

# HIDE



## **FOCUS GROUP MEETING #3**

### **SYSTEM INTEROPERABILITY**

#### **FOCUS GROUP COORDINATOR**

**International Biometric Group (IBG)**

#### **DATE**

**21<sup>st</sup> June 2010**

#### **LOCATION**

**London, UK**

**Regent's College Conference Centre**

**Meeting Room F**

#### **ORGANIZATIONAL PARTICIPANTS**

**IBG, CSSC, CESAGen, UNI-LJ**

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 focus groups exploring prominent ethical issues pertaining to biometrics and personal detection technologies. These focus groups cover subjects ranging from System Interoperability to Technology Convergence to Embedded Technology to Privacy Enhancing Technology. The System Interoperability focus group is organized by IBG. The mission of the HIDE Focus Group on System Interoperability is to become the pre-eminent international forum for discussion, analysis, and debate on ethical issues associated with interoperability in biometrics and personal detection systems.

## **SYSTEM INTEROPERABILITY FOCUS GROUP LOGISTICS**

**Contact:** Mary Collins, IBG; mcollins@biometricgroup.com; +1 212 809 9491

**Date and Time:** 21 June 2010; 11:00am-3:30pm

**Venue:** Regent's College Conference Center, Meeting Room F  
Regent's Park, London NW1 4NS

**Nearby Tube Station:** Baker Street or Regent's Park

## **SYSTEM INTEROPERABILITY FOCUS GROUP AGENDA**

11:00 AM – 11:15 AM	Welcome and Opening Remarks by IBG
11:15 AM – 11:45 AM	<b>Presentation by Alasdair Darroch, Biostore</b>
11:45 AM – 12:00 PM	Q&A and Brief Discussion
12:00 PM – 12:30 PM	<b>Presentation by Bob Carter, Identity and Passport Service</b>
12:30 PM – 12:45 PM	Q&A and Brief Discussion
12:45 PM – 1:30 PM	Lunch
1:30 PM – 2:45 PM	Open Discussion: System Interoperability
2:45 PM – 3:00 PM	Afternoon Coffee
3:00 PM – 3:15 PM	Future Work Plan chaired by IBG
3:15 PM – 3:30 PM	Conclusions and Wrap Up

# ETHICAL DIMENSIONS OF SYSTEM INTEROPERABILITY

## Introduction

This document highlights and discusses select ethical issues associated with system interoperability of biometrics and personal detection technologies. Such ethical considerations arise out of tension between individual rights, data protection, and privacy, on the one hand, and security/safety and economic needs, on the other. Generally, the former restrain and limit system interoperability, while the latter encourage system interoperability.

Key terms employed in this document are defined as follows:

- *System interoperability* is the ability of two or more systems to exchange information and to use the information that has been exchanged. This can take place within multiple contexts, including, but not limited to, technical, semantic, and legal.<sup>i</sup>
- *Biometric systems* perform the automated measurement of physiological and/or behavioural characteristics to determine or verify the identity of an individual.<sup>ii</sup> Examples of biometric systems are fingerprint recognition systems, iris recognition systems, voice recognition systems, and face 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.<sup>iii</sup>

## Context

Thanks to technological advancements in communications and transportation, the world has become increasingly interconnected. This phenomenon has prompted increased regional and international cooperation. Superstate structures, such as the European Union (EU), have arisen, facilitating the flow of information across national boundaries. The efficiency, success, and resulting value of such information exchange depend on system interoperability. Consequently, there is a critical technology trend towards system interoperability.

## Background and Discussion

The drive towards system interoperability stems mainly from two motivations:

- (1) security/safety needs; and
- (2) economic needs.

Security/safety needs generally fall within two categories:

- (1) border security; and
- (2) identification and surveillance of those within one's country or region.

The increased facility of travel from nation to nation, combined with modern terrorism concerns, has made border security a priority for many governments. Border security seeks to inhibit the entrance of unwanted individuals, such as terrorists, criminals, previously rejected asylum seekers, and those who are contagiously and seriously ill.

Identification and surveillance of those within one's country or region enables the detection, tracking, and identification of persons whom the country or region may perceive as a threat to security and safety. In addition to security/safety needs, economic considerations can encourage system interoperability. These needs include:

- (1) the desire for economies of scale;
- (2) freedom from dependency on specific proprietary solutions; and
- (3) pursuit of standardisation efficiencies.

