



POLICY FORUM ON

Outsourcing of Systems for Detection, Identification, and Authentication

FOCUS GROUP COORDINATOR

International Biometric Group (IBG)

DATE

6 February 2009

LOCATION

London, UK

Regent's College Conference Centre

Tuke Hall

Tuke Common Room

PARTICIPANTS

**HIDE Partners, Bojana Bellamy, Kirsten Bock,
Antonio Caselli, John Leach, Lokke Moerel,
Ariane Mole, Chris Pounder, Max Snijder,
Roberto Tavano**

Programme: FP7 Capacities

Science in Society

Ethics and Security Research

Funding scheme: CSA (Coordinating)





This work was supported in part by the European Commission under contract FP7-217762 HIDE. HOMELAND SECURITY, BIOMETRIC IDENTIFICATION, & PERSONAL DETECTION ETHICS.

HIDE is a project promoted by the European Commission and coordinated by the Centre for Science, Society and Citizenship, an independent research centre based in Rome, Italy. Part of this project consists of a series of policy forums exploring prominent ethical issues pertaining to biometrics and personal detection technologies. These policy forums cover subjects ranging from Outsourcing to Body Issues to Contextual Integrity. The Outsourcing policy forum is organized by IBG. The mission of the HIDE Policy Forum on Outsourcing of Systems for Detection, Identification, and Authentication is to become the pre-eminent international forum for discussion, analysis, and debate on ethical issues associated with outsourcing of biometrics and personal detection systems.

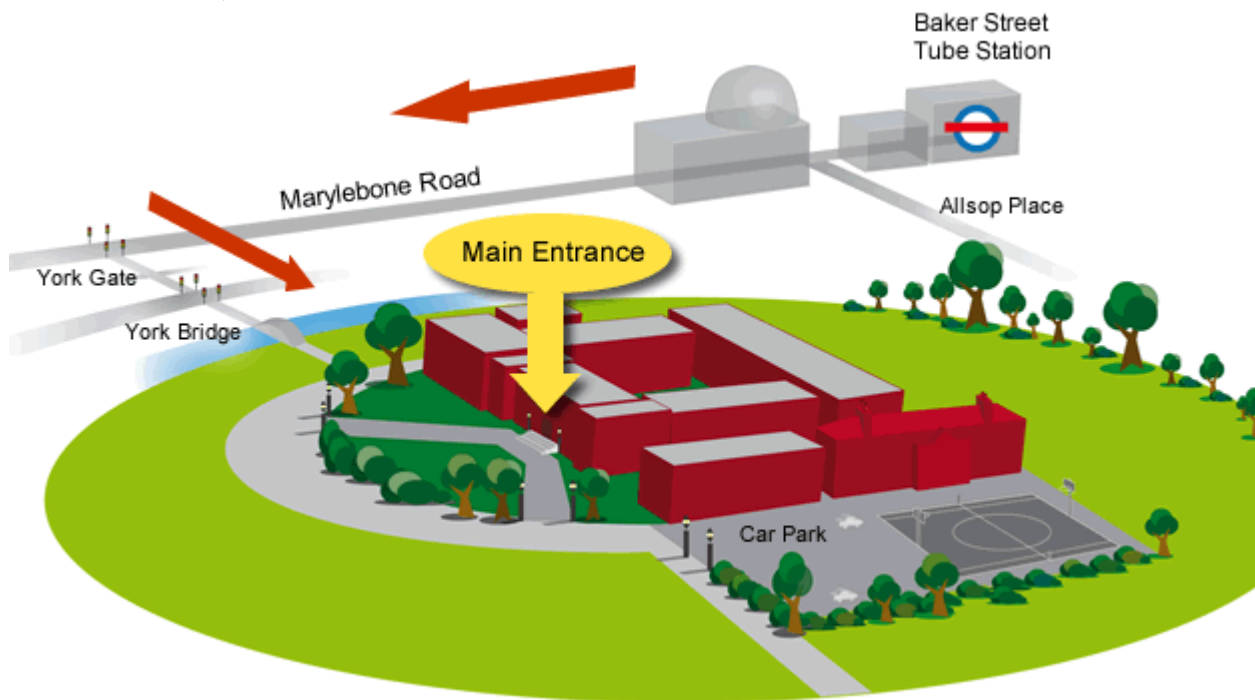
OUTSOURCING POLICY FORUM LOGISTICS

Contact: Victor Lee, IBG; vlee@biometricgroup.com; +1 212 809 9491

Date and Time: 6 February 2009; 9 AM – 5 PM

Venue: Tuke Common Room, Tuke Hall, Regent's College Conference Centre, London, UK

