



## **FOCUS GROUP MEETING ON SYSTEM INTEROPERABILITY**

### **FOCUS GROUP COORDINATOR**

**International Biometric Group (IBG)**

### **DATE**

**15th September 2008**

### **LOCATION**

**London, UK**

**King's College London (Guy's Campus)**

**Hodgkin Building**

**Large Committee Room**

### **PARTICIPANTS**

**IBG, CSSC, CESAGen, UNI-LJ, Asbjorn Hovsto,  
Ben Schouten**

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

**Date and Time:** 15 September 2008; 11 AM – 3 PM

**Venue:** Large Committee Room, Hodgkin Building, King's College London (Guy's Campus), London, UK

**Nearby Tube Station:** London Bridge (Jubilee Line; Northern Line)



## **AGENDA**

11:00 AM – 11:15 AM	Welcome and Refreshments
11:15 AM – 11:30 AM	Overview of System Interoperability and Ethics Concerns and Introduction to Background Document
11:30 AM – 12:30 PM	Identity Management in eHealth Presentation and Comments on Background Document from Asbjørn Hovstø
12:30 PM – 1:00 PM	Lunch
1:00 PM – 1:30 PM	General Discussion on Identity Management in eHealth and on Background Document
1:30 PM – 2:00 PM	User Empowerment in Biometrics Presentation and Comments on Background Document from Ben Schouten
2:00 PM – 2:30 PM	General Discussion on User Empowerment in Biometrics and on Background Document
2:30 PM – 3:00 PM	Discussion of Future Work Plan and Development of an Ethical Brief

# ETHICAL DIMENSIONS OF SYSTEM INTEROPERABILITY

## Introduction

This document introduces 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 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.

One example of a border security implementation is the United States' US-VISIT program, which collects biometric data from visa applicants, compares the data against databases of known criminals and suspected terrorists, issues visas to cleared applicants, and verifies the biometrics of cleared applicants when they arrive at a port of entry. A second, similar example is the second-generation Schengen Information System, which collects photographs and fingerprints from foreign visa applicants in order to tighten security at the borders of the EU's Schengen region, while facilitating the free flow of traffic within the area.<sup>iv</sup> A third example of border security is the worldwide movement to develop electronic, RFID-enabled passports that meet the 2004 International Civil Aviation Organization (ICAO) standard of including support for face biometrics and fingerprint biometrics. Such e-passports help in confirming that any person tendering such a document is also its legitimate owner. Border control officials in Cambodia have also used thermal imaging devices to detect airline passengers infected with severe acute respiratory syndrome (SARS).<sup>v</sup>

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. One example is the "Ring of Steel" in London. This deployment consists of CCTV cameras and automated license plate recognition technology. The cameras are strategically located at the various narrow streets at the outer edge of the City of London which cars entering the city would have difficulty avoiding.<sup>vi</sup> In another deployment in New Delhi Railway Station, a facial recognition system scans station entry and exit points for faces that match those contained in a criminal watch list. When a match is found, the cameras begin recording.

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 standardization efficiencies.

System interoperability is typically achieved via:

- (1) standardization;
- (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>vii</sup> within Norway, Iceland, and all EU member states, except Denmark.<sup>viii</sup>

Instead of relying on central databases, nations may elect instead to pursue arrangements in which information can be exchanged through systems that store, process, and transmit information according to standardized methods and formats. In 2004, for example, three US states – California, Connecticut, and Rhode Island – established statewide palmprint databases, each of which could be queried by any of the three states.<sup>ix,x</sup> With standardization and interoperable systems, nations are less likely to be restricted to market dominant vendors. This, in turn, can help nations avoid the cost premiums that often accompany proprietary solutions with near-monopolistic positions.

These nations pursuing standardization efficiencies also reduce the costs that would be involved in purchasing numerous solutions to accommodate a variety of different systems adopted in regions where near-monopolistic conditions may not be present. Additionally, adoption of standards may help nations save costs by leveraging best practices as codified in international standards.

The drive towards system interoperability, however, is not absolute. Three interrelated considerations, in particular, serve as restraining forces:

- (1) respect for individual rights;
- (2) data protection obligations; and
- (3) privacy concerns.

The Charter of Fundamental Rights of the European Union (“Charter”) 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.”<sup>xi</sup> 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 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. The following are examples of some of these interrelated ethical considerations.