System interoperability is typically achieved via:

- (1) standardisation;
- (2) establishment of central databases; and/or
- (3) reciprocity of system/database access.

Nations may attempt to realize economies of scale by, for example, partnering with allies to create a central repository of information composed from multiple individual national submissions. For the cost of configuring its systems to accommodate this central database, a nation can thus gain access to both the data it collects, as well as that collected by its allies. One example is EURODAC, a European fingerprint database under European Commission management that facilitates the identification of asylum seekers and deters "visa shopping"<sup>iv</sup> within Norway, Iceland, and all EU member states, except Denmark.<sup>v</sup>

The drive towards system interoperability, however, is not absolute. Respect for individuals and their rights can serve as a restraining force and may manifest in data protection legislation and privacy policies, such as the Charter of Fundamental Rights of the European Union.

Competing interests (e.g. – those favouring state security 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 balancing the drive and need for system interoperability with sensitivity towards individual rights and privacy concerns.

## **Ethical Problems and Challenges**

### *Consent*

One of the greatest challenges concerning the collection, movement, exchange, and use of personal data is the issue of consent. System interoperability amplifies the impact of consent-related ethical dilemmas by facilitating and extending the reach of such data collection, movement, exchange, and use.

Consent issues can be broken down into four general problem categories:

- Responsibility for Ensuring Consent
- Degree of Consent;
- Definition of Consent; and
- Challenge of Obtaining Consent.

Because of the sensitive and personal nature of the data being collected by biometric and personal detection systems, collectors of such data – especially governments – should generally have the responsibility and burden of ensuring prior consent from their data subjects. Whenever and wherever possible, data subjects should retain control over the collection, movement, exchange, and use of their personal data.

Consent, however, can come in several forms: informed and uninformed; explicit and implicit. Data collectors and users should strive to obtain explicit and informed consent for each category of data collection and use anticipated. Biometric and personal detection technologies should, by default, be limited to just uses

authorized under explicit and informed consent. Particular care should be taken with technologies that are interoperable with systems across multiple applications.

Determining if a subject is properly “informed,” however, can pose a challenge, due to the existing “public knowledge deficit.” Data collectors – and particularly governments – thus have an obligation to educate their data subjects. Data subjects have a right to a robust understanding of how their data can be collected, moved, exchanged and used. Such understanding should carry over to each potential use of their data, and each distinct use case should be specifically and explicitly approved by the data subject, whenever possible. This is particularly important as system interoperability improves, increasing the potential for rapid – and sometimes uncontrolled – expansion of data use.

Obtaining explicit, informed consent, however, is often impractical. Additionally, some applications may discourage the obtaining of explicit, informed consent. For example, law enforcement authorities may count on covert surveillance programs and technologies remaining relatively unknown; they may desire the quiet exchange of collected data with other criminal justice community members. In such cases, the covert capture of personal data and leveraging of intra-nation interoperable network might be acceptable, if necessitated by pressing public security and safety interests, and alternatives are not available.

One way of increasing voluntary participation is to adopt a “user convenience” model. Data collectors should attempt whenever possible to add an element of convenience (not just enhanced security) for data subjects to provide an incentive for them voluntarily to participate. User convenience, in turn, is tied to:

- establishment of the perceivable usefulness and necessity of a biometric or personal detection technology;
- confidence in the technology’s ease of use;
- ease of comprehension of the technology’s capabilities and limitations (both in standalone applications and in networked and/or interoperable environments); and
- trust in the data collector, including the perception that the collector has the ability to keep appropriate control over the data collected.

In some scenarios where data collectors themselves may not be trustworthy – or perceived to be trustworthy – due to poor track records or a lack of direct contact and familiarity with their data subjects, third party “trust agents” maintaining existing trust relationships with both sides could potentially be used to bridge the two.

### *Scope Creep and Expansion*

Biometric and personal detection technologies should, by default, be limited to just uses authorized under explicit and informed consent. However, even in cases where consent is properly and ideally obtainable, the default position should be to restrain the expansion of collection or use of biometric and other personal data. With the benefits of increased system interoperability, including the facilitated exchange of information and the increasing reliance and drive towards centralized databases, it is easy for scope creep to occur.

