustee for a couple of years, but then changed  
 its mind, while Google has done its privacy research and development for some  
 years in Munich. And public opinion in the USA isn’t that different from Europe:  
 most Americans think their personal data is less secure now, that the risks of  
 surveillance capitalism outweigh the beneﬁts, that they don’t understand what’s  
 going on, that they have no control and neither companies nor government are  
 accountable for abuse, but that they just don’t have any alternative. Oh, and  
 20% suffered some kind of online fraud in the last twelve months [144].

Meanwhile, data-protection law is pushing into new areas where it gives a

|  |
| --- |
| way of responding to abuses. For example, after the Brexit referendum, the UK Information Commissioner ﬁned Facebook £500,00015 after they let Cambridge  Analytica harvest personal data on 87 million people worldwide, and used this to  target election ads in both the Brexit referendum and the US 2016 presidential  election [957]. As many modern practices in marketing and in political propa-  ganda involve o↵ences under data-protection law, this gives scope for regulatory |

14There is also a case pending at the European Court of Human Rights, brought by Big

Brother Watch against US mass surveillance [420], which has been granted an appeal to the  
 Grand Chamber. If this goes the same way, the ECJ judgment will be extended to those  
 countries that are members of the Council of Europe but not of the EU, such as the UK and  
 Russia.

15The UK ﬁne was the maximum allowed under pre-GDPR data-protection law; since then

the maximum is 4% of the defendant’s turnover, which should bring European penalties into  
 line with American ones.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 863 | Ross Anderson |

*26.7. FREEDOM OF INFORMATION*

|  |
| --- |
| innovation. The US equivalent is the FTC’s use of truth-in-advertising law to  punish ﬁrms that break their privacy policies or previous agreements about user  privacy; and Facebook was in due course ﬁned $5bn by the FTC. The Elec-tronic Privacy Information Center16 had been arguing arguing ever since the  Cambridge Analytica scandal broke that Facebook had violated the terms of its  2011 settlement with the FTC. |

**26.7** **Freedom of Information**

Information tends to ﬂow from the weak to the powerful, increasing their power  
 and making it harder for others to hold them to account. As James Madison  
 wrote:

A popular government without popular information or the means of  
 acquiring it is but a prologue to a farce or a tragedy, or perhaps both.  
 Knowledge will forever govern ignorance: And a people who mean to  
 be their own Governors, must arm themselves with the power which  
 knowledge gives.

In the aftermath of Watergate, Congress passed the Freedom of Information

Act, and other countries followed; Britain got one in 199717. More radical

versions 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 a low declared income would bring. The most radical version is proposed by  
 David Brin, in ‘The Transparent Society’ [322]. 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 a Chinese–style policing system and  
 one in which officials are held to account by public scrutiny. He argues that  
 essentially all information should be open – including, for example, all our bank  
 accounts. The cameras will exist: will they be surveillance cams or webcams?  
 Social media often seem to be pushing us in that direction. In any case, Freedom  
 of Information Acts typically let the citizen demand copies of information held  
 by the state unless there’s a good reason to withhold it, and help ensure that  
 the ﬂow of information between the citizen and the state isn’t entirely one-way.

However, transparency leads to interesting tussles. Many European coun-

tries have clean-slate laws whereby most criminal convictions are expunged after  
 a period of time that depends on the severity of the offence, and in 2019 Penn-  
 sylvania, Utah and California followed suit [607]. But how can such laws be  
 enforced now that web search engines exist? Do you tag the names of offenders  
 in newspaper accounts of trials with an expiration date, and pass laws com-  
 pelling search and archive services to respect them? The Google Spain case  
 gives us the answer: someone whose conviction has expired has a right to have  
 it suppressed in searches, although it may remain in the newspaper archive for  
 those who know where to look.

16Full disclosure: I’m a member of their advisory board.  
 17Tony Blair later described it as his biggest mistake.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 864 | Ross Anderson |

*26.8. SUMMARY*

That’s one example of the shifting boundary between data protection and

freedom of information. Another has been the monitoring of former child sex of-  
 fenders, with laws in some states requiring that registers of offenders be publicly  
 available, and riots in the UK following the naming of some former offenders by  
 a Sunday newspaper and at least one innocent person being lynched. A third  
 is the release of crime statistics: home owners object to their neighbourhood  
 being stigmatised, and if the data are too granular there may be some risk of  
 individual victims being identiﬁed. For further examples, see Section 11.1 on  
 inference security.

**26.8** **Summary**

Public policy is increasingly entangled with the work of the security engineer.  
 The largest single concern of governments, if we measure it in dollar terms, is  
 intelligence; a typical government spends a hundred times more money collecting  
 information on its enemies, real and potential, than it does on ﬁghting cyber-  
 crime. Intelligence collection is also in conﬂict with both defensive security

and with privacy, both of which have historically come second. However, since  
 the Snowden revelations made clear the scale of US data collection worldwide,  
 and of Five Eyes operations against allied countries, the balance has started to  
 shift, and the effects have propagated through privacy and data protection law,  
 albeit slowly and with so far little effect on the agencies themselves. Perhaps  
 when the analysis is done, Snowden’s effect on the agencies’ capabilities will be  
 largely technical (through getting people to use cryptography more, and more  
 intelligently) while the policy effect may be to curb some of the excesses of  
 ‘surveillance capitalism’ by making privacy more salient to more people. The  
 strains between the US and European ways of dealing with privacy are becoming  
 more signiﬁcant and in the medium term we may see more localisation – where  
 US companies have to keep data on EU citizens on servers in Europe and perhaps  
 even under the control of European trustees. Other countries are starting to  
 follow suit.