## **Ethical Issue:** *Scope Creep and Data Centralization*

**Example:** In order to support state functions and needs, such as border security, nations may establish systems to facilitate the exchange of visa data. One example is the European Visa Information System (VIS), a central database that contains 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, there may be temptation to expand usage of the database to support regular criminal background checks by law enforcement. Such usage, in turn, may encourage more liberal use of the database, such as tracking applicants' movements or performing data mining to determine geographical criminal tendencies.

**Analysis:** Information of the type collected for VIS can be useful for many security and safety-oriented agencies: immigration, intelligence, local law enforcement, etc. Allowing one central database to serve the different purposes of these varying agencies would help reduce redundancy and realize efficiencies. Significant money could be saved by avoiding the creation of separate, overlapping databases. Nations would also be able to concentrate their efforts on ensuring interoperability with a single database rather than trying to make their system interoperable with various proprietary systems in other countries.

Yet, the letter and spirit of Article 6 indicates that scope creep should be kept carefully in check. The authorized use of databases created to enable interoperability and smooth exchange of information should be strictly, explicitly, and narrowly defined. A single database should not support two or more functions that are discrete and not directly related, even if both are for important security purposes. Similar, separate databases should be established, instead. Indeed, while Article 6 permits certain additional historical, statistical or scientific uses of data collected, police purposes or national security rationales are conspicuously not included.

Even when centralized databases are used for a limited, well-defined purpose, caution should be exercised. Countries may have varying degrees of institutionalized data protection. Access to centralized databases should thus be restricted only to those who meet the standards of the most stringent contributing nation, unless a common standard has been developed. The alternative, access to comparable, but separate databases, should also be carefully controlled. Under the Treaty of Prüm,<sup>xiii</sup> for example, treaty ratifiers' police forces do not have unfettered, automatic access to each others' 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.

## **Ethical Issue:** *Degree of Consent*

**Example 1:** In the EURODAC program, mentioned earlier, people voluntarily<sup>xiii</sup> submit their biometrics and other personal data to governments in order to become eligible for asylum. By doing so, they agree to allow the potential asylum-granting nation to use their biometrics to confirm that they have entered the EU lawfully and that they have not submitted multiple applications. In an ideal setup, applicants would be providing explicit, informed consent. In reality, however, applicants may not realize that EURODAC's system interoperability may enable countries that may be allies of the country from which the applicant is fleeing to see the candidate's application history – which could lead to retribution. EURODAC may also enable tracking an “asylum shopper's” movement through the EU.

**Example 2:** CCTV surveillance has become a security mainstay in many banks. The cameras that are part of such systems are often visible, contributing a deterrent benefit. Signs may be posted indicating that areas are under video surveillance. When customers choose to enter these areas, they are presumed to be tacitly or implicitly consenting to such surveillance. They may not know, though, that some banks, such as the Bank of Ireland, have pursued system interoperability to allow branch offices to share and access information across a broad network.<sup>xiv</sup>

**Example 3:** In Manchester, England, license plate recognition (LPR) enables police to use their patrol cars to setup mobile checkpoints. The LPR systems, the use of which may not be readily noticeable, can be used to identify vehicle tax evaders, terrorists, and criminals through their interoperability with England's Police National Computer, Driver and Vehicle Licensing Agency database, and local police databases.<sup>xv</sup>

**Analysis:** Article 7 of Directive 95/46/EC clearly specifies that personal data should be processed (which is understood to subsume the collection process) only with unambiguous consent from the data subject. One challenge lies in determining what is “unambiguous.”

In Example 1, applicants actively submit their biometrics, which may be seen as explicit consent. But even in this case, there is potential ambiguity. There is concern over whether or not true consent is being given if the submission is inextricably tied to a critical need (e.g. – the pursuit of asylum to sustain the human dignity and life considered to be fundamental rights). Questions may also arise as to whether explicit consent can truly be given if an individual is not informed of the various ways in which their personal data can be processed, including expansions of use resulting from increased system interoperability.

Explicit consent, therefore, should be linked to informed consent. Explicit consent should also be tied to narrow interpretations of scope. Consent should carry over to other functions and applications enabled by system interoperability only when data subjects are fully aware of, and explicitly consent to, each of those intended functions or applications beyond those originally contemplated.

In Example 2, where tacit or implicit consent is involved, the burden for demonstrating the need for system interoperability is often higher, and the need for safeguards is generally greater (see Figure 1 for a visual depiction of the relationship between consent, proof of need, and safeguards). This is because of the limitations inherent in presumption of consent. An individual can actively and consciously choose to enter an area clearly indicated as under surveillance, but they can only provide tacit and implicit consent in this fashion with respect to the circumstances they directly observe and for the uses they can reasonably expect.

