

Deliverable 3.2a – Ethical Brief on System Interoperability of Biometrics and Personal Detection Technologies



HIDE PROJECT

Project funded by the European Commission-FP7

Contract: 217762

Co-ordination and Support Action (CSA)

Start date of the project: 1 Feb 2008

Duration 36 months

1° Reporting Period

Deliverable:	D3.2a <i>Intermediary</i>
Title:	Ethical Brief on SI
Due date:	30.07.2009
Actual submission date	30.07.2009
Lead contractor for this deliverable:	IBG
Contact:	vlee@biometricgroup.com
Dissemination Level:	PU



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 International Biometric Group. 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.

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.¹
- *Biometric systems* perform the automated measurement of physiological and/or behavioural characteristics to determine or verify the identity of an individual.² 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.³

This document provides background information and guidance to government officials, policy makers, ethicists, legal counsel, technology researchers and developers, practitioners and deployers, as well as the general public. This ethical brief is born out of deliberations and debate amongst members of the HIDE Focus Group on System Interoperability, an eclectic consortium of private and public sector representatives, as well as academics, holding various perspectives on the issue of system interoperability of biometrics and personal detection technologies. While the document focuses primarily on the European perspective, international experiences also inform the issues and conclusions addressed in this paper.

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.⁴ 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).⁵

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.⁶ 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 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”⁷ within Norway, Iceland, and all EU member states, except Denmark.⁸

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.^{9,10} With standardisation 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 standardisation 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. Respect for individuals and their rights can serve as a restraining force and may manifest in data protection legislation and privacy policies.

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.”¹¹ 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.

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. For example, vascular recognition scanners in biometric identification applications should not be employed to determine a subject's medical condition unless both uses have received an informed subject's explicit consent. This will become increasingly important as technological advances increase the number of technologies that can be redirected to identification and personal detection purposes.

Determining if a subject is properly "informed," however, can pose a challenge, due to the existing "public knowledge deficit." First, biometrics and advanced personal detection technologies are unfamiliar to many people. They may not be aware of the extent of these technologies' capabilities. Second, data subjects may not know the extent to which the systems leveraging these technologies are interoperable. A partially informed or uninformed subject, for example, might be comfortable with their nation collecting their fingerprint data, but be unaware of the potential for that fingerprint data to be shared with other allied nations, something about which they could be distinctly less comfortable.

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.

In some countries, government mismanagement of personal data (e.g. – the loss of two CDs containing extensive personal data in the UK in 2007¹²) has led to distrust of governmental ability to control and protect sensitive data. By openly educating their data subjects, governments have the opportunity to re-establish or reinforce trust with their citizenry and communities. This trust is a prerequisite for successful deployments of personal detection technologies and biometrics that leverage their full capabilities and potential for system interoperability. Greater trust, after all, can be conducive to eliciting consent more freely.

Obtaining explicit, informed consent, however, is often impractical. Unanticipated improvements in system interoperability could enable new uses of data for which the obtaining of explicit consent in each instance could pose a repeated inconvenience to the data subject, in addition to practical challenges for the data collector (if the data subject has left the jurisdiction of the data collector, for instance). While both data subject and data collector might prefer to invoke blanket consent or combinations of consent at the time of first data collection or approved use/exchange, this should generally be avoided, particularly because of the common modern human tendency to execute consent forms quickly without thoroughly – if at all – reading said forms.

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. But there should be a clear and demonstrable threat to public security, safety, or order, with independent mechanisms for assessing and validating the legitimacy thereof. Such mechanisms would be the first step in safeguarding against abuse (see Figure 1 for a visual depiction of the relationship between consent, proof of need, and safeguards).

Abuse of such privilege granted under implicit social contracts subsuming citizen consent is wholly and utterly unacceptable; it should result in significant penalties clearly codified in law. Such abuse must be strictly monitored for and rapidly addressed where present. Furthermore, the exchange and use of such data across interoperable systems spanning multiple countries and governments (surpassing the jurisdiction of any implicit social contract) should be forbidden without data targets' explicit, informed consent or – at the very least – their reasonable expectation of such exchange or use, based on the culture, laws, and affiliations of their host nation. Indeed, this is effectively required for meeting the “unambiguous” provision of consent required per Directive 95/46/EC.

