VI. Securitization Technologies

We noted in Chapter III that the ratcheting up of security has created a number of problems for important liberal democratic values – in relation to security itself as well as with respect to liberty, autonomy, privacy, identity and dignity.

Here our focus will be on various securitization technologies concerned with surveillance, data mining and matching/integration, and profiling. We provide descriptions of some of the main technologies in use, indicating briefly how they impact on and challenge the values identified in Chapter III (and articulated at greater length in Chapter VIII). Our concern will not be to determine the actual and potential contribution of these technologies to security. Accordingly, this chapter should not be understood as even implicitly offering an all-things-considered evaluation of the securitization technologies described.

(A) Electronic Surveillance[1]

Surveillance technology takes many forms. Whereas some are familiar, others pass unnoticed. Examples of both include: closed circuit television (CCTV), X-ray and similar devices at airports, thermal sensors, temperature screening (for SARS), keyloggers, wiretaps, bugs, parabolic microphones, Radio Frequency Identification Devices (RFID) and Global Positioning Systems (GPS).[2,3] Why should we worry about them and in what ways do they compromise, or threaten to compromise, privacy, liberty and the like?

In the US, the use of electronic surveillance to enhance security has a long history that began soon after the invention of the telegraph in 1844. As newer technology was invented it was co-opted in the name of security. These technologies have included the telephone and computers as well as the many and multiplying electronic encroachments on public space.

[1] For background on surveillance and its theory, See David Lyon, *Surveillance Studies: An Overview* (Cambridge, UK: Polity Press, 2007).

[2] It is not possible to cover all these technologies and their ethical implications in a single chapter. For more information see, for example, M.G. Michael, Sarah Jean Fusco, and Katina Michael, "A Research Note on Ethics in the Emerging Age of Überveillance", *Computer Communications* 31 (2008): 1192–99. Also, see Roger Clarke, "Person-Location and Person-Tracking: Technologies, Risks and Policy Implications", *Information Technology & People* 14, no. 2 (Summer 2001): 206–31; Christopher S. Milligan, "Facial Recognition Technology, Video Surveillance, and Privacy", *Southern California Interdisciplinary Law Journal* 9 (2000): 295–334.

[3] There is always new technology being developed that can be pressed into action. For example, see H. Schneider, H. C. Liu, S. Winnerl, O. Drachenko, M. Helm, and J. Faist, "Room-temperature Midinfrared Two-photon Photodetector", *Applied Physics Letters* 93, no. 101114 (2008): 1–3.

As far as government surveillance is concerned, the checks provided by the Fourth Amendment have been of critical historical importance, though the Fourth Amendment's value has become marginalized in the face of increasing non-governmental surveillance and, even in those cases, because of problematic re-drawings of the public–private distinction and persisting (legal) doubts about the applicability of the Fourth Amendment to public space.

Recent years have seen the development of a range of strategies encompassed (more or less) by the general term "electronic surveillance". Included among these have been, most ubiquitously, closed circuit television (CCTV) cameras, more potent and prevalent in the UK than in the US, though increasingly used in the US in a more coordinated fashion.[4] Such electronic surveillance may take many other forms. We have already noted the use of X-ray-type devices at airports that penetrate clothing to the skin, and thermal sensors that can be used to detect activity in buildings (such as movement and marijuana growth). To these we might add wiretaps,[5] bugs[6] and parabolic microphones.[7] Moreover, so far as networked computers are concerned, electronic surveillance has taken a number of increasingly intrusive and sophisticated forms. There are, for example, programs developed by the FBI for scanning email traffic through particular servers. One such program, originally named Carnivore, with a later version renamed as DCS 1000, had both trap and trace[8] and full access capabilities.[9] The latest version of this is the Communications Assistance for Law Enforcement Act (CALEA), which the FBI is using "as a virtual blank check to force the communications industry to build surveillance capabilities . . . into every modern means of communication. This includes cellular and digital communications technology never even contemplated when CALEA was drafted in the early 1990s."[10] The latter are much more intrusive than the former. There are also keylogging devices that can record every keystroke made by an individual. However, data on FBI and DHS email surveillance are not easy to come by.

[4] It has been estimated that there are several thousand CCTV cameras in Manhattan public spaces. For articles, see Anon., "A History of Surveillance in New York City", available at: http://www.notbored.org/nyc-history.html; Kareem Faheem, "Surveillance Will Expand To Midtown, Mayor Says", *The New York Times*, October 4, 2009, available at: http://www.nytimes.com/2009/10/05/nyregion/05security.html; and Al Baker, "Police Seek a Second Zone of High Security in the City", *The New York Times*, March 31, 2009, available at: http://www.nytimes.com/2009/04/01/nyregion/01kelly.html.

[5] For information, see the Electronic Information Privacy Center (EPIC) links: http://www.epic.org/privacy/wiretap/.

[6] For general information, see http://en.wikipedia.org/wiki/Covert_listening_device.

[7] See e.g. http://www.espionageinfo.com/Nt-Pa/Parabolic-Microphones.html.

[8] See http://www.cdt.org/security/000404amending.shtml.

[9] See the EPIC links at http://www.epic.org/privacy/carnivore/foia_documents.html. Note that use of Carnivore was abandoned in 2003.

[10] Wayne Madsen, "FBI's Communications Surveillance Capabilities Widen", *Computer Fraud & Security*, no. 10 (October 2000): 16–17.

We will briefly outline several of these electronic surveillance strategies along with the ethical problems they raise. As noted previously, US policy is officially governed primarily by two documents: the Foreign Intelligence Surveillance Act of 1978 (FISA)[11] and the Electronic Communications Privacy Act of 1986 (ECPA).[12] They have been supplemented and modified by a number of other acts, most notably the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, as revised),[13] the Protect America Act of 2007 and the FISA Amendment Act of 2008.

Video surveillance[14]

CCTV camera surveillance predated the events of 9/11 by well over twenty years; their use is well-established. However, the growing and accelerating ubiquity of surveillance cameras, particularly in large urban areas, has created the theoretical possibility that almost all our daily movements in public space can now be reconstructed into a continuous visual narrative.[15] There are, of course, various practical and other impediments to this theoretical possibility. For one thing, it would be hugely expensive to have continuous human monitoring of all such cameras. What is feasible is that the footage of all cameras be available after some particular event. For another thing, there are practical limits on the extent of coverage, for example, in rural or semi-rural areas, and the availability of unsurveilled areas gives rise to the possibility of displacement. On the other hand, many current practical problems in densely populated urban areas (e.g. Manhattan), such as lack of coordination, integration and (often) preservation, look to be relatively easy to overcome. The UK is much closer to constructing a coordinated CCTV network, as evidenced by follow-up to the 7/7 and later bombings. IRA terrorism preceded the jihadist variety.

The everyday security concerns that initially provided public support for the use of surveillance cameras have been taken by authorities, both private and public, as justification for something of a *carte blanche* (given the lesser protections that exist for privacy in public) for their installation in many public places. Aided

[11] See http://www.fas.org/irp/agency/doj/fisa/. FISA's main purpose is to regulate the surveillance of those who are believed to be foreign agents.

[12] See §§ 2510, 2511 http://www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18.html. ECPA's main purpose is to regulate domestic surveillance.

[13] See http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162. Also see http://thomas.loc.gov/cgi-bin/cpquery/R?cp109:FLD010:@1(hr333) and http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.01927:.

[14] For a survey of the latest in video surveillance see Niels Haering, Péter L. Venetianer, and Alan Lipton, "The Evolution Of Video Surveillance: An Overview", *Machine Vision and Applications* 19 (2008):279–90.

[15] A city council is likely to be seen as "out of step" if it does not follow the trend. We can also add to CCTV various other "tracking" possibilities, from things such as EZ-Pass to cell phones (that now function as global positioning systems).

by the myth that what happens in public is public, the proliferation of such cameras now raises possibilities similar to those created by data mining on the internet: the development of narratives rather than simple profiles.

We can accept that what we do in public may not have as great a claim to privacy as what we do in private, but even in public we ought to have some control over personal data. For example, we should not have to conduct every conversation in public *sotto voce* – or wait until we have found some private space. The self-censoring effect of denying privacy in public would be considerable. Our freedom is not constituted simply by the absence of constraints but also by a sense of security in what we do. Should we then limit the installation of cameras and/or otherwise constrain their use?

To the extent that a CCTV unit often constitutes an unobserved observer, there is additional reason to be cautious about it, for in those cases we are not given a fair opportunity to structure our behavior/self-presentation in the knowledge that the unit is present. It does not function like the uniformed police officer. Should its use, therefore, always be accompanied by a sign to the effect that it is present?[16] In other words, should the primary use of CCTV be deterrent even as it also protects privacy? Should there also be some indication as to whether a CCTV camera is controlled by an operator who can swivel, zoom in, and focus? Should there be some contact information in the event that a person wishes to inquire about the gathered data's use, retention, security etc.? Should there be rules about data use, retention and security independent of those who might wish to inquire about such matters? The questions go on.

One problem with CCTV cameras concerns simple observability and the threat to privacy that may be involved either with live operators or later reviews of the tapes. Even our awareness of a camera's presence can be unsettling if we reflect that it may be recording and making a permanent record of what we think of as fleeting. In such cases, we cannot presume on our normal ability to blend anonymously into the situational landscape. Cameras challenge our presumption of anonymity. As Alan Westin puts it:

> [A]nonymity [as a form of privacy] occurs when the individual is in public spaces or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the rules of behavior and role that would operate if he were known to those observing him. In

[16] This is suggested by Andrew von Hirsch, "The Ethics of Public Television Surveillance", in Andrew von Hirsch, David Garland, and Alison Wakefield (eds.), *Ethical and Social Perspectives on Situational Crime Prevention* (Oxford: Hart Publishing, 2000), 68.

> this state the individual is able to merge into the "situational landscape." Knowledge or fears that one is under systematic observation in public places destroys the sense of relaxation and freedom that men [and women] seek in open spaces and public arenas.[17]

The point reaches a bit deeper. Unlike targeted searches that focus on specific items, CCTV surveillance functions more like a dragnet. It makes no distinction between those items that might be of interest, say, to law enforcement, and other items that are and ought to be regarded as private. It records them all. Daniel Solove links this electronic promiscuity with old discussions concerning general warrants and writs of assistance – practices to which the framers of the US Constitution were deeply opposed because they were undiscriminating. He quotes from Patrick Henry's opposition to writs of assistance: "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, and ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds."[18] The point is simply that because CCTV cameras record everything that occurs within their range, and therefore fail to "filter out" matters that ought to be considered private, their use imposes a significant moral burden on those who install them and, potentially, a different burden on those who have to live under their eye.

However, it is not simply a matter of our observability and subsequent capture by camera that is worrisome. Also of concern is the use to which the data are put. If, for example, what is captured is preserved in some large database (along with information gleaned from other public sources), or if the captured images are used as part of some film compilation (say, a kind of "Candid Camera"), we would also have reason to be deeply disturbed. What has been set up for one purpose may, absent controls, be used for other purposes. The principle of contextual integrity (to which we will return) will have been violated. No doubt some of those other purposes may be relatively innocent, but unless we can exercise some control over them, they may not be. In other words, we have not only an issue of privacy but also of confidentiality.

And so the main concern of CCTV's critics has been to develop adequate controls over what is gathered about us in public space. One important aspect of this control might include identification of the controller of the CCTV camera:

> Being able to identify who is watching us is crucial if we are to be able to make decisions about how to adjust our behavior (or not) in the light of such observation . . . Knowing that we are being watched by

[17] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 31.

[18] Quoted in Daniel J. Solove, "Restructuring Electronic Surveillance Law", *George Washington Law Review* 72 (2004): 1706.

> a camera is not the same as knowing the identity of who is watching us. All that we know is that we are being watched, but it is impossible for us to know why or by whom. This is the reason that we draw a distinction between being watched by a visible police officer and a CCTV camera mounted on the side of the building. Seeing, identifying, and attempting to understand the motives of whoever is watching us is an essential precursor to deciding how we feel about being observed, and to deciding on how to respond to such observation.[19]

But identification of the observer is only one step in the process of retaining some control over one's public self. More is needed if we are to ensure adequate recognition of privacy. We need to know in detail the purposes that the cameras are intended to serve and we also need to assess the weight of these purposes. That will involve some assessment of the stakes, the risks (including probabilities) and the likely effectiveness of CCTV measures. We need, in other words, to know whether the loss of privacy effected by CCTV cameras (and other surveillance technologies) is morally outweighed by gains in security (and/or other socially valued outcomes for which they are intended). The latter question can be complicated by the potential that there is for public misperception – on the one hand, an underestimation of the intrusiveness of CCTV cameras and, on the other hand, an overestimation of the risks of, say, terrorism. For many of us, the ubiquity of CCTV cameras has dulled us to what they may be recording. At the same time, our fears of terrorism have been exploited by those for whom the presence of additional CCTV cameras (*inter alia*) is desired. We also need to take account of the fact that whereas the threat of terrorism is said to be "to America" or "to Australia", the burden of CCTV tends to fall on people unequally.