Nearby Tube Station: Baker Street (Circle Line; Hammersmith & City Line; Metropolitan Line; Bakerloo Line; Jubilee Line)



AGENDA

9:00 AM – 9:15 AM	Welcome and Refreshments
9:15 AM – 9:30 AM	Overview of Outsourcing and Ethics Concerns and Introduction to Background Document (Victor Lee)
9:30 AM – 10:00 AM	Presentation and Discussion: “Outsourcing and the EU Data Protection Directive” (Chris Pounder)
10:00 AM – 10:30 AM	Presentation and Discussion: “Outsourcing Protection Requirements” (Kirsten Bock)
10:30 AM – 10:45 AM	Break
10:45 AM – 11:15 AM	Presentation and Discussion: “Data Protection and Privacy: the Italian Government Perspective” (Antonio Caselli)
11:15 AM – 11:45 AM	Presentation and Discussion: “Identity Assurance Policy Frameworks and Safeguards” (John Leach)
11:45 AM – 12:30 PM	Open Discussion of Morning Session Issues
12:30 PM – 1:15 PM	Lunch (provided)
1:15 PM – 1:45 PM	Presentation and Discussion: “Outsourcing and the EU Biometrics Visa Lifecycle” (Roberto Tavano)
1:45 PM – 2:15 PM	Presentation and Discussion: “Biometrics and the Link to Identity” (Max Snijder)
2:15 PM – 2:45 PM	Presentation and Discussion: “Biometric Systems, Outsourcing, and Data Privacy: the French Perspective – Possible Evolutions at the European Level” (Ariane Mole)
2:45 PM – 3:00 PM	Break
3:00 PM – 3:30 PM	Presentation and Discussion: “Outsourcing and Data Privacy from the Service Provider Perspective” (Bojana Bellamy)
3:30 PM – 4:00 PM	Presentation and Discussion: “The Privacy Paradox: Rethinking Laws and Technologies” (Lokke Moerel)
4:00 PM – 4:45 PM	Open Discussion of Afternoon Session Issues
4:45 PM – 5 00 PM	Introduction to HIDE Wiki, Online Tools, and Other Resources; Report Composition Role Assignment

ETHICAL DIMENSIONS OF OUTSOURCING OF SYSTEMS FOR DETECTION, IDENTIFICATION, AND AUTHENTICATION

Introduction

This document introduces ethical issues associated with the outsourcing of biometrics and personal detection technologies for detection, identification, and authentication. Such ethical considerations arise out of tension between individual rights, data protection, and privacy, on the one hand, and economic needs, on the other. Generally, the former restrain and limit outsourcing, while the latter encourage outsourcing. Security and safety considerations are also important to the issue of outsourcing: sometimes outsourcing best supports security and safety; other times, outsourcing negatively impacts security and safety.

Key terms in this document are defined as follows:

- *Outsourcing* refers to the procurement of goods or services under contract with an outside supplier.ⁱ
- *Biometric systems* perform the automated measurement of physiological and/or behavioural characteristics to determine or verify the identity of an individual.ⁱⁱ Examples of biometric systems are fingerprint recognition systems, iris recognition systems, face recognition systems, and voice recognition systems.
- *Personal detection technologies* are technologies that focus specifically on individuals and are used to detect something or someone within a security or safety context. Personal detection technologies include closed-circuit television (CCTV), radio frequency identification (RFID), infrared detectors, thermal imaging, smart cards, global positioning systems (GPS), geographical information systems (GIS), micro electrical mechanical systems (MEMS), transponders, and body scanners.ⁱⁱⁱ
- *Detection* entails discovering the existence, presence, and/or state of something or someone.
- *Identification* means determining the identity of an individual. In the context of biometrics and personal detection systems, identification is often performed through a one-to-many comparison of a subject against databases of existing profiles.
- *Authentication* is verification of a claimed identity. In the context of biometrics and personal detection systems, authentication is often performed through a one-to-one comparison of a subject, credential, or characteristic against the relevant profile associated with the claimed identity.

Context

Thanks to technological advancements in communications and transportation, the world has become more interconnected. This phenomenon has prompted increased regional and international interaction. Superstate structures, such as the European Union (EU) and European Economic Area (EEA), have arisen, facilitating the flow of information across national boundaries and supporting the establishment of transnational economic relationships. Governments and corporations, today, are more willing to outsource their functions, processes, and procurement to parties in other countries.