In some situations, governments or other data collectors may have a reasonable and compelling need for collecting and exchanging biometric and other personal data – but a need that is not driven by immediate public security and safety interests. In such cases, data collectors should not resort to the capture, exchange, and use of personal data without the data subjects' explicit and informed consent. Instead, the data collectors should tie their application of interest to another application of particular appeal to their data subjects. While both applications would require separate, explicit, informed consent, consent for the latter would only be accepted following the obtaining of consent for the former.

One example, employed in the US-VISIT program, would be tying consensual submission of fingerprint data for authenticating and determining the legitimacy of a visa holder to consensual use of the same fingerprint data for background checks. It is important, though, that there be a genuinely voluntary aspect to any consent solicited and/or obtained. While individuals may be incentivized to submit biometric or personal data (e.g. – “no data, no entry to the US”), care must be taken that “incentives” do not become “necessities.” Indeed, the long-term success of most programs that involve the collection, use, and/or exchange of biometrics and other personal data will depend on the degree to which participation in such programs is voluntary.

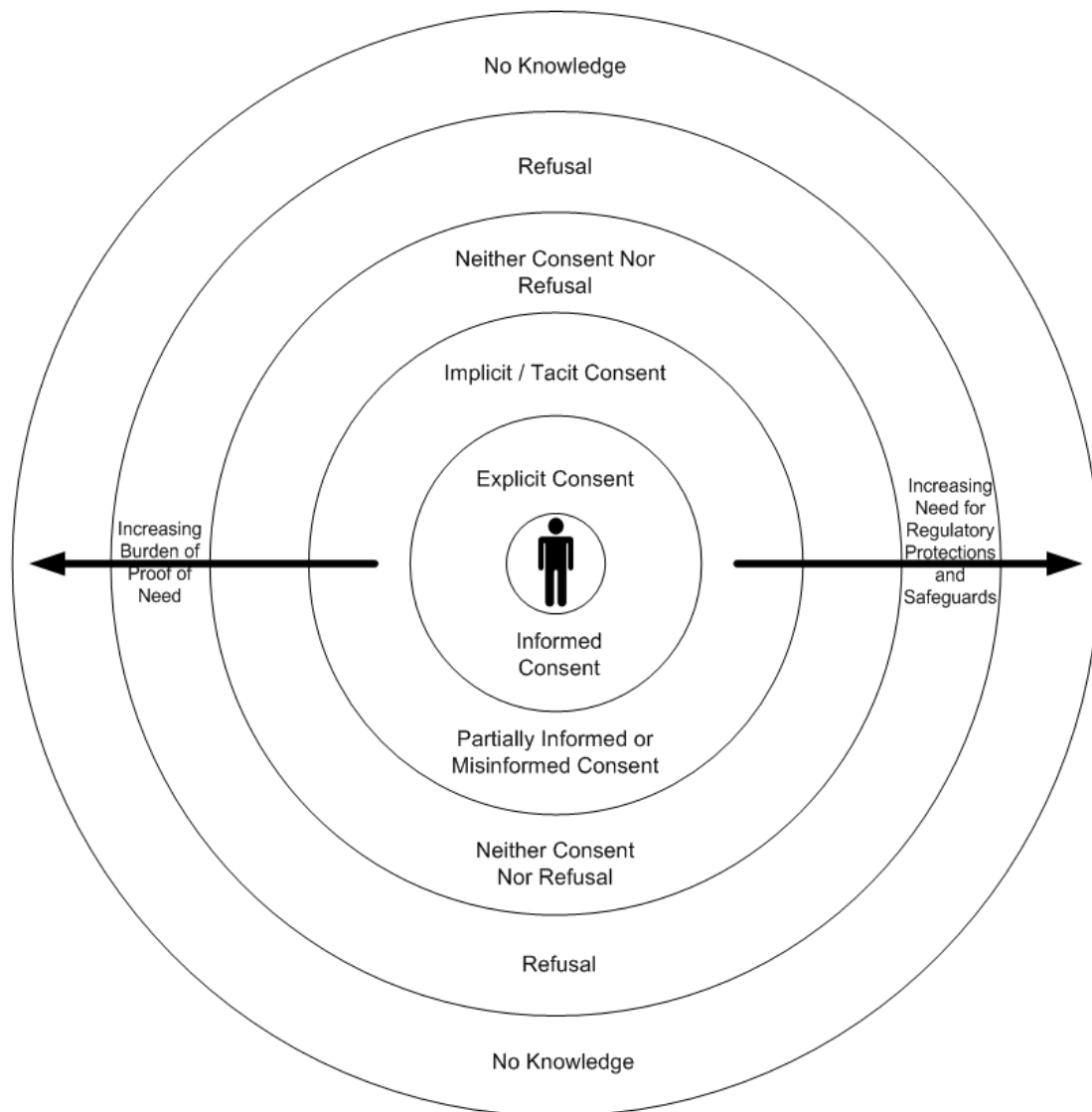


Figure 1: Interrelationship of Consent, Proof of Need, and Safeguards for Interoperable Systems

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. Ideally, such incentives would be relevant to the data collection program under consideration, rather than completely independent – which could more easily be construed as an ethically precarious bribe.