In the case of the Bank of Ireland deployment, tacit consent could also be partially informed consent, as data subjects may accept the physical presence of the cameras as indicative of local surveillance, but be unaware of the fact that the captured data is also being shared across a broad branch network. This could call into question the acceptability of the system's interoperability. Minimally, it puts heavier ethical burdens on the deployment of the interoperable system, including a stronger proof of need for interoperability and the establishment of robust safeguards to ensure that the data is not misused or insufficiently protected (e.g. – a branch studying the banking habits of a customer who has no direct relationship with that branch).

Example 3 poses the greatest ethical challenge of the three examples. The Manchester LPR deployment does not provide for a realistic element of consent or refusal. Drivers typically cannot change course easily to avoid the LPR systems; nor can they necessarily predict the systems' locations, due to their mobile element. Drivers, in fact, might not even know the systems are present and in use; this renders them incapable of exercising an option of refusal or taking protective measures – which, in turn, creates a heavy ethical burden of proof of need for the system. This burden is further heightened by the power of the system due to its interoperability with several databases whose data may not always be up to date or readily accessible by the data subjects for correction (a fundamental right, per Article 8 of the Charter).

Unlike radar guns that focus on limited, discrete instances of speeding that pose an immediate threat to safety, the interoperable LPR systems have access to databases with a broad range of personal data. Any such technology or interoperable system that enables the connection of extensive historical personal information with the present, without the unambiguous consent or knowledge of the data subject and without an immediate threat to safety, should be considered inherently highly suspect and in need of strict regulatory constraints and penalties for abuse.