Scope creep refers to the gradual, uncontrolled expansion of personal data collection and/or use. Scope creep, for example, could turn the simple collection and limited processing of fingerprints for a security guard candidate’s background check into the first step of an immigration check against several interoperable, international databases. The reverse is also possible. Consider the European Visa Information System (VIS), a central database containing fingerprint and face images. Though a key purpose of this database is to help determine whether or not a visa should be issued to an applicant, scope creep could result in an expansion of database usage to support regular criminal background checks by law enforcement. Such usage, in turn, could encourage more liberal use of the database, such as tracking applicants’ movements or performing data mining to determine geographical criminal tendencies.

Scope creep is especially problematic in situations where law may provide for the collection of personal data without consent. The United Kingdom’s Criminal Justice Act 2003, for instance, allows “the taking of

fingerprints without consent upon arrest for a recordable offense.”<sup>vi</sup> Lack of consent demands a particularly strict and narrow interpretation of scope for the use and dissemination of the collected personal data. One might argue that uncooperative subjects may be more likely to have something to hide (and, by extension, should have their biometric data searched against a more expansive set of interoperable databases). Per Directive 95/46/EC, this should only be done if truly “necessary” and for purposes directly related to the original reason justifying collection of personal data *sans* consent. Lax adherence to such principles invites loopholes and abuse.

Scope creep is a function of three components:

- the capacity of technology;
- the presence or absence of legislation and legal frameworks; and
- the social need or desire for additional functionality.

As time passes, technology capacity will continue to grow and to expand. Many technological capabilities will be exploited for purposes beyond those which they were originally intended to serve, with or without consent. This can contribute to a parallel increase in scope creep. Though technologies can be – and, in some cases, should be – developed to hinder and deter scope creep, this can result in a dangerous, rapidly escalating arms race and an overreliance on technology.

Even if legal and technology issues are carefully controlled, social forces and desires for additional functionality can still exert notable influence on scope creep. Gradually, the acceptability of the use of biometrics and personal detection technologies, which target particularly sensitive data, becomes less and less of concern. Through steady acculturation, individuals become desensitized and scope creep can proceed undetected. Yet, such efforts, often driven by market forces and creative interpretations of social needs can set the groundwork for the establishment of a surveillance state in which the deployments’ breadth and interoperability support the extensive tracking of individuals’ travel habits and histories – with biometric certainty.

Each system interoperability-enabled expansion of scope results in a new situation that is often harder to reverse – a particular problem in cases of abuse or improper action. For example, as interoperable data sharing networks expand, it can become more challenging to cut off all points of access to data once that data should no longer be accessed or if it were incorrectly acquired in the first place.

### *Data Centralisation*

As nations worldwide increasingly collaborate in supranational institutions like the European Union, North Atlantic Treaty Organization (NATO), the African Union, and the Association of Southeast Asian Nations (ASEAN), combining national informational resources with respect to biometrics and other personal data seems like a natural extension of this trend. Indeed, the European community has already established central databases such as VIS and European Dactyloscopie (EURODAC), which stores biometric data from asylum seekers. These databases are populated by submissions from multiple countries, giving access to a collective dataset that is greater than that held by any one country, alone.

Central databases can serve an important function in facilitating the smooth, cost-effective exchange of information. They can also be privacy-conducive. When a data record is no longer valid or necessary (and thus should be deleted), central databases allow for a single point of elimination of that data, reducing the chance that the information is inappropriately passed on or overlooked in a local database. Central databases also provide a central point for protection, allowing data to be protected with, in theory, the combined resources of all participating nations.

On the other hand, the single focus of central databases presents a single point of attack. If central databases are compromised, the effect can be severe and can corrupt all interoperable systems drawing data from those databases. More significantly, central databases pose a greater danger insofar as they enable the discovery of broader trends or profiles and the drawing of powerful conclusions that can easily support a Big Brother

state. The same technology that can help identify visa shoppers could easily be adapted to track the movement and activity habits of an innocent citizen entitled to his or her privacy. To help enforce a proper limit of scope, no single database should support two or more functions that are discrete and not directly related, even if both are for important security purposes. Similar, but separate, databases should be established, instead.