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

As stated earlier, 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.”¹³ 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.

Technological solutions should be complemented by policy efforts. Legislation and legal frameworks must be in place to help constrain, direct, and guide the development of technological and social solutions. Effective law and policy setting, whether by bodies like the European Commission or by individual data protection authorities, should clearly and openly define acceptable limits for uses of biometric and personal detection technologies. Legislation should also afford a course of remedial action and penalties in the event of violation or infringement. Pure reliance on market forces or organic research and development growth will not be sufficient and could disfavour poorer nations unable to afford the same technological protections as their wealthier neighbours, absent funding from the European Commission.

Ideally, such legislation would be consistent internationally, with some room for modest variation due to specific national circumstances and cultural considerations. One way to approach this would be to have the European Commission (or its designees) set policy at the European Community level, with individual data protection authorities weighing in on a case-by-case basis with respect to the implementation of policy.

A superior approach, however, would be for the European Commission to appoint an ongoing *ad hoc*, international, and apolitical group of legal and technology experts who would provide recommendations for European Commission approval. This would increase the likelihood of developing effective, consistent legislation that can address long-term considerations without succumbing to short-term political mood swings or the five-year focus of a Commissioner's term. These experts would likely be better attuned to the long-term trends in technology development and their impact on system interoperability and the potential for scope creep.

Even if legal and technology issues are carefully controlled, however, social forces and desires for additional functionality can still exert notable influence on scope creep. In several instances, technology and law respond to social influences more than they shape them. Tools, such as iris recognition technology, which were once the near-exclusive domain of the military and the security-conscious wealthy, have now been adapted and expanded in scope to accommodate registered traveller programs as Europeans demand more efficiency at border checkpoints without an accompanying decrease in security. Programs like Privium at Schiphol International Airport¹⁴ and IRIS in the United Kingdom¹⁵ ostensibly aim to serve this public need.

Such registered traveller programs can acclimate people to what was once an extraordinary application. Over time, such deployments become familiar – if not mundane – and raise the threshold for public concern. 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.

Social desires for added convenience can also drive expansion and scope creep. Registered traveller programs that were once isolated deployments are now becoming parts of larger networks of interoperable systems. In the United States, for example, Vigilant Solutions' Preferred Traveller¹⁶ and Verified Identity Pass' CLEAR¹⁷ programs were independent at one point, but have since become interoperable, enabling both companies' customers to take advantage of a broader range of serviced venues. In Europe, events like Wise Media's Registered Traveller Forum, as well as Open Skies accords, like the 2007 Air Transport Agreement, are encouraging similar continental and trans-Atlantic interoperability.

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. This invokes privacy concerns and may eventually serve as a travel deterrent, effectively derogating EU citizens' right of free movement accorded by Article 45 of the Charter.

In addition, 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. If Country X, for example, leverages system interoperability to share data on one of its citizens with Country Y but then wishes to retract all foreign instances of that data, it may be difficult to reverse this process. Increased system interoperability would also facilitate the technical exchange of that same data between Country Y and a third country without Country X's knowledge.

Though Western governments are often expected to be responsive to their constituents and sensitive to political winds, such authorities can – and should – also play a subtle role in influencing social needs and desires. Government authority and funding are needed to help ensure that the demands of the public do not end up in outcomes that, though seeming beneficial for a single individual (e.g. – faster movement through

an airport security checkpoint), may ultimately be deleterious to the public good or undermine collective civil liberties and rights (e.g. – right of free movement). As mentioned earlier, in addition to its regulatory role, government should assume the role of educator. Governments should allocate funds to road shows, publications, workshops, etc. designed to inform the public of the true capabilities of biometrics and personal detection technologies. With more complete knowledge, the citizenry make better educated decisions that will be reflected in the overall social need and mood.

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.