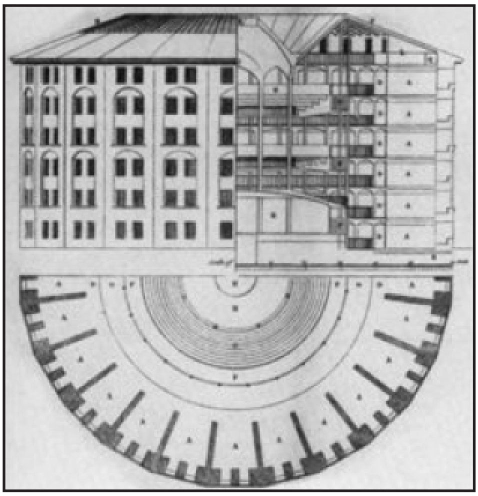
Assuming that we have successfully defended particular uses of CCTV, we then need to address several other questions at whose existence we have already hinted. Some concern the storage and dissemination of information: How timely? How safely? For how long? Who has access? Another set of questions relates to the issues of implementation and oversight: Who ensures that answers to the previous questions are implemented and adhered to?

Useful, though obviously not decisive, is the American Bar Association's *Standards for Criminal Justice: Electronic Surveillance, B: Technologically-Assisted Physical Surveillance*.[20] What is required is some assurance that these standards will be observed, that they are worth more than the paper on which they are written. Some, such as Benjamin Goold, doubt whether an oversight agency could provide the requisite assurance, given the huge proliferation of

[19] Benjamin Goold, "Privacy Rights and Public Spaces: CCTV and the Problem of the 'Unobservable Observer'", *Criminal Justice Ethics* 21, no. 1 (2002): 24.

[20] Third ed. (Washington, D.C.: ABA 1999). See http://www.abanet.org/crimjust/standards/electronicb.pdf.

CCTV cameras. He thinks that the kind of spot checks that an oversight agency is likely to provide (given the funding that could be expected) would not be sufficient to assure us that significant abuses were not occurring.[21] Goold's own solution takes the form of an appeal to Bentham's Panopticon[22]:



As Bentham himself puts it:

> The final application of the inspection principle was of the whole of the prison by the whole of the outside world. The central tower would enable judges and magistrates to inspect the prison quickly and safely . . . The design of the building would also enable any member of the public safely to enter the prison and to view every prisoner in it: "I take it for granted, as a matter of course, that . . . the doors of these establishments will be, as, without very special reasons to the contrary, the doors of all public establishments ought to be, thrown wide open to the body of the curious at large – the great open committee of the tribunal of the world.[23]

Taking his cue from Bentham, Goold wants to argue that all CCTV scans should be publicly available – available to all, so that those who are responsible for them can be scrutinized at any time.

[21] Benjamin Goold, "Open to All? Regulating Open Street CCTV", *Criminal Justice Ethics* 25, no. 1 (2006): 11–12.

[22] Bentham spelled out his views in an eponymous series of letters written in 1787, though he also referred to it elsewhere in his writings (see http://www.cartome.org/panopticon2.htm). See Jeremy Bentham, *The Panopticon Writings*, ed. Miran Bozovic (London: Verso, 1995). Most of the contemporary discussion takes as its point of departure Michel Foucault's discussion of Bentham in *Discipline & Punish: The Birth of the Prison*, trans. Alan Sheridan (NY: Vintage Books 1977), 195–228.

[23] Jeremy Bentham, *The Works of Jeremy Bentham,* ed. John Bowring (London: W. Tait, 1838–43), vol. 4, 46.

We are not so sanguine about Goold's solution, even though we are also troubled by the frequent inadequacies of oversight agencies. There is just too much out there, and the likelihood that improper use of CCTV data will go undetected or unpenalized is substantial. Moreover, as we have learned with the doctrine of *caveat emptor*, we cannot presume that people in general will have the energy, inclination or ability to police such matters. The mere capacity to review material, though important, is not enough. Nor can we presume that complaints will be appropriately addressed any more than we can presume that oversight mechanisms will work effectively. Moreover, there is a danger that the availability of such materials could provide yet another resource for those whose perverted tastes would review, rework and distribute materials in such a way as to constitute an unacceptable invasion of privacy. True, some technological safeguards might be provided (for example, barriers on cut, paste and print options), but even these would not be foolproof. At best – and maybe it is the best – we can hope that the possibility of misuse being uncovered because of a policy of transparency might operate to deter those who would otherwise be inclined to misuse such data. As in other cases, however, the effectiveness of a policy of deterrence will depend significantly on perceptions of the likelihood of being caught and, if so, the actual penalties for misuse.[24]

To some extent, Goold's solution seems to move in exactly the wrong direction. We do wish to maintain some measure of privacy in public and surveillance technology threatens that. Making such information available to all exacerbates the problem by enabling whatever private acts took place in public to be communicated even more widely than might have been presumed when they took place. The values that informed confidentiality as well as privacy – the values of contextual integrity as well as agency – would be compromised.

The next issue we need consider is the quality of the technology itself and our reliance on its apparent infallibility.[25] In an attempt to examine the claims of facial recognition software using CCTV footage, James Meek, a journalist from the *Guardian*,[26] had his mugshot taken and then challenged the CCTV system on the streets of the east London borough of Newham to identify him. However, the software used, FaceIt, failed to recognize him. Although official results are secret, the system has, according to the Newham police, never recognized a person from its database of faces. The value of the system is apparently in

[24] To this end, we think it is important that those engaged in surveillance operations know that they are, in fact, subject to reviews of ongoing accountability. The implementation of performance management systems, audits, program evaluations, inspections and the use of Techno-ethics Boards to address emerging concerns will put practitioners on notice that transparency is valued and, more importantly, actively pursued.

[25] See Peter Kovesi, "Video Surveillance is Useless", Presentation at the 18th International Symposium of the Australia and New Zealand Forensic Society, April 2–7, 2006, Fremantle Western Australia. Also Peter Kovesi, "Video Surveillance: Legally Blind", presentation at DICTA 2009, Digital Image Computing: Techniques and Applications, December 1–3, 2009, Melbourne, Australia, http://dicta2009.vu.edu.au/, viewed December 31, 2009.

[26] James Meek, "Robo Cop", *The Guardian*, 13/06/2002.

its deterrence effect, though even this is disputed. Indeed, according to the article that Meek wrote in Tampa, Florida, fourteen false positives and no true positives were recorded on one day. If this result is typical, perhaps we need not worry about any imminent actual infringement upon our privacy. Maybe we should be more concerned about government agencies spending enormous sums of money on systems that do not work! We will return to the issue of the quality of technological systems later in this study.

Even if the quality of the technology of video surveillance improves, there are some practical difficulties with serious consequences. The practical difficulties are volume and human error. The sheer volume of stored video information is overwhelming. Human evaluation capability is simply not up to the task of viewing all that information. The other problem, human error, applies to both stored and real-time video monitoring. According to the US National Institute of Justice, "Monitoring video screens is both boring and mesmerizing."[27] Smart Surveillance is being proposed as a solution to these problems.[28] Smart surveillance, of which IBM's S3[29] is but an example, offers the technological capability of providing real-time alerts (such as user-defined, generic, class specific, behavioral and high-value video capture), automatic forensic video retrieval and situation awareness. Although the current state of this technology faces challenges (both technical and evaluative), should these difficulties be resolved significant implications present themselves. The first is that these systems need to be able to prove their reliability by having few or no false positives. Another is the unprecedented challenge to privacy posed by the use of this technology to enhance privacy! The point is not that the challenge could not be met, but that it would be met only if its use could be adequately overseen, something that already constitutes a major issue.

Scanning devices[30]

Along with watch lists, there has been increased scrutiny not only of luggage but also of persons. Following the Richard Reid incident, shoes must now be

[27] Mary W. Green, *The Appropriate and Effective Use of Security Technologies in U.S. Schools, A Guide for Schools and Law Enforcement Agencies*, Sandia National Laboratories, September 1999, NCJ 178265.

[28] Arun Hampapur, Lisa Brown, Jonathan Connell, Sharat Pankanti, Andrew Senior, and Yingli Tian, "Smart Surveillance: Applications, Technologies and Implications", available at: http://domino.research.ibm.com/comm./research_projects.nsf/pages/s3.pubs.html/$FILE$/PCM03.pdf.

[29] See Ying-li Tian, Lisa Brown, Arun Hampapur, Max Lu, Andrew Senior, and Chiao-fe Shu, "IBM Smart Surveillance System (S3): Event Based Video Surveillance System with an Open and Extensible Framework", *Machine Vision and Applications* 19 (2008):315–27, DOI 10.1007/s00138-008-0153-z. The article claims that such systems provide "not only the capability to automatically monitor a scene but also the capability to manage the surveillance data, perform event based retrieval, receive real time event alerts thru standard web infrastructure and extract long term statistical patterns of activity" (315).

[30] For further discussion of the law and ethics relating to the use of this technology, see Julie Solomon, "Does the TSA Have Stage Fright? Then Why are they Picturing you Naked?", *Journal of Air Law and Commerce* 73, no 3 (2008): 643–71; Tobias W. Mock, "Comment: The TSA's New X-Ray Vision: The Fourth Amendment

routinely removed for X-ray inspection and, following another incident, carry-on liquids have been banned or restricted. Computers are sometimes checked for traces of explosives. To try to ensure that weapons etc. do not escape the metal detectors through which passengers must pass, some passengers are subjected to a further level of scrutiny using a wand or pat-down search.[31] However, the latter has led to complaints of sexual touching or acute anxiety, and so efforts have been made to develop technologies that will achieve the same effect without touching.

A few years ago, an X-ray backscatter imaging system was developed to detect weapons or explosives concealed on the body. The system penetrates clothing and reveals anything on the body surface (though it cannot pick up items that may be hidden in body folds).[32] It was trialed in a number of airports in the US (e.g. Orlando) and elsewhere. The technology has now developed further and the current system of choice is called an Active Millimeter Wave body scanner.[33] It uses high-frequency millimeter waves and not radiation.

Devices such as these are already in use in the UK, Netherlands, Japan and Thailand. They were tested at Phoenix Sky Harbor Airport and trialed in LA and New York[34] before becoming standard equipment in many airports around the world.

Implications of 'Body-Scan' Searches at Domestic Airport Security Checkpoints", *Santa Clara Law Review* 49 (2009): 213–51; TSA website http://www.tsa.dhs.gov/approach/tech/castscope.shtm. In addition, the technology is being considered for use in other contexts via mobile units; see Glen W. Fewkes, "New Public Surveillance Technologies May Alter Fourth Amendment Standards", *Government Security News*, March 6, 2009, available at: http://www.gsnmagazine.com.

[31] However, as the recent case of Umar Farouk Abdulmutallab has shown, the problems may not be with technologies but with the humans who administer them. See Eric Lipton and Scott Shane, "Questions on Why Terror Suspect Wasn't Stopped", *The New York Times,* December 2, 2009: http://www.nytimes.com/2009/12/28/us/28terror.html?_r=1&scp=2&sq=Umar%20Farouk%20Abdulmutallab%20&st=cse.

[32] See Austin Considine, "Will New Airport X-Rays Invade Privacy?", *The New York Times*, October 9, 2005, TR3; also the Rapiscan website: http://www.rapiscansystems.com/sec1000.html and, more graphically, http://www.electromax.com/rapiscan%20secure%201000.html.