Additionally, the growing proliferation and rapid development of biometrics, personal detection systems, and related technologies in the private sphere have provoked a paradigm shift in which public sector entities increasingly rely on the often faster-moving and more cost-efficient private sector for once-core government responsibilities, such as security operations and identity management. This growing global trend is driving “extensive outsourcing of personal information processing and storage.”^{iv} This document begins to weigh the benefits and costs of such a trend towards outsourcing.

Background and Discussion

In order to understand the trend towards outsourcing, it is important first to understand the different forms outsourcing can take. Outsourcing may be divided geographically into onshore and offshore outsourcing. Onshore outsourcing, also called “domestic outsourcing,” refers to outsourcing conducted entirely within a single country.^v Offshore outsourcing refers to outsourcing that transcends national borders or jurisdictions.

Outsourcing may also be categorically divided into business process outsourcing and technology services outsourcing. Business process outsourcing is the outsourcing of operational functions and responsibilities to third-party providers. Technology services outsourcing refers to the research, development, manufacture, production, provisioning, and/or support of hardware and software systems by a third-party provider.

While all of these forms of outsourcing give rise to ethical challenges and dilemmas, it is the newer trends of offshore outsourcing and business process outsourcing that are perhaps most critical.

The drive towards outsourcing stems mainly from economic motivations. These include:

- (1) lower labor costs;
- (2) lower supply costs;
- (3) superior tax/regulation policies;
- (4) greater political/economic stability;
- (5) greater efficiency; and
- (6) superior competency/quality.

Most of these motivations surface in both private and public sector entities. Both the private and the public sector are generally eager to minimize impacts on their budgets, and the savings can be significant.

According to a May 2008 Identity Cards Scheme report released in the United Kingdom, outsourcing the collection of biometric data for UK identity cards could save the UK £860 million.^{vi}

The private and public sectors also want to ensure that those who are most qualified, reliable, and efficient are offering or creating the highest quality service or product. By outsourcing certain functions or supplies, private and public sector entities can allocate more of their time, money, and energy to matters where their personal attention is required or where they have expertise and unique qualifications.

The most significant ethical questions arise, however, when the public sector outsources its functions or procurement activities to the private sector, especially when the private outsourcer lies without the traditional national boundaries and jurisdiction of the public sector contractor. This is largely because of the special responsibilities and authorities held by public sector entities who wield legal, not consumer-driven, mandates. Governments, for example, have the authority to collect, process, maintain, and store sensitive, personal data from their citizenry. They also have the responsibility for ensuring national security and

defending their citizens' individual rights. Reliance on the private sector and its free-market principles and economic incentives for these activities could result in dangerous degrees of risk-taking or compromise as to the "acceptable" costs of data loss or theft; this is especially problematic when the private sector may be less open than the public sector about how it handles and deals with personal data.

And yet, such public-to-private outsourcing not only occurs, it is becoming increasingly common. For example, 43 of the countries who have adopted e-passport systems, including the United States, Italy, Germany, Austria, and France, use smart chip technology produced by Netherlands-based NXP Semiconductors.^{vii} These are chips that are embedded in e-passports; the chips contain important personal data and, in some cases, hold biometric information.

The United States goes a step further. Not only does the US government send blank passports to NXP for smart chip implantation, it sends those same passports to a Smartrac Technology factory in Thailand where RFID antennas are inlaid in the passports.^{viii} This offshore outsourcing has netted the US Government Printing Office tens of millions of dollars in profit, but it has also introduced reason for concern, as Smartrac Technology admitted in 2007 that China had stolen its e-passport chip technology.^{ix}

In the United Kingdom, the UK Border Agency has outsourced its visa application process, which involves the collection of fingerprint and face biometrics,^x to VFS Global and WorldBridge.^{xi} On 19 May 2007, however, The Tribune of India reported that the UK had (temporarily) suspended visa applications in India, Russia, and Nigeria, after learning that up to 50,000 Indians' personal data may have been stolen.^{xii}

In France, the National Secure Credentials Agency outsourced its biometric passport implementation and deployment to Atos Origin and Sagem Sécurité, two international, non-governmental technology services firms headquartered in France. Though the two headquarters fall within French jurisdiction, this is a notable example of what was once a core government function migrating to the private sector, resulting in the acquisition of sensitive data by the private sector.