Thus, the use of VIS (and not a parallel, comparable database) to support prevention of terrorist activities should be discouraged, if not outright prohibited. Granted, while access to VIS data in such scenarios would be via indirect, central access points with data protection checks,<sup>vii</sup> such protections should instead be built into a separate database with different stringency levels for accessibility, given the different application for which the data is collected. By leveraging one database for multiple applications, one is likely to violate principles of obtaining informed consent.

One of the challenges with central databases fed by data from various nations is how to deal with countries' varying degrees of institutionalized data protection. France's National Commission for Data Protection and the Liberties (CNIL), for example, views the French VISABIO database of foreign visa-applicants' biometrics with concern and scepticism,<sup>viii</sup> while, for the United States, data protection has often been an afterthought to security concerns, particularly when foreign nationals are involved. Access to central databases should be restricted only to those who meet the standards of the most stringent contributing nation, unless a common standard has been developed.

Even better than reliance on central databases, however, would be the realisation of interoperability through central systems supporting the exchange of limited data from databases wholly controlled by individual countries. Under the Treaty of Prüm,<sup>ix</sup> for example, treaty ratifiers' police forces do not have unfettered, automatic access to each others' fingerprint, DNA, and vehicle registration databases; rather, they only have the ability automatically to determine if the data they seek is in the possession of one of their partner members. Access to that specific data should then be provided on a direct member-to-member basis using existing data exchange channels. This compromise provides the scalability benefits of a central database without the loss of direct control over data collected and the possible infringement of citizens' rights that could arise as a consequence.

#### *Standardisation, Harmonisation, and Openness*

Standardisation has been actively pursued to achieve system interoperability, whether facilitating the sharing of personal data or enabling personal data to be processed by a range of vendor technologies. The contactless payment industry, for example, has enabled the development of point-of-sale terminals that are interoperable with contactless cards from multiple vendors. Standardisation also facilitates the interchange of fingerprint data amongst European criminal justice authorities for border applications.

Many of these standards are public to encourage widespread adoption and conformity. They are open and exposed to critical analysis and commentary. This, in turn, can help improve the standards and make them more robust. Additionally, open standards can reveal anomalous behaviours or setups, deterring abuse of biometrics and personal detection technologies. They can reveal when applicable laws or practices are not being followed. Indeed, the use of open standards has been recommended by the European Commission in the European Interoperability Framework for Pan-European eGovernment Services.<sup>x</sup>

However, the openness of these standards can provide dangerous insight for those with malevolent intent. In the case of RFID-based technologies, open standards could facilitate skimming or jamming contactless payment transactions; a discovered vulnerability in one system could lead to broad exploitation of a range of systems. Similarly, open standards – or open standardised processes – may facilitate the development of biometric spoofs, such as fake fingerprints or artificial data. In some situations, therefore, standards (such as the specific frequency at which EZ-PASS<sup>xi</sup> transponders operate) may exist but be difficult to uncover.

Keeping technical standards and standard practices “closed” and/or limited to those with a defensible “need to know”<sup>xii</sup> may be tempting – especially in cases where public safety or security is at stake. However, this

makes it challenging for individuals to take precautions to ensure the safety of their personal data and to exercise their implicit right to know how their data is being used (Article 8 of the Charter). Open standards and transparent processes are thus generally encouraged.

Indeed, a similar approach – the open source Linux model – has demonstrated that openness can be a positive element. Several countries, many of whom are already cooperating in other areas, can offer their collective expertise through public standards bodies to resolve problems, challenges, or discrepancies for the betterment of all. Vulnerabilities and exploits can be more rapidly detected and addressed worldwide through a single, cohesive effort, rather than by nation-by-nation patches.

Standardisation, however, can also contribute to the danger of system scope creep. Standardisation increases the risk that personal data or biometric information submitted could be easily shared with entities unauthorized by data subjects to see their data. An individual applying for a new job, for example, might have felt comfortable submitting their fingerprints to the local police for a background check as part of a job application; but they might be uneasy having these same fingerprints accessible by other states with standardized systems compliant with ANSI/NIST-ITL-1-2000, yet less scrupulous data protection measures. Standardisation facilitating data exchange should thus be limited whenever possible to nations or entities that maintain at least the same level of data protection as that practiced by the data capturing institution.