[33] Although a number of companies are using this technology, most of the ones being trialed at present are manufactured by L3 Communications for the Transportation Security Agency (Department of Homeland Security), http://www.l-3com.com/products-services/productservice.aspx?id=533&type=b. For technical data and assessments, see Committee on Assessment of Security Technologies for Transportation, National Research Council, *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons* (Washington, DC: National Academies Press, 2007). http://books.nap.edu/openbook.php?record_id=11826&page=R1. For the latest in such technology, see S. Oka, H. Togo, N. Kukutsu, and T. Nagatsuma, "Latest Trends in Millimeter-Wave Imaging Technology", *Progress In Electromagnetics Research Letters* 1 (2008): 197–204. For discussion of ethical issues see http://www.mindfully.org/Technology/2007/Active-Millimeter-Wave11oct07.htm.

[34] See Calvin Biesecker, "TSA to Test Additional Personal Imaging Systems at Airports", *Defense Daily*, 8/21/2007. For further updates, following the Christmas Day 2009 terror attempt, see "UK Introduces Full-body Screening in Heathrow Airport", available at: http://www.edri.org/edrigram/number8.3/uk-introduces-naked-body-scanners; "EU Considers Full Body Screening in Airports", available at: http://www.edri.org/edrigram/number8.1/airport-body-scanners-europe.

Critics of devices such as Rapiscan also raise the specter of X-Ray contamination, though the amounts to which people are exposed fall well below allowable levels and, as we have noted, do not constitute a problem in the case of more recent technologies.

Source: http://www.thetechherald.com/media/images/200826/Provision_1.jpg; http://www.mytvmoments.com/view.php?v=14579

Nevertheless, the problem with such devices is that even though they seem[35] to avoid the privacy concerns associated with pat downs they create privacy issues of their own: screen images showing genital areas can be viewed as well as medical information that people may wish to keep private (such as colostomy bags or physiological oddities). In theory, the images may be saved and downloaded, though it appears that the machines do not need to have a save/download function.[36] New machines can also obscure the head, so that the passenger is not identifiable (though this is a feature that can be easily changed and may be not much of a hindrance to identification). A further privacy-enhancing feature is the stationing of monitors some distance from the device itself. A partial technological solution to the privacy problem is available: instead of the screen image being "what the machine sees", the raw data can be projected onto a generic outline so that all that appears are any metallic, plastic or otherwise dense objects. Although this important further step appears not to have been taken with many of the machines currently in use and under review, it has been taken in many settings, including a number of international airports. However, it should be noted that this is not sufficient for some civil liberties groups, who

[35] It has been claimed that, because the machines cannot always disambiguate images, subsequent pat-downs are still sometimes required. Nevertheless, surveys suggest that people are more willing to have a "virtual strip search" than a pat-down.

[36] There have, however, been cases in which images have been improperly saved and distributed. See Jeanne Merserve and Mike M. Ahlers, "Body Scanners Can Store, Send Images, Group Says", CNN News, January 11, 2010, available at: http://edition.cnn.com/2010/TRAVEL/01/11/body.scanners/index.html.

take the view that unless there is some other, compelling reason to think that a particular person could have terrorist connections (say, the appearance of his/her name on a watch list), no person should be subjected to such searches. This replication of pat-downs is also not without its problems. Recently the latest in body-scanning technology has raised a new problem; the seeming creation of child pornography.[37] The graphic nature of the latest technology scanning children means that the resulting images may breach child protection laws of the UK. The result is that, at the moment, individuals under the age of eighteen are exempt from scanning.[38] The problem with this is obvious: children could easily be carriers of the very objects that the scanning was devised to detect.

A further complaint concerning scanning devices has to do with their cost-effectiveness. The machines currently cost about US$200,000, have high support requirements and are time-consuming to operate and maintain. Do the gains in security match the expenditure involved? Might the money and human resources be better invested elsewhere? James Carafano of the Heritage Foundation takes the view that "where you want to spend your money is [where you have a prospect of] getting the terrorists long before they get to the TSA checkpoint."[39]

Wiretaps, bugs, and parabolic microphones

In the US, the tapping of telegraph lines goes back to the Civil War, with telephone tapping beginning in the 1890s, soon after the development of the telephone recorder. Tapping is covered primarily by FISA, ECPA and the Communications Assistance for Law Enforcement Act of 1994 (CALEA),[40] and is supplemented by the other acts that we have already referred to. CALEA requires telecommunications providers to ensure that upgrades to their technologies do not exclude the possibility of governmental tracking and interception.

Whereas wiretaps generally involve some external interception of telecommunications, bugging devices are usually located within the premises that are being monitored. They mostly take the form of microphones, often disguised as objects whose real function is unlikely to be detected: fountain pens, desk calculators, clock radios etc. Sometimes they are video-capable as well. The planting of bugs will frequently require unauthorized entry into private premises. ECPA has important provisions regarding the sale and use of bugging devices.

[37] See Alan Travis, "New Scanners Break Child Porn Laws",*The Guardian*, Monday, January 4, 2010 22.14 GMT.

[38] *Ibid*. See also Leonora LaPeter Anton, "Airport Body Scanners Reveal All, but What About When It's Your Kid?", *St Petersburg Times*, July, 17, 2010.

[39] See http://www.cnsnews.com/ViewNation.asp?Page=/Nation/archive/200710/NAT20071015a.htm.

[40] Available at http://www.epic.org/privacy/wiretap/calea/calea_law.html.

Parabolic microphones use satellite dish technology to focus sounds from up to about 1,000 feet (305 meters) away. There are stereo versions that give even better quality sound. Along with bugging and wiretap devices, they are easily available for purchase online. Indeed it is relatively simple to obtain product reviews of monitoring software (with a view to purchasing the most effective for one's own special purposes).[41]

Because of its invasiveness, wiretapping has always been contentious. As Justice Brandeis famously remarked:

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.[42]

As we have already noted, FISA has undergone various modifications since 9/11 and there is some evidence that its provisions have been circumvented.[43] The strength of that controversy is largely expressive of Brandeis's concerns, though in the US it also taps into the ongoing controversy about the reach of the president's authority under the Constitution.[44]

In light of the potential threats to privacy posed by electronic and other interception and scanning devices, in most liberal democracies their use is legally permissible by law enforcement agencies only in the case of serious crimes. Moreover, such use is typically subject to oversight and accountability, including the requirement for independently adjudicated warrants. Nevertheless, here, as elsewhere, as a consequence of rapid technological development, there remain gaps in relevant legislation and accountability.

[41] See, for example, the "Internet Activity Monitoring Software Consumer Guide", with recommendations on the top products reviewed, at: www.monitoringsoftwarereviews.org.consumerguide.html. This guide covers such topics as remote data access, accessibility of information, stealth, key logging (hardware and software versions), blocking, data filtering and screen shots.

[42] *Olmstead v. United States*, 277 U.S. 438 (1928).

[43] See "NSA Warrantless Surveillance Controversy", http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy.

[44] This also connects with the subsequent controversy (November, 2007) about holding responsible those companies that acquiesced in executive requests while knowing FISA requirements.

Online surveillance

Even before 9/11, the US Government was developing technologies capable of scrutinizing ("sniffing") internet traffic (IP packets) and recording those that met certain security-related criteria. The main instrument for this was a software-based tool known initially as Carnivore, later to become the less predatorily-named Digital Collection System 1000 (DCS 1000). The story of Carnivore's development was broken by the *Wall Street Journal* in 2000.[45] In response to concerns *inter alia* about communicative privacy, Carnivore was tendered for an "independent" review, which was completed in September 2000.[46] This did not allay the worries of critics, though the renamed version was for a time placed on some servers. It appears that DCS 1000 was able to function in either pen-register/trap and trace (compare to the recording of outgoing phone numbers and incoming phone numbers) or full intercept (compare to wiretapping) mode. How it operates in either mode depends on what it is asked to do by way of recognizing keywords or strings. DCS 1000 is no longer used, having been abandoned in favor of commercially available technology.[47]

A key issue for the kind of technology involved in DCS 1000 (and its surrogates) has been one of accountability. Accountability can be incorporated by building into the search software constraints that will make violations of privacy or other abuses less likely and/or by ensuring (using various forms of oversight[48]) that data collected will be used only for limited, approved purposes.

Unlike telephone communications, in which the content of the call and the identifying number calling/called are quite separate, or mail, in which the envelope and its contents are clearly differentiated,[49] the IP packets that are sniffed by programs such as DCS 1000 are more closely integrated. Transactional

[45] Neil King, Jr., "FBI's Wiretaps to Scan E-Mail Spark Concern", *Wall Street Journal*, 7/11/2000, A3. At the time, the primary purpose of Carnivore was not terrorism but crime, particularly financial crimes and child pornography.

[46] The review was carried out by a Research Institute at the Illinois Institute of Technology (IIT). The terms of the review were constrained in a number of ways (critics spoke of it as a whitewash), and several prestigious institutions reputedly refused approaches to conduct it. The review, largely technical, can be found at http://www.dojgov.net/carnivore-iitri.pdf. An official public (censored) version is also available on the web at: http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf. Nevertheless, the IIT review found that "it is not possible to determine who, among a group of agents with the password, may have set or changed filter settings. In fact, any action taken by the Carnivore system could have been directed by anyone knowing the Administrator password. It is impossible to trace the actions to specific individuals."

[47] FoxNews, "FBI Ditches Carnivore Surveillance System", available at: http://www.foxnews.com/story/0,2933,144809,00.html. One of the supposed strengths of Carnivore was its capacity to track only what was authorized by court order.

[48] Some of these will necessarily be internal FBI procedures along with legislative provisions and/or judicial powers. Others no doubt will take the form of external monitors such as EPIC, the Electronic Privacy Information Center (http://www.epic.org). The latter form of monitoring is made somewhat difficult because the software, its capabilities and some of its uses are classified.

[49] This is not to say that envelope details are unimportant. How often *A* communicates with *B*, and how large the packets, may reveal quite a bit. One can presume some degree of anonymity in this context as well.

and substantive data are not easily separable, and that raises a problem. Whereas access to the former does not require a search warrant, access to the latter does. In addition, because of the "packet switching" that occurs (in which packets of information take the most efficient route to their destinations, where they are reassembled) a search program is likely to sniff a lot of innocent and private communications. And so, "a simple search to see if two people are emailing each other – which can be approved without a search warrant – requires that Carnivore digest the private correspondence of millions of people."[50] It is not like putting an intercept device on a particular phone number to see who is being called.

The disanalogy with telephone records has been magnified by the USA PATRIOT Act,[51] which has extended permissible searches to include IP (Internet Protocol) addresses and URLs (Uniform Resource Locators) visited. Once someone has access to an IP address (i.e. an address that refers uniquely to an internet-accessed computer) it is possible to track where that user has been. Similarly, URLs can show what content the person accessed on the internet (e.g. whether pornographic or jihadist sites were visited and, if so, how often).

Of course, the interception of communications is just one dimension of online vulnerability. There is also the issue of stored communications – say, emails on a server waiting to be read, or the inbox storage of emails. What protections should these have against the intrusions of others? Are they adequate? Do they have teeth?

Another piece of controversial software – a keystroke logging program known as Magic Lantern – embeds itself (usually via a technique known as a Trojan horse)

[50] Joseph Goodman, Angela Murphy, Morgan Streetman, and Mark Sweet, "Carnivore: Will it Devour Your Privacy?", *Duke Law & Technology Review* (2001): 0028 http://www.law.duke.edu/journals/dltr/articles/2001dltr0028.

[51] These are contained in sections 201–225 of the USA PATRIOT Act. The Act included a number of provisions relating to surveillance, including the interception of wire, oral or electronic communications. Many of its surveillance-related provisions predated the Act, but were extended to cover various terrorism-oriented investigations. Some provisions relate to the sharing of information gathered under the aegis of the Act (always a problem area, not only because of cracks in the security of data but also because such data are sometimes of questionable accuracy, de-contextualized and may be put to expanded uses). The expansion of provisions previously available under FISA to engage in extended "roving wiretaps" has also generated some controversy: normally (limited) wiretap requests require explicit detailed specifications before they are granted. Under the USA PATRIOT Act these requirements, as well as geographical requirements for warrant service, have been loosened. The use of pen registers/trap and trace devices is also made easier under the Act, it being no longer required that the person whose communications are targeted is "an agent of a foreign power". It is enough that the gathering of intelligence be a significant purpose of interception and surveillance. The focus may be domestic as well as international terrorism. Most controversial of all has been sect. 215, which allows the FBI (under FISA or through the issue of a "national security letter") to compel the handing over of any item or record that it requests and to forbid the party from whom it seeks the item from disclosing such requests to others. Libraries have been particularly reluctant to disclose loan records. The major problem with a number of these provisions is that the government is not first required to establish why some particular person is a legitimate object of its surveillance powers.

on a target's hard drive and then records all that computer's keystrokes. One of the main purposes has been to access various passwords.[52] Magic Lantern (and its predecessor, Key Logging System) also circumvents the problems/safeguards created by encryption (whereby communications are coded in such a way that only recipients with a "key" are likely to be able to read them). Again, there are significant issues of accountability, encompassing targeting, data review, data retention, data security and so on.[53]

WWWveillance

Beyond the scope of this study is the importance[54] for surveillance of the emerging trend of more and more information about individuals being available on the internet, including their social activities and private musings. This opens a new field of surveillance activities that are even harder for the individual to detect. Entire categories of new surveillance tools, such as web crawlers, cookies, bugs and webcams, have emerged. These provide surveillance agents with a plethora of new information with which to carry out new patterns of surveillance. Colin Bennett identifies glitch, default, design, possession and subject as examples of such patterns of surveillance.[55] Note that this sort of surveillance is subtly different from the online surveillance described previously.