Indeed, the outsourcing of once-core government functions has expanded to the point where privately-run registered or trusted traveller programs leveraging biometrics and personal detection technologies have arisen, allowing sophisticated systems to take the place of government border control officers. In Amsterdam Airport Schiphol, for example, Privium program members use iris recognition to allow them to cross the border into Amsterdam without having to pass through passport control. A similar program, called IRIS, exists in the United Kingdom at Heathrow, Manchester, Birmingham, and Gatwick airports. Though overseen by the UK Border Agency, IRIS' core iris recognition system was outsourced to systems integrator Sagem SA by the UK Home Office.^{xiii}

Public-to-private outsourcing is also prevalent in airport passenger screening across Europe. Belgium, Denmark, France, Greece, Ireland, the Netherlands, and the United Kingdom have adopted decentralised aviation security models in which private airport authorities have assumed responsibility for passenger screening, often under government supervision.^{xiv} In some cases, such as at Athens International Airport, the airport authorities themselves outsource these tasks to private security companies like 3D, ICTS, and Wackenhut.^{xv} This differs from the centralised practice in Austria, Finland, Germany, Iceland, Italy, Luxembourg, Norway, Portugal, Spain, Sweden, and Switzerland, where the appropriate government authority takes direct, operational control of security.^{xvi}

All of the aforementioned examples of outsourcing raise legitimate national security concerns and data protection concerns. Consider the e-passport chip outsourcing example. The Netherlands is arguably one of

the more neutral countries in Western Europe and is in good standing with most of the Western Hemisphere nations. NXP Semiconductors, a spin-off from Philips, holds a strong reputation. It is unlikely that either country or company would, in the foreseeable future, enter into an antagonistic relationship with any of the 43 states using the NXP chips for their e-passports. Still, these 43 nations are placing great faith in the stability of their relationship with the Netherlands, which holds jurisdiction over NXP's headquarters. These nations are indirectly putting the security of their citizens' data in the hands of a foreign government and a foreign-based company with whom they merely have a contractual, transactional relationship and no superseding government authority. Were NXP to compromise (intentionally or unintentionally) the security of their chips and thus risk the security of their clients' e-passport data, their client nations would only be entitled to compensation dictated by the terms of their contract and would possibly be dependent on the Netherlands to support their legal claims against NXP. They would not be able to exercise the full force of governmental authority, but would rather depend dominantly on the weight of their governmental purchasing power and desirability as a future client. And even if monetary or nominal compensation were available, such compensation could be moot in light of the potentially far greater costs and security threats of compromised e-passport documents and data.

The Smartrac example already shows that the existence of diplomatic and trade relations amongst nations (China and the Netherlands, as well as China and Thailand) may not be sufficient to deter some countries from stealing important, sensitive technology from companies based in another country. Indeed, it may have been Smartrac's very lack of diplomatic protection as an outsourced outfit and the arguably looser controls and protections in Thailand that allowed Smartrac's e-chip technology to be stolen. Such theft could have enabled China to discover vulnerabilities in e-passports issued by a foreign country, something that should gravely concern nations, given their inherent responsibility to protect their citizens. After all, it would only take one fake or compromised passport to slip an individual who is a security threat into a target nation. Also, knowledge of e-passport weaknesses could enable covert, illegal data mining and identity theft.

As for registered or trusted traveller programs, outsourcing to private sector companies can lead to threats to airport security or border control when corners are cut for economic expediency. In 2008, Verified Identity Pass, operators of the Clear registered traveller program in the United States, announced that they had lost a laptop containing name, birth date, address, and identity documentation (drivers licenses, passports, etc.) for 33,000 Clear members.^{xvii} Though the laptop had been password-protected, Verified Identity Pass had chosen not to encrypt the data, as would have been required of most of their government counterparts. Subsequent to this fiasco, with new financial incentive, Verified Identity Pass proceeded to encrypt all of the sensitive personal data it possessed.

In deployments such as the Privium project, reliance on outsourcing for key technology that will make a critical security decision (whether or not to admit an individual at a border checkpoint) places a heavy reliance on the infallibility and purity of the technology. Companies like LG, the South Korea-based manufacturer of Privium's iris recognition systems, have strong reputations built partly on successes in independent technology tests and evaluations. But even when such companies mean well and have no secret objectives or motivations to place Trojan horses in their technologies, outsourcing can invite trouble. On 11 January 2008, the US Federal Bureau of Investigation reported that, through subcontractors and outsourcing, some US military agencies had received and installed compromised, counterfeit Cisco routers.^{xviii} It could be only a matter of time before outsourced biometric devices are compromised and counterfeited, too. And, unlike with routers and other commonplace IT equipment, many countries still lack the familiarity and expertise with biometric technologies even to have a chance at detecting such security threats. Ironically, the increasing ease, prevalence, and cheapness (at least, up front) of outsourcing may actually deter the development of such capabilities in-house.