Standardisation, however, is not alone in supporting system interoperability; there is also harmonisation. Harmonisation occurs when two or more systems may not meet a given formal standard, but may still be able to interact and smoothly exchange data. For example, while there are conventional ranges for iris systems' near-infrared wavelength illumination, there is no single, standard wavelength for iris biometrics. Still, some iris capture systems can process images generated by others.

Governments should view harmonisation efforts with caution and care, as they provide room for uncontrolled and unchecked interoperability. Standardisation should form the baseline; it should establish the minimum requirement for development and deployment of interoperable biometric and personal detection technologies.

### *System Combinations*

When personal detection technologies and/or biometric technologies are combined, new possibilities arise. System combinations can enable increased efficiency and expansion of scope.<sup>xiii</sup> Whereas the efficacy of CCTV surveillance has traditionally been limited by the live and forensic capabilities of human monitors and system operators, facial recognition technology allows for processing and analysis of data and images at orders of magnitude above what humans can achieve, alone. This can, for example, enable security and law enforcement officials to uncover the presence of undesirable individuals amongst a large crowd with greater ease and speed. The combination of technology expands surveillance from an anonymous, behaviour-based approach to one that also fundamentally assesses identity.

The rise of system combinations can introduce potential threats to privacy and individual rights. Data mining, such as the sifting through hours of surveillance footage to determine subject tendencies and habits that might otherwise have escaped notice, could impact people's freedom of association (Article 12 of the Charter). Concern over being tracked could contribute to a constant aura of concern over disrespect for individual privacy. The same CCTV *cum* facial recognition technology that helps United Kingdom authorities detect the presence of criminals in Newham<sup>xiv</sup> could potentially also be used to create a broad network for tracking, for example, at which rallies persons of interest tend to appear. The increased potential of system combinations should automatically demand extra care to ensure scope creep does not ensue, including delimiting clearly in advance the purpose and objective of combining the systems (in line with the spirit of Directive 95/46/EC's Article 6).

The power of combining systems can also radically alter the balance between reasonable expectation of privacy and government/law enforcement privilege. The 19 arrested attendees<sup>xv</sup> at Super Bowl XXXV, for example, surely did not expect to have voluntary participation in an entertainment event translate into

unwitting and involuntary participation in a law enforcement dragnet lacking specific, predefined targets (which, possibly, would contravene Article 7 of Directive 95/46/EC). As technology continues to advance – often faster than public awareness – the line defining “reasonableness” will have to be redrawn continuously, with “reasonableness” constructed by default as conservatively as possible. The European Commission would be well advised to establish an independent, apolitical body of technology and legal experts to perform this function; it could be the same body as the *ad hoc* group mentioned in the earlier discussion on scope creep.

The above speaks to the larger issue of balancing public interest with individual rights. Where economic needs are the main driver for aggressive pursuit of interoperable system combinations (e.g. – surveying crowds at events to save energy, time, and monetary resources spent on tracking and serving warrants individually), the balance should lie favourably with individual rights, and penalties for the infringement of such rights should be stringent. Where security and safety issues are the main drivers, however, the balance point depends on the principle of proportionality. The immediacy, level, and extent of the threat should dictate the acceptability of the utilized or deployed system combination. Deploying a CCTV and facial recognition system in Newham to catch violent criminals or vandals in vulnerable communities is one matter; surveying a sports audience to discover and arrest tax evaders is another.

### *Cyberspace and the Virtual World*

Cyberspace is as much a part of the contemporary operating environment as the land, sea or air. Moreover, as identified by the National Security Strategy (NSS), it is “the most important new domain in national security of recent years.”<sup>xvi</sup> Its existence is undeniable, and has been for a period of decades, yet it remains a poorly understood domain which is all too often seen as the realm of computer specialists.

Cyberspace, social networking and virtual worlds have created new environments within which people can interact and therefore represent new and challenging areas of research for human and social scientists. New ethical concerns have arisen as a result of the unique relationships possible through virtual interactions.