Digitizing surveillance

Already hinted at in the previous section is the change from simple video and audio taping, which then has to be watched by humans, to the so-called digitizing of analogue recordings.[56] Indeed, with the latest technology the analogue step is bypassed completely in favor of direct digital recording. This is relatively common: these days how many do not have a digital camera with a hard drive or flash card? These "digitized" recordings can then be examined by software.[57] According to Stephen Graham and David Wood, this is important for several reasons, including widening geography and real-time monitoring. This is compounded by the increasing use of automated systems that require little or

[52] See *US v. Scarfo*, 180 F. Supp. 2d 572 (DNJ 2001).

[53] Chapter IX of this study offers accountability options to be considered when addressing these concerns.

[54] For an example of the importance of this, see Tamara Dinev, Paul Hart, and Michael R. Mullen, "Internet Privacy Concerns and Beliefs about Government Surveillance – An Empirical Investigation", *Journal of Strategic Information Systems* 17 (2008): 214–33. See also Ian Brown, "Terrorism and the Proportionality of Internet Surveillance", *European Journal of Criminology* 6, no. 2 (2009): 119–134.

[55] Colin J. Bennett, "Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web", *Ethics and Information Technology* 3 (2001): 197–210.

[56] See the James Meek article on facial recognition software applied to CCTV footage introduced earlier.

[57] Stephen Graham and David Wood, "Digitizing Surveillance: Categorization, Space, Inequality", *Critical Social Policy* 23, no. 2 (2003): 227–48.

no human intervention: what Jones calls the "digital rule".[58] On the one hand, this automated processing can be used to overcome biases of human decision makers; on the other hand, the systems can be designed and built to exclude whole classes of persons with there being no overt acknowledgement that such exclusion is occurring.

Of course, these digitized recordings are stored in databases (which can be combined with other related databases and so on) which can then be further combed through in a secondary process called "dataveillance".

Dataveillance

Although not discussed in detail in this study the notion of monitoring not individuals but rather data about individuals is important.[59] Here, dataveillance is understood as the monitoring of data systems rather than of persons directly. While the ultimate end of this monitoring is to keep track of individuals it does so indirectly, making it less intrusive, more covert and less likely to be known by the individual(s) being monitored. It is important also because of the increasing acceptance of the notion that the identity of a person being watched is nothing but what is *recorded* about that person.

An important new development is the use of syndromic surveillance. This is the use of dataveillance techniques to track patterns in (nondiagnostic health information[60]) symptoms. Although originally intended to aid early intervention in the outbreak of potentially catastrophic pandemics (a worthwhile enterprise), its techniques can also be used to track patterns of any kind in any population, all without the permission or knowledge of the members of that population.[61]

RFIDs

A little-recognized form of surveillance, Radio Frequency Identification Devices (RFIDs), is beginning to be understood as a serious threat to privacy. Originally developed to manage warehouse inventories, the use of these short range devices

[58] R. Jones, "Digital Rule: Punishment, Control and Technology", *Punishment and Society* 2, no. 1 (2001): 5–22.

[59] For a history of the transition from conventional electronic surveillance to dataveillance see Mun-Cho Kim, "Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea", *International Sociology* 19, no. 2 (2004): 193–213. For more recent attempts see Yuval Elovici, Bracha Shapira, Mark Last, Omer Azzfrany, Menahem Friedman, Moti Schneider, and Abraham Kandel, "Content Based Detection of Terrorists Browsing the Web Using an Advanced Terror Detection System", in *Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security*, ed. Hsinchun Chen, Edna Reid, Joshua Sinai, Andrew Silke, and Boaz Ganor (Springer, 2008), 365–384.

[60] See Lyle Fearnley, "Signals Come and Go: Syndromic Surveillance and Styles of Biosecurity", *Environment and Planning A*, 40 (2008): 1615–1632.

[61] Leslie P. Francis, Margaret P. Battin, Jay Jacobson, and Charles Smith, "Syndromic Surveillance and Patients as Victims and Vectors", *Bioethical Inquiry* 6 (2009): 187–195.

has expanded to include tracking of employees while at work.[62] RFIDs can be read without the wearer's knowledge or permission. Indeed, some RFIDs can be placed on employee work badges, clothing or other work-specific apparel. According to Jeremy Gruber, once confined simply to location information they have in recent times been expanded to include information such as "fingerprints, social security number, driver's license number". Also, according to Gruber (and others), there are no legal constraints on the use of RFIDs in the workplace.

Participatory surveillance

Most of the discussion of surveillance so far has concerned covert practices or compulsory surveillance. Here we discuss a new and often overlooked form of surveillance: consensual or buying-in technology. This is technology that users must have in order to carry out their work/social activities but implicit in the technology is the ability to use it as a surveillance tool.

In the workplace, the use of "consent to be surveilled" as a means of claiming that the employee is "OK" with surveillance is used by employers to meet their moral obligations of "informed consent" and similar concepts. However, this consent frequently amounts to nothing more than coercion: no agreement to surveillance, no job. This is morally problematic, as the consent involved is at best superficial.[63]

In the context of ordinary society, twittering, tweeting and blogging are part of a new phenomenon, known as social networking or social media,[64] that has enormous potential for surveillance. In these technologies, people voluntarily post (hence the term participatory) information (often intensely personal) on websites that they believe (indeed hope) are accessible to millions. Although it is a social phenomenon of interest in its own right, we are interested here mainly in the ethical implications of such activity.

Many of the subscribers are teens and young adults with little experience in the adult world. One of the problems they face is that employers can, and do, check a prospective employee's activity on these social sites. Exuberant and youthful outbursts appropriate for the time may be seen in a less-than-favorable light.

[62] For an example of this, see Jeremy Gruber, "RFID and Workplace Privacy", on the National Workrights Institute website, http://www.workrights.org/issue_electronic/RFIDWorkplacePrivacy.html, December 23, 2009, and Paul Roth, "Workplace Privacy Issues Raised by RFID Technology", Privacy Issues Forum, March 30, 2006, University of Otago, New Zealand.

[63] For a more detailed treatment see, Jo Ann Oravec, "Secret Sharers: Consensual and Participatory Surveillance Concerns in the Context of Network-Based Computer Systems", *ACM SIGOIS Bulletin* 14, no. 1 (July 1993): 32–40.

[64] For an excellent examination of the issues see Anders Albrechtslund, "Online Social Networking as Participatory Surveillance", *First Monday* 13, no. 3 (March 2008). Note that this omits sites such as Facebook from consideration.

Thoughts once divulged to close friends in a cloak of intimacy and presumed secrecy are now broadcast to millions of subscribers. Such disclosures can be damaging to the individual and their friendships.[65] Friendships that are physically and emotionally close can be harder to develop as a result of a loss of a sense of whether the blogger/tweeter can be trusted with confidential information.

However, as Anders Albrechtslund says, it can be empowering: "participatory surveillance is a way of maintaining friendships by checking up on information that other people share. Such a friendship might seem shallow, but it is a convenient way of keeping in touch with a large circle of friends, which can be more difficult to handle offline without updates of personal information – untold and unasked."[66]

So what is the problem for surveillance/security? As Albrechtslund puts it, although the original intention of such sites was "mutuality, empowerment and sharing", this unprecedented level of disclosure makes possible fraud, social sorting and identity theft.[67] Surveillance by anyone with an account (which can be gained with little verification of the subscriber's identity) is automatic and easy.

Some social commentators have said that, taken to its extreme, where others post information about us on their sites, this saturation of information about the everyday and mundane is not big brother but rather little sister.[68]

[65] For a recent review, see Jeffrey Rosen, "The End of Forgetting", *The New York Times Magazine*, July 25, 2010, 30 et seq. One of the difficulties here is that privacy settings can be difficult to understand and control and, on some social networking sites, privacy policies change with some regularity and it can be difficult to keep up with the changes. Although it is arguable that young people have very different privacy expectations from those of an earlier generation, this might be questioned, see Chris Jay Hoofnagle, Jennifer King, Su Li, and Joseph Turow, "How Different Are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?", available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864. See also, "In the Matter of Google, Inc." (March 30, 2011), available at: http://www.ftc.gov/os/caselist/1023136/index.shtm.

[66] See also Dean Cocking and Steve Matthews, "Unreal Friends", *Ethics and Information Technology* 2, no. 4 (2001): 223–31.

[67] For another excellent list of worries see Christian Fuchs, *Social Networking Sites and the Surveillance Society* (Salzburg: Förderung der Integration der Informationswissenschaften, 2009).

[68] It is difficult to be certain of the origin of the phrase "little sister". Here is one claim: "The Reverend and Doctor Omed, We Are Little Sister and We Are Watching Us", http://www.dailykos.com/story/2009/4/16/720852/-We-Are-Little-Sister-and-We-Are-Watching-Us, viewed 20 January 2010:

> I would like to suggest a new meme as an overlay and even a successor to Big Brother: Little Sister. Little Sister is everyone who carries a cellphone with a digital camera that can upload pics and viddy to the intertubes. Little Sister is whoever cops a feed off Fox News, and everyone who posts it online. Little Sister is the "Macaca" who provided now former Senator George Allen an opportunity to destroy his political career. Little Sister is the 3 or more BART riders who viddied BART policeman Johannes Mehserle shooting Oscar Grant as Grant lay prone on the floor of the car. Little Sister is an emergent property of people interacting via the ever-faster global communications grid and all the technologies, software, and infrastructure that make, extend, and connect it.

Resisting surveillance[69]

Also called privacy-enhancing techniques, resisting surveillance has a history as long as surveillance itself. There are many ways in which individuals and privacy-seeking groups have sought to respond to the aforementioned surveillance techniques. Gary Marx identified some eleven ways of resisting by neutralizing the effect of surveillance.[70] In discussing ways of resisting online profiling, Ira Rubinenstein et al. mention multiple identities, cookie-blocking settings and commercially available tools such as the Anonymizer,[71] as well as techniques including onion-routing, unlinkable pseudonyms and anonymous credentials.[72] Some additional examples of resisting-surveillance technologies are: encryption (the most well-known being public key cryptography) and steganography (the art/science of secret writing. In the modern context this most commonly amounts to embedding information within images). Indeed, for almost every piece of surveillance technology there is a counter technology.

Onion-routing is the routing of a message through a series of proxies, each of which has an unpredictable path with limited information about where the message has come from or is going to.[73] *Unlinkable pseudonymy* is the creation of multiple pseudonyms for a single identity, each of which cannot be linked to any of the other pseudonyms. This allows a person to sign up anonymously to several websites without revealing that he or she is the same person. Credentials are needed to satisfy sign-on requirements for loyalty programs, website registration and the like. These are requested to ensure that the person signing on is genuine and not, for example, a web-crawler. *Anonymous credentials* have the feature of providing verification information without revealing the identity of the real or genuine person.

[69] For a general theory of resisting surveillance, see Aaron K. Martin, Rosamunde van Brakel, and Daniel Bernhard, "Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework", *Surveillance & Society* 6 no. 3 (2009): 213–32.

[70] Gary T. Marx, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 59, no. 2 (2003): 369–90. The eleven ways are: discovery, avoidance, piggybacking, switching, distorting, blocking, masking, breaking, refusal and cooperative and counter-surveillance.

[71] See http://www.freeproxy.ru/en/free_proxy/cgi-proxy.htm (viewed 20 January 2010) for an extensive list of anonymizing tools. To quote from the web page (http://www.online-proxy.net/), "Online-Proxy.net is a free web based anonymous proxy service, which allows anyone to surf the web privately and securely."