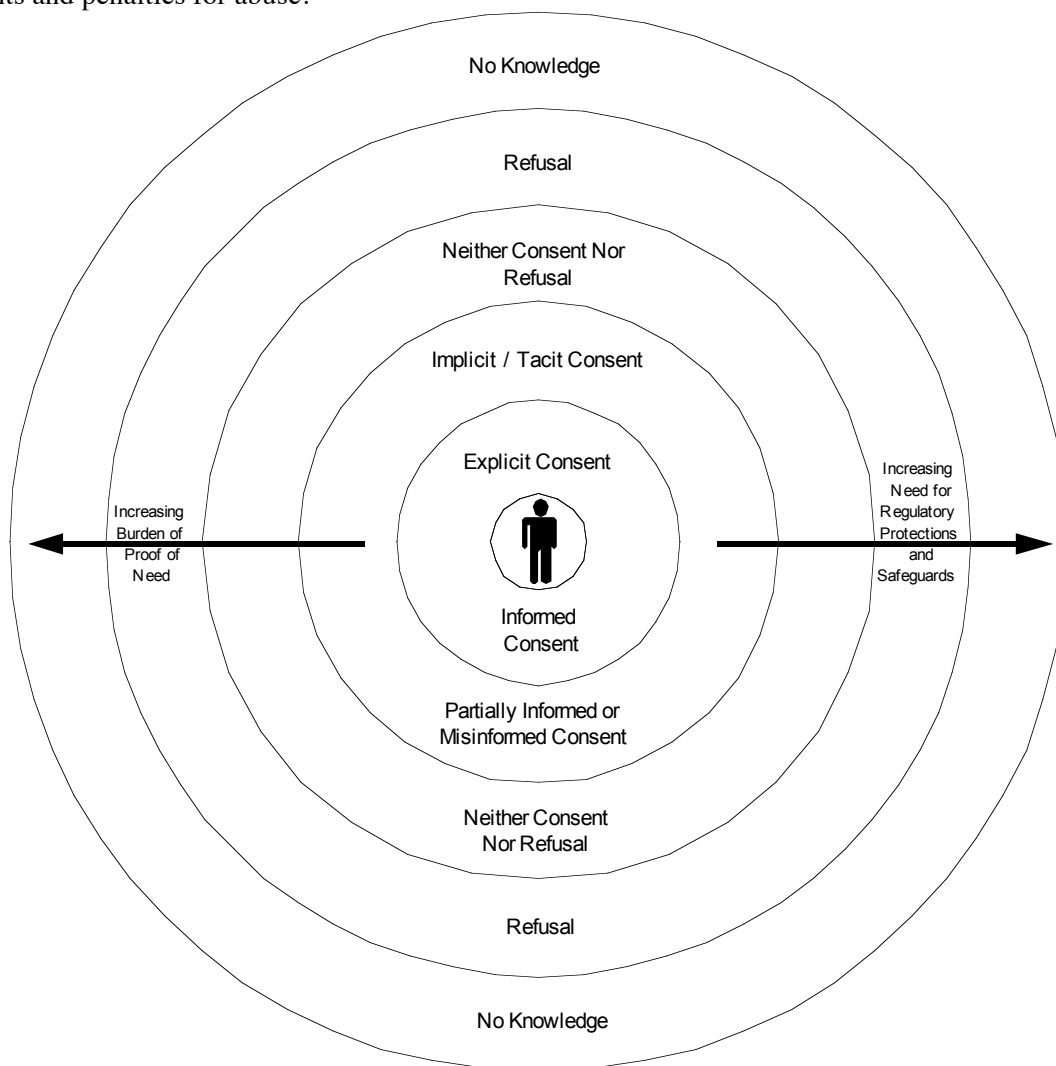


Figure 1: The Interrelationship of Consent, Proof of Need, and Safeguards for Interoperable Systems

## **Ethical Issue: *Standardization and Openness***

**Example 1:** Most major credit card companies have begun deployments of contactless payment systems in the EU. These systems, such as PayPass and payWave, operate based on RFID technology compliant with the ISO 14443<sup>xvi</sup> standard. This standardization, combined with draft specifications from EMVCo.,<sup>xvii</sup> has enabled the development of point-of-sale terminals that are interoperable with contactless cards from multiple vendors.

**Example 2:** In order to facilitate the interchange of fingerprint data amongst European criminal justice authorities and to support border applications, standards have been developed. These standards include ANSI/NIST-CSL 1 1993<sup>xviii</sup> (for EURODAC),<sup>xix</sup> the Interpol Implementation of ANSI/NIST-ITL-1-2000,<sup>xx</sup> and ISO/IEC 19794-2.<sup>xxi</sup> They are open standards that address issues ranging from image quality to descriptors.

**Analysis:** Standardization 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. Many 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. The use of open standards has been recommended by the European Commission in the European Interoperability Framework for Pan-European eGovernment Services.<sup>xxii</sup>

However, the openness of these standards can also 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. In some situations, therefore, standards (such as the specific frequency at which EZ-PASS<sup>xxiii</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>xxiv</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).

Standardization can also contribute to the danger of system scope creep. Standardization 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. Standardization 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.

## **Ethical Issue: *System Combinations***

**Example:** In the east London borough of Newham, United Kingdom, CCTV cameras in public spaces have been augmented by Visionics<sup>xxv</sup> facial recognition technology.<sup>xxvi</sup> The local authorities have arranged for the software to be interoperable with the pre-existing CCTV system consisting of over 200 cameras. This allows Newham more efficiently to surveil its citizenry and visitors for matches against criminal watch lists. The deployment also seeks to deter inappropriate behaviour. A similar deployment combining CCTV and facial recognition technology has also been implemented in Beijing for the 2008 Olympics.<sup>xxvii</sup> Surveillance cameras and facial recognition technology were also infamously used during Super Bowl XXXV.<sup>xxviii</sup>

**Analysis:** When personal detection technologies and/or biometric technologies are combined, new possibilities arise. System combinations can enable increased efficiency and expansion of scope. 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 technology that helps Newham detect the presence of criminals 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>xxix</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 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.

## Conclusion

The ethical issues presented, above – Scope Creep and Data Centralization; Degree of Consent; Standardization and Openness; and System Combinations – do not encompass all the ethical concerns revolving around system interoperability of biometrics and personal detection technologies. However, they provide an introduction to some of the key challenges that can arise when there is tension between individual rights, data protection, and privacy, on the one hand, and security/safety and economic needs, on the other hand. This document seeks to provoke discussion, including delineation of boundaries and clarification of principles, which may support further work on development of formal rules and regulations governing the system interoperability of biometrics and personal detection technologies.

---

<sup>i</sup> “Description of Work,” 217762 (HIDE) Annex 1 part-B, version 1 of 6-Nov-07, Section A.3.2

<sup>ii</sup> [www.biometricgroup.com](http://www.biometricgroup.com)

<sup>iii</sup> [www.hideproject.org/about/project.html](http://www.hideproject.org/about/project.html) (8 July 2008)

<sup>iv</sup> Europa, “Second-generation Schengen Information System (SIS II) – 1<sup>st</sup> pillar legislation,” <http://europa.eu/scadplus/leg/en/lvb/l14544.htm> (27 August 2008)

<sup>v</sup> Asian Economic News, “Cambodia installs thermal imaging scanners to detect SARS,” [http://findarticles.com/p/articles/mi\\_m0WDP/is\\_2003\\_June\\_16/ai\\_103396494](http://findarticles.com/p/articles/mi_m0WDP/is_2003_June_16/ai_103396494) (9 July 2008)

<sup>vi</sup> Wall Street Journal, “License Plate Recognition Ring of Steel from NYC,” <http://www.platescan.com/news/displaynews.asp?NewsID=21&targetid=1> (9 July 2008); IEEE Spectrum, “Ring of Steel II,” <http://ieeexplore.ieee.org/iel5/6/34647/01652996.pdf> (9 July 2008)

<sup>vii</sup> “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.