The internet has increased the availability of information to a much wider audience. Trends towards increased bandwidth and widespread connectivity have led to significant data security risks and vulnerabilities. Surveillance footage may be uploaded, streamed live, and/or downloaded by anyone, making it virtually impossible to secure personally identifying information.

With the emergence of new biometric tools that can conduct reliable face recognition on low resolution and poor quality images, anonymity is no longer possible. In 2007, face recognition specialists from the Massachusetts Department of Motor Vehicles were able to apprehend a rape suspect by running his mugshot from the America’s Most Wanted website against their driver license image database.<sup>xvii</sup> With the saturation of photographs online and increasing tools which leverage these images (such as Polar Rose, which features user-driven identity verification), cases like this are becoming more and more common.

## **Discussion**

Questions for consideration for focus group members include:

- Review the definitions of system interoperability, biometrics, and personal detection technologies. Can these be refined or broadened? What are further examples of specific technologies which may have similar ethical considerations?
- Are the ethical issues discussed above sufficiently comprehensive to cover potential features of future systems? Are there any additional recent cases which may shed light on these discussions or provide further considerations?
- Consider the unique ethical considerations of cyberspace technologies. As we look to the future, are there other potential areas in which increased system interoperability may lead to further ethical issues and complications? What policy and practical measures can this group recommend to minimize potential negative effects?

- 
- i “Description of Work,” 217762 (HIDE) Annex 1 part-B, version 1 of 6-Nov-07, Section A.3.2
- ii [www.biometricgroup.com](http://www.biometricgroup.com)
- iii [www.hideproject.org/about/project.html](http://www.hideproject.org/about/project.html) (8 July 2008)
- iv “Visa shopping” is a phenomenon in which asylum seekers submit applications to multiple nations, simultaneously, or go from country to country looking for asylum, even after being denied, in search of a nation who will accept them.
- v European Commission, “EURODAC: The fingerprint database to assist the asylum procedure,” [http://ec.europa.eu/justice\\_home/key\\_issues/eurodac/eurodac\\_20\\_09\\_04\\_en.pdf](http://ec.europa.eu/justice_home/key_issues/eurodac/eurodac_20_09_04_en.pdf) (10 July 2008)
- vi Nuffield Council on Bioethics, “The forensic use of bioinformation: ethical issues,” [http://www.nuffieldbioethics.org/fileLibrary/pdf/The\\_forensic\\_use\\_of\\_bioinformation\\_-\\_ethical\\_issues.pdf](http://www.nuffieldbioethics.org/fileLibrary/pdf/The_forensic_use_of_bioinformation_-_ethical_issues.pdf) (24 March 2009), p. 40
- vii “EU Backs Biometric Visa Database,” <http://www.findbiometrics.com/article/384> (30 March 2009)
- viii CNiL, “Regulating biometrics,” <http://www.cnil.fr/index.php?id=2455> (30 March 2009)
- ix EDRI, “Prum’s Treaty is now Included into the EU Legal Framework,” <http://www.edri.org/edriagram/number5.12/prum-treaty-eu> (18 August 2008)
- x European Commission, “European Interoperability Framework for Pan-European eGovernment Services.” <http://ec.europa.eu/idabc/servlets/Doc?id=19529> (22 August 2008)
- xi The EZPASS system in the northeast United States allows drivers to use RFID-based transponders to pay tolls at toll booths more efficiently.
- xii Determining who has a legitimate “need to know” is, itself, a debatable issue. However, this is beyond the immediate scope of this document.
- xiii See [http://www.hideproject.org/events/fg-technology\\_convergence.html](http://www.hideproject.org/events/fg-technology_convergence.html) for more information on technology convergence and system combinations.
- xiv James Meek, “Robo Cop,” <http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.html> (6 August 2008)
- xv Scott McNealy, “Privacy is (Virtually) Dead,” <http://www.jrmyquist.com/aug20/privacy.htm> (15 August 2008)
- <sup>xvi</sup> *National Security Strategy: Annual Update 2009*, (UK: Cabinet Office), Jun 09, para.46.
- <sup>xvii</sup> [http://www.nytimes.com/2007/02/17/us/17face.html?pagewanted=1&\\_r=2](http://www.nytimes.com/2007/02/17/us/17face.html?pagewanted=1&_r=2)