[72] Ira S. Rubinstein, Ronald D. Lee, and Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", *University of Chicago Law Review* 75, no. 1 (2008): 261–85, esp. 274–80.

[73] This belongs to a class of technology called anonymous remailers. See, for example, Wayne Madsen, "FBI's Communications Surveillance Capabilities Widen", *Computer Fraud & Security*, 2000, no. 10, (October 2000): 16–17; George F. du Pont, "The Time Has Come For Limited Liability For Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils", *Journal of Technology Law & Policy* 6, no. 2 (2001): 175–218, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

Not only do these technologies protect the privacy of individuals but they are also indiscriminate in that they serve to block (or at least make more difficult) both commercial surveillance as well as police efforts to track or uncover criminals, terrorists and the like.

Although the above discussion has focused on ways of avoiding surveillance, there are also methods used by surveillance technology to limit its own reach. Yu et al. describe a method whereby visual surveillance technology can limit its access into personally identifying information.[74] Through the use of abstraction operators, the system known as PriSurv can limit the degree and kind of information the system can display, though the authors note that "excess visual abstraction makes video surveillance meaningless."[75] There are other techniques, such as pixelization, blurring and blacking out that also achieve the aim of making sensitive information unavailable. Of course, the use of all of these techniques is at the discretion of the operator/programmer.

Steganography[76] usually refers to the use of covert or hidden writing but can be expanded to include any form of communication. As Gary Kessler points out, this is different from *cryptography*, which makes the communication unreadable but does not seek to hide the communication itself. Combining the two technologies can make for a very powerful way of resisting digital surveillance. Steganography can take many forms – from the microdots of B-grade spy movies to more ancient techniques such as invisible ink (so-called technical steganography). This method of avoiding communications being surveilled has received renewed interest recently with the increased sophistication of digital technologies. With these new technologies communications can be hidden in image or audio files. Data can be hidden in unused file space or file headers. All digital communications are packaged into some form through protocols. The most commonly known and used protocols are Internet Protocol (IP) and Transmission Control Protocols (TCP). Information can be hidden inside segments of these carriers. Finally, hard disks can be divided into secret partitions which are undetected by normal surveillance or scanning technologies. Of course steganography is available to terrorists as well as others.[77]

[74] Xiaoyi Yu, K. Chinomi, T. Koshimizu, N. Nitta, Y. Ito, N. Babaguchi, "Image Processing, 2008", ICIP 2008, 15th IEEE International Conference, October 12–15, 2008, 1672–75.

[75] *Ibid.*, 1673.

[76] See Gary C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner" (an edited version), *Forensic Science Communications (Technical Report)* 6, no. 3 (July 2004), available at: http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm; http://www.garykessler.net/library/fsc_stego.html.

[77] See Rebecca Givner-Forbes, *Steganography: Information Technology in the Service of Jihad* (Singapore: The International Centre for Political Violence and Terrorism Research, a Centre of the S. Rajaratnam School of International Studies, Nanyang Technical University, 2007).

(B) Second Data Mining[78,79] and Integration/Matching[80]

By way of introduction . . .

If you order many of your books from Amazon.com and use the Amazon web site as a convenient way to check on book data (authors' initials, exact titles, publishers, dates of publication, editions etc.), you will also be aware that you subsequently receive emailings from Amazon indicating that people who have shown interest in your book have also shown interest in other books that Amazon is now happy to let you know about. Amazon has applied an algorithm to the large amount of data that it amasses/warehouses as a result of site visits, which is used to gauge your purchasing proclivities. It then dangles before you the possibility of additional purchases in line with "interests" you have shown. The overall process of determining what data is to be retained, amassing it, patterning it and acting on it is often referred to in literature as knowledge discovery; within that knowledge discovery process data mining is the application of algorithms to enable predictions or judgments to be made.[81]

[78] The term "data mining" is somewhat of a misnomer. It conventionally means sifting through large amounts of information, usually held in one database, in search of specific pieces of information or data. Traditional mining is always held to have a reason for believing that mining a specific location will likely result in the discovery of a particular mineral. Gold mining is looking for gold using a body of knowledge that says that certain geographical formations are likely to contain deposits of gold. Data mining does not work like this. Usually there is scant or little information that even so much as implies that specific information looked for is contained in the database being searched. In the case of Amazon, described below, the intent of the data mining is not so much to find information but to create information using the available database. Using the gold mining example at its best, the Amazon activity is like using the surrounding minerals in a deposit to create gold and then calling this activity/process gold mining. At its worst, what Amazon is doing is more like taking whatever materials can be found in a given location, combining them using the laws of chemistry and calling whatever is produced an intended result. This is hardly mining in the traditional sense.

[79] Of course, data mining for national security or policing is not the only use. Perhaps of even more importance and worry for privacy is data mining by corporations in which, according to John Soma et al., there is an equating of information with financial value. See John T. Soma, et al., "Corporate Privacy Trend: The 'Value' of Personally Identifiable Information ('PII') Equals the 'Value' of Financial Assets", *Richmond Journal of Law & Technology* 15, no. 4 (2009), available at: http://law.richmond.edu/jolt /v15i4/article11.pdf.

[80] A note on terminology: in some countries the common term for the aligning of information across a number of disparate sources is termed "data integration" and in others it is termed "data matching." Matching is the more correct term when discussing the use of collected information to be used as a predictive tool. Integration implies the simple putting together of information whereas matching implies the more important (in this context) putting together of information that, when put together, adds value or is said to "match".

[81] Kim Taipale offers the following useful differentiation and breakdown: "The steps that compose the knowledge discovery process are (1) pre-processing (including goal identification; data collection, selection, and warehousing; and data cleansing or transformation), (2) 'data mining' itself, and (3) post-processing (including interpretation, evaluation and decision-making or action)" (see "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data", *Columbia Science and Technology Law Review* 5 (2003): 24–25). In 2005, the Department of Homeland Security Privacy Office used the following definition: "Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. Data mining consists of more than collecting and managing data; it also includes analysis and prediction." In 2006, as the result of a House demand, the definition was changed to: "a query or search or other analysis of 1 or more electronic databases, whereas – (A) at least 1 of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired

Although such predictions can show an uncanny ability to track books that might be of interest to you, they can also be a bit irritating if some of the books you purchased were purchased for other people or if the tracked volume was simply a footnote reference for which you needed a publisher. The algorithm should be sophisticated enough to screen out "casual" visits that do not say anything – or anything accurate – about your reading interests.

Such is one use of data mining. There are many others. Data mining can be used to provide an understanding of human behavior,[82] forecast trends and demands, track performance or transform seemingly unrelated data into meaningful information.[83]

The importance of data mining and integration was highlighted by the events of 9/11, when it subsequently turned out that a number of those involved in the attacks were already on the radar screens of security officials and that there were even data to suggest that a terrorist attack was imminent. One of the things the attack revealed was that government agencies charged with responsibility for preventing such occurrences were not adequately equipped to analyze, evaluate and integrate the data available to them. Nor, as it subsequently turned out, were they equipped to tackle the information in a manner consistent with the values of a liberal society – that is, with due regard for privacy and other civil liberties. Outcries stemming from this lack of attention to liberties resulted in the proposed Total/Terrorist Information Awareness (TIA)[84] program being abandoned and the updated Computer Assisted Passenger Prescreening (CAPPS II) program (now Secure Flight) being delayed by a number of years.

Ethical questions arise at every step of the data mining process. In what is referred to as the "pre-processing" stage, for example, decisions must be

initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement; (B) a department or agency of the Federal Government or a non-Federal entity acting on behalf of the Federal Government is conducting the query or search or other analysis to find a predictive pattern indicating terrorist or criminal activity; and (C) the search does not use a specific individual's personal identifiers to acquire information concerning that individual." The change had consequences: some "data mining" activities discussed in the 2005 report were not reviewed in the 2006 report, and some reviewed in the 2006 report had not been considered in the 2005 report.

[82] In an unusual take on the problem, Andrew McClurg, "A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling", *Northwestern University Law Review* 98, no. 1 (2006): 63–143, claims that a serious concern is that data mining by businesses could result in complete dossiers of individuals that would give businesses a better understanding of an individual's purchasing patterns than the individual themselves is consciously aware of. According to McClurg, this better profile could then be appropriated without permission and used to target similar in-profile persons.

[83] The algorithms used for data mining vary considerably in kind and sophistication. There are many commercial packages available, often directed at or customized for niche concerns (marketing, law enforcement etc.), and purpose-oriented institutions (e.g. Google) often develop their own. Organizations concerned with tracking terrorist activity (e.g. the FBI, the CIA) may draw on commercial as well as internal databases in seeking to identify links and patterns that warrant further investigation. See Chapter VII.

[84] For an overview of TIA see Leslie Regan Shade, "The Culture of Surveillance: G-Men Redux and Total Information Awareness", *Topia* 9 (2003): 35–45.

made about the goals to be served by the data mining. Is it simply to identify (potential) terrorists or are other goals also contemplated (e.g. organized crime, money laundering, tax fraud)? The moral worthiness of the goals will obviously have some bearing on the privacy risks that might be justified. "Potential" also operates as something of a weasel word: what level of probability will satisfy that?[85] Goals will also need to be tempered by ethical considerations (for example, those mandated by liberal democratic values).[86] When it comes to data collection, decisions will need to be made about where the data are to come from and whether their sources avoid illegitimate breaches of privacy. Data given to institutions for certain limited purposes should not normally be used for other purposes.

The Department of Homeland Security's (DHS) Office of Inspector General (OIG) helpfully classifies data mining activities into two groups; commercial and government. In this security context we are interested primarily in those of the government.[87] These include: monitoring employee expenditures; speeding up employees' security clearance investigation process; identifying improper payments under federal benefit and loan programs and helping to detect instances of fraud, waste, and abuse; ranking government programs quickly; and assisting law enforcement in combating terrorism.

Government data mining is more or less coincident with the development of data mining technologies. Prior to 9/11 it was employed to combat various kinds of criminal activities, (such as money laundering, drug trafficking and tax fraud) but since 9/11 significant data mining efforts have also been directed at the prevention of terroristic acts and the apprehension of aspiring terrorists. An array of software has been developed and/or used to discover patterns and relationships and to make predictions or define rules that can be used in the so-called war on terror.

In August 2006 the OIG released its *Survey of DHS Data Mining Activities*, in which it described 12 data mining activities carried out under the aegis of the DHS. The list was not meant to be exhaustive, nor was it confined to operational data mining activities – it included several that were "under development",

[85] Cf. the old feminist slogan: "All men are potential rapists."

[86] As with any means-end reasoning, the use of data mining techniques must satisfactorily respond to the relevant questions that such reasoning generates.

[87] The commercial uses are given as: to analyze and segment customer buying patterns and identify potential goods and services that are in demand; to identify and prevent fraudulent and abusive billing practices; to analyze sales trends and predict the effectiveness of promotions; to predict the effectiveness of surgical procedures, medical tests and medications; to search information from a number of documents and written sources on a particular topic (text mining); and to identify trends and present statistics in ways that are easily understood and useful. From the Office of Inspector General, Department of Homeland Security, *Survey of DHS Data Mining Activities*, OIG-06-56 (Washington, DC: Office of Information Technology, August 2006), 6, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-56_Aug06.pdf. Although the survey distinguishes commercial and government uses, it does not as clearly say that government purposes are outsourced to commercial data miners. See Chapter VII.

and there may well have been others that were “classified”. Nevertheless, it is interesting to review some of the kinds of data mining activities because of the different ethical challenges that they provide.

The OIG survey distinguished several types of analytical processes that arguably come under the umbrella of data mining:

- *Expert systems*: programs designed to analyze information about a specific class of problems, analyze the problems themselves and, usually, to recommend courses of action (e.g. the Automated Commercial Environment Screening and Targeting Release S1 (ACE S1) that, from a centralized data base, identifies high risk cargo shipments for further detailed examination).
- *Association processes*:[88] processes which link two or more variables (e.g. persons and place), for example, the Immigration and Customs Enforcement Pattern Analysis and Information Collection System (ICEPIC) that works with various DHS databases to detect patterns and relationships and enable investigators to conduct targeted checks of non-resident aliens.
- *Threat and risk assessment tools*: tools that identify, prioritize and help to reduce risks. These include the Risk Management Reporting System (RMRS) that collects information and scores it based on the level of risk posed to national assets (such as maritime facilities, airports and mass transit).
- *Collaboration and visualization processes*: processes that collect, tag, classify, organize and apply appropriate material and expertise and then represent it in an illuminating visual form (e.g. Numerical Integrated Processing System (NIPS), a web-based tool that assists agents in identifying anomalies indicative of criminal activity – immigration violations, customs fraud, drug smuggling and terrorism).
- *Advanced analytics*: analytics that ingest information and facts from diverse types of data, both structured and unstructured, and then provide simulation and modeling tools for analysts (e.g. Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE), a meta-tool that had not been implemented at the time of the report but which was intended to incorporate and integrate comprehensive chemical, biological, radiological, nuclear and explosive threat and effects data).