Censorship is a real issue; some countries, like China, ban many of the large

US service ﬁrms outright, while more and more are demanding that they take  
 down not just abusive material but also material that offends local political  
 sensitivities. The Internet still makes it harder for countries that won’t go as  
 far as China to censor subversive content, but much of the optimism we had ten  
 years ago has dissipated with the failure of the Arab Spring. Even the developed  
 countries push the large service ﬁrms to moderate and ﬁlter user-generated  
 content at scale, and despite the cost and complexity, it’s becoming universal  
 except on end-to-end encrypted services. It’s now 25 years since AOL barred  
 users from living in Scunthorpe, and large-scale ﬁltering still raises a host of  
 policy issues whether we’re talking about copyright, radicalisation, harassment  
 or fake news.

The security-industrial complex, whose growth was fuelled by the climate of

fear whipped up after the 9/11 attacks, has got a second wind from China and  
 the Arab Spring, as the world’s authoritarians buy surveillance systems to keep  
 track of their populations. This has led to the proliferation of computer and

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 865 | Ross Anderson |

*26.8. SUMMARY*

network exploitation tools that erode our security, our liberty, and our quality  
 of life. This proliferation is aided and abetted by Western governments who  
 should know better, and is bound to be extended as social media ﬁrms and  
 others are co-opted into ever more content screening as a condition of doing  
 business. Understanding and pushing back on the surveillance ecosystem while  
 mitigating online harms 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 careful accumulation  
 of data and 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, and its terrible  
 consequences in terms of spending money on security theatre that should have  
 been spent on pandemic preparedness.

**Research Problems**

Technology policy involves a complex interplay between science, engineering,  
 psychology, law and economics. There is still too little serious cross-disciplinary  
 research, and initiatives which speed up this process are almost certainly a  
 good thing. Since 2002 I’ve worked to build up the security-economics research  
 community; and since 2008 we’ve run an annual workshop on security and hu-  
 man behaviour to engage psychologists, anthropologists and philosophers too.  
 But we need much, much more. Where are the historians, the sociologists and  
 the political scientists? (And perhaps if there’s a fourth edition, we’ll add the  
 philosophers.)

**Further Reading**

It’s extraordinarily easy for technology policy arguments to get detached from  
 reality, and many of the scares conjured up to get attention and money (such  
 as ‘cyberterrorism’) are the modern equivalent of the monsters that appeared  
 on medieval maps to cover up the cartographer’s ignorance. An engineer should  
 look for primary sources – from material written by experienced insiders such  
 as R.V. Jones [992] to the thousands of documents leaked by Ed Snowden. As  
 for the use of information warfare techniques in the Brexit referendum and the  
 2016 US election, Carole Cadwalladr’s movie ‘The Great Hack’ is unmissable.

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 pro-  
 cess [558], and an NRC study on cryptography policy was also inﬂuential [1411].  
 There’s a video on my website of the history of the crypto wars from a European  
 perspective.

The history of export control is tied up with Soviet attempts to buy US

computer, semiconductor and energy technology during the 1970s and 80s, and  
 the US and French intelligence community’s work to block them and feed them

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 866 | Ross Anderson |

*26.8. SUMMARY*

misleading information: see the memoir on Gus Weiss, a CIA maverick involved  
 in this work [723].

Resources on online censorship include Reporters without Borders, who pub-

lish a ‘Handbook for bloggers and cyber-dissidents’ on how to circumvent cen-  
 sorship, with a number of case histories of how blogging has helped open up the  
 media in less liberal countries [1594].

The standard work on computer forensics is by Tony Sammes and Brian

Jenkinson [1644], while Privacy International has a survey of mobile phone  
 forensics [1555] and the Department of Justice’s “Guidelines for Searching and  
 Seizing Computers” also bear some attention [550]. For early computer crime  
 case histories, see Peter Neumann [1429] and Dorothy Denning [539]. The stan-  
 dard work on computer evidence in the common law countries is by Stephen  
 Mason [1236].

On the topic of privacy versus data protection, there is a huge literature

but no concise recent guide that I know of. Recent material can be found on  
 the web sites of organizations such as EPIC [631], EFF [618], FIPR [708] and  
 EDRi [643], and of Max Schrems [1683].

As for the policy problems around the ﬁltering of inﬂammatory content and

propaganda, the two most thought-provoking books for me are those by Tim  
 Wu [2050] and Yochai Benkler [227], while Facebook’s former CISO Alex Stamos  
 now discusses the tech companies’ view of ﬁltering political ads [999].

Finally, the deﬁnitive story of the Cambridge Analytica scandal is told in the

book by the whistleblower Chris Wylie [2052], and in the journalism by Carole  
 Cadwalladr based on information that he and others supplied [363].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 867 | Ross Anderson |