Information of the type collected for VIS and EURODAC can be useful for many security and safety-oriented agencies: immigration, intelligence, law enforcement, etc. Allowing one central database to serve the different purposes of these varying agencies can help reduce redundancy, realize efficiencies, and highlight fraudulent activity through duplicate detection. Significant money can be saved by avoiding the creation of separate, overlapping databases. Instead of trying to make their own systems interoperable with various proprietary systems in other countries, nations can concentrate their efforts on ensuring interoperability with a single database.

Central databases can thus serve an important function in facilitating the smooth 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,¹⁸ 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,¹⁹ 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,²⁰ 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 leveraged RFID technology compliant with the ISO 14443²¹ standard. This standardisation, combined with draft specifications from EMVCo.,²² 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. These standards include ANSI/NIST-CSL 1 1993²³ (for EURODAC),²⁴ the Interpol Implementation of ANSI/NIST-ITL-1-2000,²⁵ and ISO/IEC 19794-2.²⁶ They are open standards that address issues ranging from image quality to descriptors.

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.²⁷

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-PASS²⁸ 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”²⁹ 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.³⁰ 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 Newham³¹ 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 attendees³² 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.

Conclusion

The ethical issues presented, above – Consent, Scope Creep and Expansion, Data Centralisation, Standardisation, Harmonisation, 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 greater insight into 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.

To help address these ongoing and ever evolving challenges, the HIDE Focus Group on System Interoperability of Biometrics and Personal Detection Technologies recommends that the European Commission appoint an ongoing *ad hoc*, international, and apolitical group of legal and technology experts who would provide recommendations for European Commission approval. Such a consortium would be able to resolve questions of policy reasonableness, facilitate coordination and consistency across geographical and geopolitical regions, and provide guidance and direction from a long-term perspective partly removed from the immediate pressures and influence of vacillating political stances in the short-term.

This brief has offered guidance and recommendations drawn from inputs provided by representatives from the private, public, and academic sectors. The brief aims 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.

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

2 www.biometricgroup.com

3 www.hideproject.org/about/project.html (8 July 2008)

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

5 Asian Economic News, “Cambodia installs thermal imaging scanners to detect SARS,” http://findarticles.com/p/articles/mi_m0WDP/is_2003_June_16/ai_103396494 (9 July 2008)

6 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)

7 “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.

8 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 (10 July 2008)

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

10 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).

11 European Parliament, “Directive 95/46/EC,”

http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_1 (11 July 2008)

12 BBC News, “UK’s families put on fraud alert,” http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm (23 March 2009)

-
- 13 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 (24 March 2009), p. 40
- 14 C. Perri, “The Eyes have it: Iris scanners a hit,” http://www.biometricgroup.com/in_the_news/miami_herald.html (27 March 2009)
- 15 UK Border Agency, “Iris recognition immigration system,” <http://www.ukba.homeoffice.gov.uk/managingborders/technology/iris> (27 March 2009)
- 16 See <http://www.jax-vip.com/Default.aspx>.
- 17 See <http://flyclear.com>.
- 18 “EU Backs Biometric Visa Database,” <http://www.findbiometrics.com/article/384> (30 March 2009)
- 19 CNIIL, “Regulating biometrics,” <http://www.cnil.fr/index.php?id=2455> (30 March 2009)
- 20 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)
- 21 ISO/IEC is the International Organization for Standardisation
- 22 D. Balaban, “Standard Reader on Tap for Contactless Payments,” <http://www.cardtechnology.com/article.html?id=20071204B0EQM8XS> (21 July 2008)
- 23 ANSI/NIST is the American National Standards Institute / National Institute of Standards and Technology
- 24 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)
- 25 D. Benini, “Storing biometric images in documents,” *Keesing’s Journal of Documents*, Issue 4 (2004)
- 26 IEC is the International Electrotechnical Commission
- 27 European Commission, “European Interoperability Framework for Pan-European eGovernment Services.” <http://ec.europa.eu/idabc/servlets/Doc?id=19529> (22 August 2008)
- 28 The EZPASS system in the northeast United States allows drivers to use RFID-based transponders to pay tolls at toll booths more efficiently.
- 29 Determining who has a legitimate “need to know” is, itself, a debatable issue. However, this is beyond the immediate scope of this document.
- 30 See http://www.hideproject.org/events/fg-technology_convergence.html for more information on technology convergence and system combinations.
- 31 James Meek, “Robo Cop,” <http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.html> (6 August 2008)
- 32 Scott McNealy, “Privacy is (Virtually) Dead,” <http://www.jnyquist.com/aug20/privacy.htm> (15 August 2008)