Means and ends

What privacy and other ethical issues are raised by such data mining activities? Because data mining is a purposive activity – a means employed to achieve

[88] This is also known as relational surveillance. See, for example, Katherine J. Strandburg, “Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance”, *Boston College Law Review* 49, no. 1 (2008): 1–81.

certain ends – it is important to keep in mind the following questions: Are the ends good or good enough? Are the ends proportionate to the means? Can the ends be secured in a less-invasive manner? Will the means secure the ends? Is there something intrinsically problematic about the means? Will the means have deleterious consequences making their use inappropriate?

These questions, which are overlapping rather than completely discrete, can more or less arise at every step of the data mining process: definition of the problem to be solved, data identification and collection, data quality assessment and data cleansing and, finally, data modeling (building, validation and deployment). Such a process is iterative, because information learned in later steps may lead to a clarification of and adjustments to earlier steps.[89]

Good (enough) ends

It needs to be determined that the purposes for which data are being gathered and manipulated are legitimate, both ethically and legally. So data that are oriented more to the detection of political dissent than to the prevention of clearly defined national disasters are likely to be problematic just because the legitimacy of the ends to be served is questionable. Legitimate ends, moreover, will need to be sufficiently important to warrant the devotion of the government resources that will be required. There may also need to be a determination of whether the interest of a particular agency is legitimate – that is, whether it falls within its authority to gather and analyze such data. That may be problematic for cases in which (for reasons of efficiency) different agencies jointly gather data. Connected with this requirement (and touching on others as well) will be questions about confining the use of data to the purposes for which they were originally gathered; there are often memoranda of understanding between agencies that allow information that is gathered for one purpose (say, terrorism) to be shared with other agencies concerned with another (say, financial crime). Are such extensions justified? "Mission creep" is a common problem; although it seems cost-efficient, it may violate important privacy protections. Apart from any impropriety that may be involved, it is also possible that data collected for one purpose are not in a form that is well-suited (or of adequate quality) for another purpose. Moreover, as data are shared, control over the uses to which they are put and security controls on the data themselves are often lost.

[89] Useful documents are Maureen Cooney, *Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties* (Washington, DC: DHS, July 6, 2006), available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_data_%20mining_%20report.pdf; and Hugo Teufel III, *2007 Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties* (Washington, DC: DHS, July 6, 2007), available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2007.pdf.

Proportionate means/ends

Ends may be legitimate without being important enough to justify the kinds of means that are contemplated or employed to achieve them. Data mining, given the risks to civil liberties associated with it, is likely to be justifiable only if important ends are at stake. Some – but not all – crime is likely to qualify, and a judgment needs to be made about the legitimacy of using scarce government resources to mine data for particular purposes, given the seriousness of the issues and the available alternatives.

Restrictive means/ends

As well as some proportionality of means and ends, the means should be as little restrictive/invasive as possible. Could anonymized data be used rather than identifiable data? – a critical question when data might be shared among agencies. *Ceteris paribus*, other ways of achieving the ends, if less invasive, should be chosen. Such a requirement impacts on the issue of data retention: are the data to be kept permanently or should they be discarded after a determinate period of time? Agencies are strongly tempted to hold onto data "just in case" they turn out to be useful at some future date. However, the longer data are kept the more likely it is that they will become outdated. The principle of the least restrictive alternative may also have an important bearing on the target data: whether the software should operate dragnet style or be more tightly circumscribed.

Calibrated means/ends

The means have to be appropriately calibrated to the ends so that they are likely to be effective in achieving the ends for which they are employed. It needs to be established that accessing a particular raw data set is appropriate to the investigation at issue – that is, that it is likely to contain relevant information – and that the software used is likely to capture it and process it in a way that will enable the ends to be realized.

The ethics of scientific/experimental design

This is also important with regard to the "cleansing" of raw data – that is, the removing of inaccuracies and coping with incompleteness in such a way that patterns, relationships and rules will be accurately depicted. The issue of reliability is important not only when developing the modeling software but also at the point of its application to actual data, lest false positives lead to unwarranted invasions of rights. (False negatives can be a problem too.) Furthermore, the kinds of patterns that software tracks do not *ipso facto* constitute meaningful or causal relationships, and so caution needs to be exercised with respect to the kinds of conclusions that are drawn from them. They should be seen as investigative tools rather than probative techniques.

Appropriate means/ends

Although some data sets are likely to be public and involve no breaches of privacy that is not always the case. The privacy-invasive character of the means will have to be taken into account along with more instrumental questions about the suitability of the means to achieving the ends. These are not simple "balancing" issues – they require attention to the trade-offs involved. Where collected data are privacy-invasive there should be sufficient transparency and oversight for there to be effective means of redress in the event that privacy is improperly invaded or inappropriate conclusions are drawn.

Unintended consequences

Finally, unintended side effects will need to be addressed, for example, the augmentation of governmental power and the increased vulnerability of a (particular) population should governmental policies shift in a demagogical direction. Other side effects might include the vulnerability of a population to other threats as a result of inadequately secured data. Hackers, spies and others may have reasons for wanting to access data that has now been conveniently gathered for them.[90]

As we have already noted by implication, conceptions of privacy and formulations of privacy law have not developed *in vacuo* but have been significantly influenced by historical circumstances. Consider a few salient ones. Americans, because of their founding history, have always had an issue with the power of central government and hence with activities – such as surveillance – that would appear to enhance governmental power. At the same time, American dedication to the market as a distributor of social goods has often left it less concerned with the private mining and assembling of data. Offsetting this has been the concern that Warren and Brandeis expressed about the growth of the media and telecommunications, and the potential that they had for both governmental and private intrusions into space/activities that should be left alone. European countries have similarly been affected by historical events. In 1944, during the Nazi occupation of Norway, the Nazis decided that the German army needed a further infusion of soldiers. It was decided to conscript Norwegian men based on factors such as their age, using government files. Unable to destroy the files and thus to thwart this initiative, the Norwegian resistance succeeded in

[90] In each of the scenarios of means/ends relationships and unintended consequences the value of Techno-ethics Boards is clear. As bodies charged with unpacking these problems, the insight and guidance that emerge would, it is hoped, clear away many thickets early rather than forcing retroactive action.

destroying the two machines used to sort the files, so the conscription plan had to be dropped. The lesson about the vulnerability of innocently centralized data was, however, imported into European privacy law.[91] Combine this with the accusation that IBM was instrumental in assisting the genocide program of the Nazis through allowing them access to their sorting machines, and it can be seen why there is a special nervousness about privately gathered data in the EU.[92]

Overall, Americans seem more complacent than Europeans[93] about the centralized gathering of certain kinds of data about its citizens. Although it caused an uproar when discovered in May 2006, the revelation that the National Security Agency (NSA) database contained at least five years' worth of the call records of tens of millions of US citizens – calls that had been routed through AT&T and Verizon/MCI – indicated the ease with which governmental authorities were able to get access.[94] The NSA may have acted illegally, though the activity was probably not as dicey as the earlier-discovered warrantless wiretapping that the US government subsequently made efforts to kosher.[95] In the European context, the mining of such data would have required a public law reviewed by an independent privacy agency and, even if access could have been gained by an intelligence agency, the data would not have been able to be retained for as long as the NSA had retained its data.

The NSA data gathering occurred shortly after 9/11, when it approached the major telecommunications carriers for customer call records (from one number to another, giving time and duration of call) and for regular updates of such. Some

[91] It would have been interesting to see whether the recent loss of data in the UK would have derailed plans for a national ID card. See Eric Pfanner, "Data Leak in Britain Affects 25 Million", *The New York Times*, November 22, 2007. However, the change of government has rendered this moot.

[92] Edwin Black, *IBM and the Holocaust* (New York: Time Warner Paperbacks, 2001).

[93] "Europe" is somewhat ambiguous. It may refer – more narrowly – to those countries that constitute the European Union (currently comprising twenty-seven states: http://en.wikipedia.org/wiki/European_Union_member_state) or – more broadly – to those forty-seven countries that comprise the Council of Europe (http://en.wikipedia.org/wiki/Council_of_Europe). The discussion here will (primarily) concern the second, though it generally encompasses the first.

[94] See Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls", *USA Today*, May 11, 2006, A1; Susan Page, "Lawmakers: NSA Database Incomplete", *USA Today*, June 30, 2006, A1.

[95] See "Legal Authorities Supporting the Activities of the National Security Agency Described by the President", *Indiana Law Journal* 81 (2006): 1374. With regard to the call records, most of the current debate concerns whether the telecommunications companies involved should be granted immunity if it turns out that they acted contrary to legal requirements. ECPA (1986), which bears on the NSA initiative, requires – in its Stored Communications Act (U.S.C. §§2701 – 2711) – that companies can disclose their records to the government only under certain conditions, for example, if the government obtains a warrant, court order or administrative subpoena such as a national security letter (18 U.S.C. §2702 (c)). In the present instance, the information was handed over without any warrant. However, if it can be established that the President's inherent constitutional power takes precedence, that may relieve the telecommunications companies from liability. With regard to the warrantless wiretapping, however, FISA almost certainly required a warrant – hence the koshering activity of the Protect America Act of 2007. Given FISA's explicitness, the appeal to Article II of the Constitution was not very convincing (see *Youngstown Tube & Sheet, Co. v. Sawyer*, 343 U.S. 579, 635–38 (1952, J. Jackson, concurring), for the president's powers are at their "lowest ebb" when exercised contrary to "the expressed or implied will of Congress".

companies complied; others (Qwest, BellSouth) did not. This information was subsequently mined, though exactly how is not clear. Were they, for example, used to generate certain hypotheses about who might be engaged in terrorist activities, or were they used to target those who had previously been suspected of terrorist sympathies?

However the data were (or are) being used, the situation in the US is markedly different from what is possible in Europe for a number of reasons. Firstly, in the US a distinction is drawn between content and incidents, that is, between the *substance* of a communication between A and B and *date-time stamps* of communication between A and B (i.e. between the "letter" and the "envelope"). The former is generally well-protected in the US, but in Europe both kinds of data are protected (though even there it is recognized that content deserves greater protection than incidents). Secondly, there is a distinction that functions more stringently in Europe than in the US between personal and other kinds of communication data. European countries are far more protective (with respect to both government and private actors) of a broad category that encompasses "all types of personal data", whereas US law focuses on specific kinds of personal data, such as health and financial information, video-store records etc. Thirdly, a further distinction concerns the purposes for which data are collected, whether for law enforcement or national security. In both Europe and the US, constraints on law enforcement data gathering are more stringent than those on national security data gathering. In part this is because law enforcement has more dramatic consequences for individuals than national security intelligence gathering. Finally, as far as national security interests are concerned, European agencies pay attention to domestic as well as foreign threats to national security, whereas the US has until recently viewed national security in terms of foreign threats (covered by the CIA and NSA) regulated by FISA. The FBI, which covers both federal criminal investigations and domestic intelligence, is covered by regulations mostly attuned to law enforcement matters. It was the lack of an assigned domestic national security agency that led to the NSA taking it on.

Fourth Amendment jurisprudence allows the mining of call records. It is argued that because the records are available to the phone companies themselves they are not private in the way that the content of a phone conversation is.[96] Rather than doing the mining itself the NSA simply requested the information from telecommunications providers. The failure of such jurisprudence to provide for the comprehensive protection of personal data constitutes a major difference between US and European law on data protection/privacy.

[96] Compare *Smith v. Maryland*, 442 U.S. 735 (1979) with *Katz v. United States*, 389 U.S. 347 (1967). Cf. also *United States v. Miller*, 425 U.S. 435 (1976), where it is argued that users of certain services "assume the risk" that their information will be made known to others.