For established personal detection technologies and their operators, the outsourcing issue is no more easily resolved. While several countries have employed a decentralised airport screening model without major event, 11 September 2001 revealed the risks with privatization and outsourcing of passenger and baggage screening. Prior to 9/11, airport screening in the United States varied by the quality of the screening service used, including level of personnel training, and the technologies employed. Some surmise, for example, that some of the 9/11 hijackers started their journey via Portland Airport in Maine in part to avoid presumably more stringent security checks at the busier Logan International Airport in Massachusetts. After 9/11, the Aviation and Transportation Security Act authorized the US Transportation Security Agency to take over airport screening duties with federal employees trained to the same, rigorously enforced standard across the nation.^{xix}

One could argue, however, that insourcing is not necessarily any better than outsourcing and that there are security advantages to be gained from outsourcing – not just monetary benefits. Some, for example, have worried that several US federal airport screeners may simply be the same incompetent screeners who once worked for private, outsourced contractors. Others are concerned that, if airlines add on new flight schedules, the slower (relative to the private sector) pace at which the public sector often works could delay the addition of new airport screeners and screening technologies. This could, in turn, lead to more hasty or sloppy screening in order to maintain throughput levels. And when it comes to data protection, governments are not always more careful in practice. Just consider the high profile loss by Her Majesty's Revenue & Customs (UK) of two compact discs containing over 15,000 people's names, dates of birth, national insurance numbers, and pension data.^{xx}

With outsourcing, governments have the option of leveraging private sector competition to ensure only the most efficient and highest quality providers win contracts. The time and money that is saved could then be reallocated to other purposes also oriented towards security, such as more in-depth interviews of suspicious individuals and investment in superior technology for secondary checks.

Furthermore, several countries lack the internal resources and expertise to develop in-house systems and mastery of sophisticated biometrics, personal detection, and e-identification technologies. These countries may believe that it would be safer for them not to reinvent the wheel or to rely on their inferior technology, but to take advantage of the higher quality, more secure systems and services offered by their allies (or companies under the jurisdiction of their allies). Although this creates a potentially dangerous dependency on others, these countries may find this risk and cost offset by other in-house security methods and options they choose to employ.

The ideal model for many European nations is reserving each government's right for standards setting, evaluation, and enforcement, but letting outsourcers work out most implementation details and procurement challenges. While what such standards should be is subject to debate, with several differences in European practice still remaining to be resolved, there are some basic data protection obligations and individual rights that all European nations agree must be met, especially when sensitive biometric and personal data is involved.

The Charter of Fundamental Rights of the European Union ("Charter"), for example, explicitly recognizes several individual rights including, but not limited to:

- right of human dignity (Article 1);
- right to life (Article 2);
- right to liberty and security of person (Article 6);

- right to the protection of personal data, which data “must be processed fairly for specified purposes and on the basis of the person concerned or some other legitimate basis laid down by law;” (Article 8);
- right to access data which has been collected concerning oneself and to have such data rectified (Article 8);
- right to freedom of peaceful assembly and to freedom of association (Article 12); and
- right for EU citizens to move and reside freely within EU Member States (Article 45).

The Charter also recognizes the right to respect for private and family life, home and communications (Article 7).

In addition, the European Parliament issued Directive 95/46/EC on 24 October 1995. This Directive addresses “the protection of individuals with regard to the processing of personal data and on the free movement of such data.”^{xxi} It provides for EU Member States:

- collecting personal data for “specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes” (Article 6);
- keeping personal data “in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed” (Article 6); and
- processing personal data only if the data subject has unambiguously provided consent (Article 7).

However, Directive 95/46/EC also notes that personal data may be processed:

- if necessary “for compliance with a legal obligation to which the data controller is subject” (Article 7);
- if necessary in order “to protect the vital interests of the data subject” (Article 7); and
- if necessary “for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed” (Article 7).

Competing interests (e.g. – those favouring cost-efficient performance of state functions versus those prioritizing individual liberties) may differ on the boundaries of the Directive’s provisions. This gives rise to ethical dilemmas and issues that revolve around the extent to which outsourcing (and, by extension, data movement and processing) can and should be undertaken without compromising individual rights and privacy concerns.