<sup>viii</sup> 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)

<sup>ix</sup> NEC Solutions America, “NEC Solutions America Customer Honored by California’s Center for Digital Government,” <http://www.necus.com> (December 2004)

<sup>x</sup> Cogent Systems, “Cogent Systems has just received a contract to provide an Advanced Integrated Cogent Automated Palm and Fingerprint Identification System (CAPFIS) for the States of Connecticut and Rhode Island,” <http://cogt.client.sharedholder.com> (October 2003).

<sup>xi</sup> European Parliament, “Directive 95/46/EC,” [http://www.cdt.org/privacy/eudirective/EU\\_Directive\\_.html#HD\\_NM\\_1](http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_1) (11 July 2008)

<sup>xii</sup> EDRI, “Prum’s Treaty is now Included into the EU Legal Framework,” <http://www.edri.org/edrigram/number5.12/prum-treaty-eu> (18 August 2008)

<sup>xiii</sup> Some may argue that asylum seekers lack a realistic alternative to submitting their biometrics (i.e. – their need for asylum and avoiding persecution is so high) and thus the submission is not truly “voluntary.” This is a valid contention that merits further discussion, but exceeds the scope of this document.

<sup>xiv</sup> TAC Satchwell, “Bank of Ireland: Case Study,” [http://www.tac.com/data/internal/data/04/05/1147362496115/10665\\_Bank+of+Ireland+Case+Study.pdf](http://www.tac.com/data/internal/data/04/05/1147362496115/10665_Bank+of+Ireland+Case+Study.pdf) (17 July 2008).

<sup>xv</sup> msnbc.com, “La difference’ is start in EU, U.S. privacy laws,” <http://www.msnbc.msn.com/id/15221111/> (17 July 2008); “Permanent Automatic Number Plate Recognition cameras in Manchester,” <http://www.prlog.org/10070300-permanent-automatic-number-plate-recognition-cameras-in-manchester.html> (17 July 2008)

<sup>xvi</sup> ISO/IEC is the International Organization for Standardization

<sup>xvii</sup> D. Balaban, “Standard Reader on Tap for Contactless Payments,” <http://www.cardtechnology.com/article.html?id=20071204B0EQM8XS> (21 July 2008)

<sup>xviii</sup> ANSI/NIST is the American National Standards Institute / National Institute of Standards and Technology

<sup>xix</sup> Council Regulation (EC) No 407 / 2002, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:062:0001:0005:EN:PDF> (22 July 2008)

<sup>xx</sup> D. Benini, “Storing biometric images in documents,” *Keesing’s Journal of Documents*, Issue 4 (2004)

<sup>xxi</sup> IEC is the International Electrotechnical Commission

<sup>xxii</sup> European Commission, “European Interoperability Framework for Pan-European eGovernment Services.” <http://ec.europa.eu/idabc/servlets/Doc?id=19529> (22 August 2008)

<sup>xxiii</sup> The EZPASS system in the northeast United States allows drivers to use RFID-based transponders to pay tolls at toll booths more efficiently.

<sup>xxiv</sup> Determining who has a legitimate “need to know” is, itself, a debatable issue. However, this is beyond the immediate scope of this document.

<sup>xxv</sup> Now part of L-1 Identity Solutions.

<sup>xxvi</sup> James Meek, “Robo Cop,” <http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.html> (6 August 2008)

---

<sup>xxvii</sup> Emily Chang and John Vause, “100,000 security forces on alert for Olympics,”  
<http://www.cnn.com/2008/WORLD/asiapcf/08/06/olympics.security/index.html?iref=topnews> (6 August 2008)

<sup>xxviii</sup> Declan McCullagh, “Call It Super Bowl Face Scan I,” <http://www.wired.com/politics/law/news/2001/02/41571> (22 August 2008)

<sup>xxix</sup> Scott McNealy, “Privacy is (Virtually) Dead,” <http://www.jrnyquist.com/aug20/privacy.htm> (15 August 2008)