Nor does the Privacy Act of 1974 provide much solace. True, it imposes several duties on government agencies: to alert the public to the existence of a records system; to reveal its purposes; to collect data that are relevant to those purposes only; to ensure the accuracy and timeliness of the mined data; to not transfer information to other agencies without the consent of those whose data are being mined; to guarantee the security and confidentiality of the acquired data; and to give those concerned a right to check and have corrected the data concerning them. This sounds pretty good, but closer inspection suggests otherwise. The Act has few teeth and it provides for many exceptions that cover most of the current contested uses, provided that notice is given to that effect (for example, unless secrecy is in the interest of national defense).

In Europe, the situation is significantly different. Data mining of the kind indicated by call records requires a law to permit it that explicitly specifies the purposes for which the data are being gathered and the limits that will be observed in their gathering, use and retention. Because data mining requires a specific law allowing it, there is likely to be public debate over its purposes and the kinds of data that will be aggregated and mined. It is most likely that only anti-terrorist purposes would be legitimated and then only in the event of a "concrete danger." Even an intelligence agency would have to conform to the latter expectation, in which there is some individualized suspicion,[97] and would not be permitted to retain the data for as long as the NSA has had it: three years is about the European limit (though between six months and two years is more common). In European law, individuals also have a right to check on the accuracy of information gathered about them, something that is denied to Americans.

Data mining has the potential to provide many legitimate benefits, especially to law enforcement agencies. However, data mining, in many of its forms and with the right sort of technology,[98] can also represent a serious threat to democratic values such as privacy and autonomy. Accordingly, there is a need to determine the ethical constraints that should apply to data mining and to devise and implement appropriate accountability mechanisms.

Of course, data mining can be an important tool in profiling.[99]

[97] German law, however, does permit strategic surveillance of international phone calls as part of an anti-terrorism initiative.

[98] Such technologies are being developed all the time. For a recent example of such technology see N. Memon, H.L. Larsen, "Investigative Data Mining Toolkit: A Software Prototype for Visualizing, Analyzing and Destabilizing Terrorist Networks", in *Visualising Network Information* (2006), 14-1–14-24. See also the so-called Investigative Data Mining techniques, Nasrullah Memon, "Detecting Terrorist Activity Patterns Using Investigative Data Mining Tool", IFSR 2005: Proceedings of the First World Congress of the International Federation for Systems Research: The New Roles of Systems Sciences For a Knowledge-based Society, Nov. 14–17, 2123, Kobe, Japan.

[99] As an example of this crossover, see Ira Rubinstein, Ronald D. Lee, and Ira Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches". Other technologies can also be

(C) Profiling[100, 101]

> *The process of reaching out to foreign nationals and their communities fostered new trust between law enforcement and these communities.*[102]

In the introduction to *Profiles, Probabilities and Stereotypes*, Frederick Schauer states that his purpose is to challenge "the primacy of the particular" – that is, the view that our decisions have to be guided exclusively or primarily by the particulars of a case rather than by generalities that we can bring to it. As he puts it, he seeks to "defend the morality of decisions by categories and by generalizations, even with its consequent disregard for the fact that decision-making by generalization often seems to produce an unjust result in particular cases."[103] He makes it very clear, however, that what follows from this is not that all generalizations (in the form of stereotypes or profiles) will pass ethical muster – even when they have a sound statistical basis – only that some may.

The notorious profiled New Jersey Turnpike stops were almost certainly based on spotty evidence. Schauer compares the profiling involved there with that developed by Bob Vogel, the Florida Highway Patrol officer who became famous for his drug interdiction work. Vogel's profile was based on his thirty biggest drug arrests; it was not meshed with the experience of others or moderated by the experience of stops that yielded nothing. New Jersey's profiling was hardly better grounded and, Schauer writes, "the original New Jersey procedure ought not to be glorified by referring to it as a 'profile,' for it would be more accurate to call it a 'guess'."[104]

difficult to classify according to the standard grouping such as surveillance and profiling. See, for example, Sudhir Saxena, K. Santhanam, and Aparna Basu, "Application of Social Network Analysis (SNA) to Terrorist Networks", *Strategic Analysis* 28, no.1 (January–March 2004): 84–101.

[100] Although this study focuses on profiling in military and criminal contexts, its uses in the commercial sector can be just as worrying, morally speaking. See, for example, Axiom software's DISC system, in which they offer commercial, personal, reselling, and hosting and profiling services at http://www.axiomsoftware.com, viewed December 10, 2009.

[101] An emerging technology for profiling (and other security issues) is translation technology. Roughly, this is the use of computers to translate documents, audio and sundry foreign (i.e. not English) language sources used in profiling. It is justified as a way of speeding up the processing of such sources. For Érika Nogueira de Andrade Stupiello, there is the fundamental problem of "the illusion that the machine is able to translate", in "Ethical Implications of Translation Technologies", *Translation Journal*, 2007, at http://translationjournal.net/journal/43ethics.htm, viewed January 3, 2010.

[102] Attorney General John Ashcroft, commenting (March 20, 2002) on the "voluntary" interview program initiated by the US government on November 9, 2001 http://www.yale.edu/lawweb/avalon/sept_11/ashcroft_018.htm. Some 5,000+ young men who had recently entered the United States on visas from "countries with suspected terrorist links" were individually "invited" to talk with government agents about their reasons for visiting, past movements, knowledge concerning 9/11 and feelings about the same. Few felt able to refuse. A follow-up group of a further 3,000+ was indicated in the March 20 announcement.

[103] Frederick Schauer, *Profiles, Probabilities and Stereotypes* (Cambridge, MA: Harvard University Press, 2003), ix.

[104] Schauer, 192. This irks David Harris, who sees the kind of profiling that the New Jersey state police engaged in as exactly what the public thinks of as profiling. It might have been smarter for Schauer to have

A far more sophisticated example, one that Schauer holds up as something of a model, is the FBI's serial killer profile. The people who constructed this profile studied everything they could on serial killings, interviewed serial killers where they were able and gathered whatever other information they could that would be relevant, before painstakingly analyzing it in the process of developing a profile of "serial killer indicators". These, however, were to be used only after a field of suspects had been narrowed in order to determine who might be the most likely one. As we saw several years ago, however, in the case of the Washington snipers, too great a dependence on a profile, even a well-developed one, can lead one astray. On more than one occasion, John Muhammad and Lee Malvo were "passed over" by searching police because the profile had pointed them in the direction of a lone white male.[105] Indeed, Simon Cole and Michael Lynch suggest that "the construction of DNA databases in Britain, the United States, and elsewhere shifts criminal investigation toward suspect populations and statistical suspects."[106]

CAPPS

Since 9/11 there has been an upsurge in the profiling of airline passengers.[107] Early profiling was done by way of CAPPS (Computer-Assisted Passenger Prescreening System), developed initially in 1997 by a White House Committee chaired by Al Gore.

The first CAPPS profile made no reference to race or ethnicity except to exclude it (without providing reasons). It focused on factors such as gender, age, form of purchasing the ticket (cash or credit card, last minute or well in advance, direct or through a travel agent), membership of a frequent flyer program, time of check-in, type of luggage, presence or absence of a hotel or rental car reservation at destination, demeanor etc.[108] Even so, it was shown that CAPPS could be easily circumvented through such algorithms as Carnival Booth.[109]

seen it as a profile informed more by prejudice or guesswork than by careful development, rather than not seeing it as a profile at all. See Harris's review of Schauer in "Profiling: Theory and Practice", *Criminal Justice Ethics* 23, no. 2 (2004): 51–57.

[105] Jennifer Daw Holloway, "The Perils of Profiling for the Media: Forensic Psychologists Speak Out on the Lessons Learned from the Washington-Area Sniper Case", APA Online http://www.apa.org/monitor/jan03/perils.html.

[106] Simon A. Cole and Michael Lynch, "The Social and Legal Construction of Suspects", *Annual Review of Law and Social Science* 2 (December 2006): 39–60 (doi: 10.1146/annurev.lawsocsci.2.081805.110001).

[107] A practice that was upheld by the Supreme Court in *US v. Sokolow*, 490 US 1 (1989).

[108] Schauer, 184.

[109] Samidh Chakrabarti and Aaron Strauss, "Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System", *Electrical-Engineering-and-Computer-Science* (2002), available at: http://www.mit.strathmore.edu/NR/rdonlyres/Electrical-Engineering-and-Computer-Science/6-805Fall-2005/4E484655-6947-4D60-B789-32F2FFE6199A/0/caps.pdf, viewed December 18, 2009.

The events of 9/11 prompted calls for the revision of CAPPS, one that would provide a "risk score" for air travelers. As we have already had occasion to observe, the proposed revision – CAPPS II – came to grief in 2004 over civil rights and privacy issues, and the new system, Secure Flight, was frequently delayed by privacy concerns.[110]

Geographic profiling

Geographic profiling is the use of "knowledge about the relative locations of an offender's crime sites to predict the highest probable location of his or her residence (or some other anchor point, such as a work place)."[111] Although this technology has its origin in domestic serial crimes, recent work has attempted to use it to find the home base of other kinds of offenders, particularly terrorists.[112] Such profiling uses several assumptions about the criminal/terrorist/insurgent (here we shall refer to them as offenders). These assumptions are: multiple offenses by a single offender; the relative closeness of the offenses to the home base of the offender; the distribution of the offenses; and a stationary home base. The profile identifies an area within which the probability of an offender's home base is measured. This then allows those using the profile to target locations with the highest probability. Further it is used to prioritize probable offenders based on how closely their home base is to the site of the offense.

This form of profiling is highly dependent upon the accuracy of the underlying assumptions. If any of the assumptions is inaccurate then the profile is useless. However, as has been observed:

> An analysis of such factors was not possible within this chapter because of a lack of detailed data, but such an analysis must be carried out before any firm conclusions can be reached about whether geographic profiling techniques have the potential to be effective [for profiling terrorists].[113]

[110] For official materials, see http://www.tsa.gov/public/display?theme=5&content=09000519800cf3a7.

[111] Craig Bennell and Shevaun Corey, "Geographic Profiling of Terrorist Attacks", in *Criminal Profiling: International Theory, Research, and Practice*, ed. R. N. Kocsis (Totowa, NJ: Humana Press, 2007), 190.

[112] National Technology Alliance, *Geographic Profiling and the Hunt for Insurgents* (2007), available at: http://www.nta.org/docs/Geoprofiling.pdf, accessed on February 15, 2007.

[113] Bennell and Corey, "Geographic Profiling of Terrorist Attacks," in *Criminal Profiling: International Theory, Research, and Practice*, 201.

(D) Limitations of Technology[114]

All this discussion of the use of technology in trying to secure our society may incline us to the conclusion that all technology does is cloud the security issue with both certainty (though this, as it turns out, is false) for those ignorant of the actual capabilities and limitations of technology, and pessimism in those who are not.[115] John Gentry succinctly summarizes the systemic problems stemming from the US military's approach to technology.[116] According to him, these problems are: narrow applicability; vulnerable infrastructure; easy countermeasures; and institutional impediments.

The efficacy of technology can be assessed on (at least) two fronts: the quality of the technology and the information needed to make it useful; and the way the technology is used.

Quality of information and quality of technology

There is a common phrase in the information technology field – "garbage in, garbage out"[117] – which is both a swipe at the unwarranted trust that people put in the output of computers and a succinct way of saying that the quality of the output is absolutely dependent upon the quality of the source of the information used. Although the military does not reveal the nature or extent of the quality of its information or information technology, we can, given its record in the rest of technology development and use, deduce that its record is similar to commercial systems and that there are significant problems with its

[114] The point of this is not to deny that technology, especially information technology, can be used effectively in the military or security fields. See Nicholas S. Argyres, "The Impact of Information Technology on Coordination: Evidence from the B-2 'Stealth' Bomber", *Organization Science* 10, no. 2 (1999): 162–80 for an example of where it has assisted the development of a significant piece of military (and surveillance) technology. Our point here is that this is not always the case. Indeed, as the following examples show, the success of IT is more the exception than the rule. The GOA regularly issues reports on the failure of US government agencies and departments to adhere to proper IT project management techniques. This failure costs billions of dollars, according to the GOA. See, for example, David A. Powner, Director, United States Government Accountability Office, Information Technology Management Issues, *Management and Oversight of Projects Totaling Billions of Dollars Need Attention*, Testimony before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, US Senate, April 28, 2009.