Presently, it is the opinion of the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs that outsourcing of biometric data collection may be ethical and feasible in certain deployments, such as visa applications, but that decisions as to which biometrics to collect and accept, as well as how such gathered personal data should be utilized, should remain a purely public sector function.^{xxii} European Parliament members, such as Baroness Sarah Ludford, have also pressed for diplomatic protection to be extended to outsourcers handling sensitive personal data such that those outsourcers cannot be pressed or compelled by their host countries to yield up such important data.^{xxiii} These proposals and perspectives, along with many others, will be addressed at the HIDE Policy Forum on Outsourcing of Systems for Detection, Identification, and Authentication.

RELEVANT RESOURCES / RELATED ARTICLES

- ⁱ Modified from: "outsource." Merriam-Webster Online Dictionary. 2009. Merriam-Webster Online, <http://www.merriam-webster.com/dictionary/outsource> (21 January 2009)
- ⁱⁱ www.biometricgroup.com
- ⁱⁱⁱ www.hideproject.org/about/project.html (8 July 2008)
- ^{iv} HIDE "Description of Work," Annex 1, part-B, version 1, Section T4.3 (6 November 2007)
- ^v Modified from: "onshore outsourcing." SearchCIO.com, http://searchcio.techtarget.com/sDefinition/0,,sid182_gci927957,00.html (22 January 2009)
- ^{vi} Iain Thomson, "UK ID card costs rise 37 per cent," vnunet.com, <http://www.vnunet.com/vnunet/news/2216212/id-card-costs-set-soar> (26 January 2009)
- ^{vii} "Germany Adopts Next-Gen NXP E-Passport Chip," <http://www.rfid-world.com/news/202801967> (22 January 2009)
- ^{viii} Bill Gertz, "Outsourced passports netting govt. profits, risking national security," Washington Times, <http://www.washingtontimes.com/news/2008/mar/26/outsourced-passports-netting-govt-profit-56284974> (22 January 2009)
- ^{ix} "Myrick Incensed at US Government's Outsourcing Passport Security Technology," http://www.house.gov/list/press/nc09_myrick/4208epassport.html (22 January 2009)
- ^x "VFS' visa application outsourcing service is going global," http://www.vfsglobal.com/images/Business%20India_Nov08.pdf (23 January 2009)
- ^{xi} <http://www.ukvisas.gov.uk/en/> (22 January 2009)
- ^{xii} "Online visa applications to UK suspended," <http://www.tribuneindia.com/2007/20070520/world.htm#1> (23 January 2009)
- ^{xiii} "Iris recognition to be installed across UK airports," <http://software.silicon.com/security/0,39024655,39121368,00.htm> (23 January 2009)
- ^{xiv} "Aviation Security Comparison of Europe and the United States," http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_8.pdf (23 January 2009)
- ^{xv} "Rebuilding Athens: from security pariah to security torch," Airport Security International. June 2002. http://www.aia.gr/UserFiles/File/Press/ClippingsEn/AviationSI2002_full.pdf (23 January 2009)
- ^{xvi} "Aviation Security Comparison of Europe and the United States," http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_8.pdf (23 January 2009)
- ^{xvii} "Missing SFO Laptop with Sensitive Data Found," <http://cbs5.com/local/tsa.security.clear.2.788083.html> (24 January 2009)
- ^{xviii} "US Military had counterfeit computer gear, FBI says," <http://www.iht.com/articles/2008/05/09/technology/cisco.php> (24 January 2009)
- ^{xix} "Gov't. Takes Over Airport Screening This Weekend," <http://www.allbusiness.com/transportation-communications/transportation-services/4133924-1.html> (25 January 2009)
- ^{xx} Paul Lewis, "Thousands at risk after data loss," <http://news.bbc.co.uk/2/hi/programmes/moneybox/7076106.stm> (26 January 2009)
- ^{xxi} European Parliament, "Directive 95/46/EC," http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_1 (11 July 2008)
- ^{xxii} European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Working Document, Part II, DT\661526EN.doc," http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/661/661526/661526en.pdf (26 January 2009)
- ^{xxiii} Baroness Sarah Ludford, "The implications of using biometrics in the VIS," <http://www.eubiometricsforum.com/dmdocuments2/3rdEBFRSSarahLudfordSpeech.doc> (26 January 2009)