[115] In a recent simulation exercise, "Mr. Lynn, one of the Pentagon's top strategists for computer network operations, argues that the billions spent on defensive shields surrounding America's banks, businesses and military installations provide a similarly illusory sense of security." John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent", *The New York Times*, January 26, 2010.

[116] See John A. Gentry, "Doomed to Fail: America's Blind Faith in Military Technology", *Parameters* (2002–03): 88–103.

[117] For the origin of this phrase see the Free Online Dictionary of computing at http://foldoc.org/garbage+in, viewed January 30, 2010.

information quality. According to Barbara Klein: "Data stored in organizational databases have a significant number of errors. Between one and ten percent of data items in critical organizational databases are estimated to be inaccurate."[118]

Much of the work of terrorists is planned in third world countries. However, it is in just these places that the quality of data in information systems is most suspect.[119] This deficiency in data quality severely compromises efforts to monitor terrorist activities.

In a recent US government report "Cyberspace Policy Review" a review team of government cybersecurity experts concluded that "the architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations."[120]

An example of the weakness of various securitization technologies is biometric national identity systems.[121] These systems depend for their usefulness upon the quality of (low-security) documents such as drivers licenses, birth certificates and the like. Such documents are relatively easy to (falsely) obtain. Once this has been achieved, NIDs (falsely) authenticate individuals, thus generating false negatives.

An aspect of the quality of technology that is often overlooked is its own security – that is, how well does it prevent unauthorized users from getting access to its information and decision-making process? A military example of this is the recent newspaper article by Siobhan Gorman et al., which reported that $26 worth of commercial software is able to "intercept live video feeds from U.S. Predator drones."[122] In 2009 more than 285 million data records were compromised in the business field.[123] Although military and security agencies are secretive about the safety of their systems, there is little to make one confident that their systems comprise any better technology.[124]

[118] Barbara D. Klein, "Data Quality in the Practice of Consumer Product Management: Evidence from the Field", *Data Quality* 4, no. 1 (1998).

[119] David W. Chapman and Roger A. Boothroyd, "Threats to Data Quality in Developing Country Settings", *Comparative Education Review* 32, no. 4 (1988): 416–29. Although this report is dated, the situation in developing countries has not changed in twenty years.

[120] White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Structure* (May, 2009), available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[121] For a detailed examination of this phenomenon, see See Bijon Roy, "A Case against Biometric National Identification Systems (NIDS): 'Trading-off' Privacy Without Getting Security",*Windsor Review of Legal & Social Issues* 19 (March 2005): 45–84.

[122] Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones, $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected", *The Wall Street Journal*, December 17, 2009, A1.

[123] Wade H. Baker, Alex Hutton, C. David Hylender, Christopher Novak, Christopher Porter, Bryan Sartin, Peter Tippett, M.D., Ph.D. and J. Andrew Valentine, *2009 Data Breach Investigations Report*, Verizon Business, available at http://securityblog.verizonbusiness.com, viewed December 14, 2009.

[124] There are many examples of technology failures in the military and security fields. See, for example, the U.S. Navy's Smart Ship technology of the late 1990s that failed so spectacularly, Gregory Slabodkin, "Software Glitches Leave Navy Smart Ship Dead in the Water", *Government Computer News*, 13 July 1998.

In another example, Stephen Feinberg makes the point that data mining's success "depend[s] heavily on matching and record-linkage methods that are intrinsically statistical in nature and whose accuracy deteriorates rapidly in the presence of serious measurement error. Data mining tools cannot make up for bad data and poor matches."[125] It is absolutely essential that securitization technologies have quality data.

Another difficulty with measuring the quality of information comes through quantity: if the quantity is large enough then it is not possible to measure the quality of a given set of information. According to Minnesota Internet Traffic Studies (MINTS), the total known digital content is roughly 500 billion gigabytes, or 500 exabytes (with more than 60 exabytes produced every year).[126] With current technology it is not possible to process this much information.[127] As a result new theories for information processing (especially concerning money laundering and terrorist financing) are being developed, but researchers are not yet optimistic about the possibilities.[128] This is an especially acute problem for the military use of spy drones. In a recent article, Christopher Drew of the *New York Times* reported that the military was recording video data at a greater rate than can be analyzed.[129]

The quality of technology is underpinned by the quality of the assumptions made. In the section on surveillance we pointed out that much of the technology is not of sufficient quality to be useful. This can be seen in facial recognition software (an issue visited earlier in this discussion, reviewing James Meek's experiment) that depends upon the "idea that certain anatomical characteristics, facial configurations, gestural expressions and behaviors are universal, rather than specific or framed by the context in which they appear."[130] According to Andrew Speirs, this is a flawed notion that consistently fails to deliver suspects. Here it is the quality of the design (underlying assumptions) of the technology that fails to deliver. Also underpinning the quality of technology is the quality of the personnel employed by agencies to develop the technology. In a recent

[125] Stephen E. Feinberg, "Privacy and Confidentiality in an e-Commerce World: Data Mining, Data Warehousing, Matching and Disclosure Limitation", *Statistical Science* 21, no. 2 (2006): 143–54.

[126] An exabyte is 10246 or approximately one billion gigabytes. See Minnesota Internet Traffic Studies (MINTS), at http://www.dtc.umn.edu/mints/home.php, viewed February 1, 2010.

[127] David S. Alberts made just this point and called it information swamping. See David S. Alberts, *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative* (Diane Publishing Co. 1996), especially pp. 16, 31, 34, 38. The legal profession refers to the term "information inflation" to describe this phenomenon/problem: see George L. Paul and Jason R. Baron, "Information Inflation: Can the Legal System Adapt?", *Richmond Journal of Law & Technology* 13, no. 3 (2007), at http://law.richmond.edu/jolt/v13i3/article10.pdf, viewed January 25, 2010.

[128] Dionysios S. Demetis, "Data Growth, the New Order of Information Manipulation and Consequences for the AML/ATF Domains", J*ournal of Money Laundering Control* 12, no. 4 (2009): 353–70.

[129] Christopher Drew, "Military Is Awash in Data from Drones", *The New York Times*, January 11, 2010.

[130] Andrew Speirs, "The Individual and the Stereotype: From Lavater to the War on Terror", Australian Council of University Art and Design Schools (ACUADS) ACUADS 2003 Conference, Hobart 1–4 Oct 2003, http://www.acuads.com.au/conf2003/papers_refereed/speirs.pdf.

job advertisement for a business consultant, the National Security Agency (NSA) specified in the job requirements that the successful candidate would "perform various types of business analyses (e.g. Business Case, Cost/Benefit, Cost Effectiveness, etc.), as well as analysis of special topics that will be used by Senior Leadership to make better-informed decisions."[131] Yet the qualifications asked for stated: "The successful candidates should possess at least 2+ years of related experience and a Bachelor's degree in engineering, mathematics, operations research, business, or economics." There was not a word about information technology qualifications, especially analysis and design. How can such agencies be confident of their employees' ability successfully to complete complex information technology tasks without any professional qualifications? This is not a new problem. In 1996, Alberts noted the US government's inability to "maintain the expertise required to adapt" commercial software for military use.[132]

In another example of flawed assumptions, Geoff Dean found the idea of profiling terrorists as persons to be "neither simple nor necessarily helpful and could in fact be dangerously misleading. It is argued that it is more fruitful to shift the focus of the profiling paradigm by engaging in profiling the 'process' of terrorism rather than the 'person'."[133] This can be seen in the results of the NSA's domestic spying program. According to the Electronic Frontier Foundation (EFF) this program is next to useless: "Reports have shown that the data from this wholesale surveillance did little more than commit FBI resources to follow up leads, virtually all of [which], current and former officials say, led to dead ends or innocent Americans."[134]

More directly addressing the quality of technology itself is the doubt cast on the quality of many technologies. For example, in the geographic profiling software referred to earlier, Derek Paulson found that his "study casts doubt . . . on the overall accuracy of profiling strategies in predicting the likely home location of an offender."[135] A final example of the worry that technology is not up to the task is steganography. Kessler points out that "there are few hard statistics about the frequency with which steganography software or media are discovered by law enforcement officials in the course of computer forensics analysis. Anecdotal evidence suggests, however, that many computer forensics examiners do not

[131] This job was posted on CareerBuilder.com on January 6, 2010, viewed January 10, 2010.

[132] See Alberts, *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative*, 44.

[133] Geoff Dean, "Criminal Profiling in a Terrorism Context", in R. N. Kocsis (ed.), *Criminal Profiling – International Theory, Research and Practice* (Humana Press, 2007).

[134] Electronic Frontier Foundation FAQ, at http://www.eff.org/nsa/faq, viewed 2 January 2010.

[135] Derek J. Paulsen, "Connecting the Dots: Assessing the Accuracy of Geographic Profiling Software", *Policing: An International Journal of Police Strategies & Management* 29, no. 2 (2006): 306–34.

routinely search for steganography software, and many might not recognize such tools if they found them."[136] He further points out that "it is impossible to know how widespread the use of steganography is by criminals and terrorists".

The quality of technology can also be measured by the degree to which it meets its stakeholders' expectations. A recent Standish Report found that "in 1995, U.S. government and businesses spent approximately $81 billion on cancelled software projects."[137] Most of these projects were cancelled due to difficulties in specifying and meeting user requirements.

The use of information (and its) technology

Much of the technology described in this study creates an enormous amount of information that would be useful in the right hands. Indeed, the use of technology to gather and process information has led to significant improvements in many areas, including law enforcement. However, in some cases that information has gone not into the right hands but, indeed, into the wrong hands (as seen in the drone article above).

One of the criticisms of the various government agencies in the aftermath of 9/11 was the failure to share information.[138,139] This failure points to a general lack of protocols, procedures and governance defining the importance, scope and circumstances of information sharing. Stewart Baker, in his testimony before Congress, said that "the government's failure to find the hijackers was caused in the first instance by a lack of information technology tools."[140]

Of course, much of the foregoing discussion offers an implicit evaluation from a privacy perspective of existing information technology systems. Nevertheless, we should not forget those projects that did not get even as far as being implemented. The most outstanding example of this is the FBI's Trilogy Project

[136] See Gary C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner"(edited version), *Forensic Science Communications (Technical Report)* 6, no. 3 (July 2004), available at: http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm; http://www.garykessler.net/library/fsc_stego.html.

[137] The Standish Group, "Chaos", 1995, at http://www.standishgroup.com/chaos.html, viewed December 30, 2009. See also Lorin J. May, "Major Causes of Software Project Failures", at http://www.stsc.hill.af.mil/crosstalk/1998/07/causes.asp, viewed November 20, 2009.

[138] In the information field, information sharing is called information transparency. See Peter P. Swire, "Privacy and Information Sharing in the War on Terrorism", *Villanova Law Review* 51 (2006): 951–80; and Matteo Turilli and Luciano Floridi, "The Ethics of Information Transparency", *Ethics and Information Technology* 11 (2009): 105–12.

[139] The Christmas 2009 attempt to bomb a commercial airliner highlights the fact that information sharing has not improved. See Eric Lipton, Eric Schmitt and Mark Mazzetti, "Jet Bomb Plot Shows More Missed Clues", *The New York Times,* January 18, 2010.

[140] Testimony of Stewart Baker before the National Commission on Terrorist Attacks Upon the United States December 8, 2003.

(better known as the Virtual Case File Project).[141] It is estimated to have cost at least $100 million (cost estimates vary from $100 to $400 million) with no return for the investment. This system was intended to overcome the problem of sharing of information between those who *ought* to have had access to and those who *actually* had access to critical information. Fundamentally, it failed because of the FBI's reluctance to engage professional IT project managers, preferring to use its own (unqualified, in IT terms) agents. Although this example may seem to be an outlier, in fact it is consistent with normal commercial industry practice.[142]

[141] There is an enormous amount of literature examining this failed software project. See, for example, Harry Goldstein, "Who Killed the Virtual Case File?", *IEEE Spectrum*, at http://lrv.fri.uni-lj.si/~franc/COURSES/VP/FBI.pdf, viewed 5 July 2009, and T. Frieden, "Report: FBI Wasted Millions on 'Virtual Case File'", *CNN* (2005, February 3), at http://www.cnn.com, viewed September 7, 2009. See also,http://www.sdtimes.com/link/28788, viewed 16 November 2009.

[142] Robert N. Charette, "Why Software Fails", *IEEE Spectrum*, at: http://spectrum.ieee.org/computing/why-software-fails, viewed January 3, 2010.