

Deliverable 4.3a– Policy Forum Report on Outsourcing of Biometrics and Personal Detection Technologies for Detection, Identification, and Authentication



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:	D4.3a <i>Intermediary</i>
Title:	Ethical Brief on Outsourcing
Due date:	30.07.2009
Actual submission date	30.07.2009
Lead contractor for this deliverable:	IBG
Contact:	vlee@biometricgroup.com
Dissemination Level:	PU

www.hideproject.eu



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

BACKGROUND

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. HIDE's mission is to set up a platform devoted to ethical and privacy issues of biometrics and personal detection technologies which addresses transnational (European) and international problems. HIDE aims to become the preeminent catalyst for innovative policy solutions to emerging ethical problems in the area of surveillance technologies, especially where collaboration among national and international agencies, communities, businesses, and non-governmental organizations (NGOs) is crucial. HIDE promotes creative problem solving and provides for concrete tools for a successful dialogue.

One of HIDE's areas of focus is the outsourcing of biometrics and personal detection technologies. Today, governments and corporations are more willing to outsource their functions, processes, and procurement to entities in other countries. This is due in part to technological advancements in communications and transportation that have prompted increased regional and international interaction. Moreover, the emergence of super-state structures such as the European Union (EU) and the European Economic Area (EEA) facilitates the flow of information across national boundaries and supports the establishment of transnational economic relationships.

The growing proliferation and rapid development of biometrics, personal detection systems, and related technologies in the private sphere have provoked a paradigm shift in which public sector entities increasingly rely on the often faster-moving and more cost-efficient private sector for once-core government responsibilities such as security operations and identity management. This growing global trend is driving extensive outsourcing of personal information processing and storage.

International Biometric Group (IBG) organizes and chairs the HIDE Policy Forum on Outsourcing of Biometrics and Personal Detection Technologies for Detection, Identification, and Authentication. The mission of the Outsourcing Policy Forum, a component of the HIDE project, is to become the pre-eminent international forum for discussion, analysis, and debate on privacy, data protection, and other ethical issues associated with outsourcing of biometrics and personal detection systems.

Outsourcing Policy Forum participants represent the public and private sectors, as well as academia. Vendors, system integrators, academics, data protection authorities, advocacy groups, and think tanks all contribute to the forum. The forum's business is conducted through face-to-face meetings, newsletters, email listserves and exchanges, online bulletin board discussions open to the general public (<http://forum.hideproject.org>), and a custom Wiki.

POLICY FORUM ACTIVITIES

Policy Forum activities commenced with IBG developing a background document and drafting a position paper that outlined key ethical, privacy, and data protection issues regarding the outsourcing of biometric and personal detection systems. Simultaneously, IBG began raising awareness of these outsourcing issues by reaching out to academia, data protection authorities, think tanks, law firms, vendors, trade associations, consultancies, and system integrators. From these entities, IBG selected nine guest experts to participate in the first face-to-face meeting of the Policy Forum.

On 6 February 2009, IBG hosted the first HIDE Policy Forum event, titled “Outsourcing of Systems for Detection, Identification, and Authentication.” 27 forum participants from 10 countries across North America, Europe, and Asia gathered at Regent’s College in London, United Kingdom for a day-long conference. A list of participants and speakers is presented, below.

Name	Affiliation	Role
Valeria Balestrieri	CSSC	Participant
Bojana Bellamy	Accenture	Speaker
Wieslaw Bicz	Optel	Participant
Kirsten Bock	Independent Centre for Privacy Protection	Speaker
Alastair Campbell	National University of Singapore	Participant
Antonella Caretta	Garante per la Protezione dei Dati Personali	Speaker
Antonio Casseli	Garante per la Protezione dei Dati Personali	Speaker
Simon Dobrisek	University of Ljubljana	Participant
Katja Jacobsen	CESAGEN	Participant
John Leach	IAAC	Speaker
Victor M. Lee	IBG	Moderator / Speaker
Karen Maschke	The Hastings Center	Participant
Paul McCarthy	CESAGEN	Participant
Lokke Moerel	De Brauw	Speaker
Ariane Mole	Bird & Bird	Speaker
Emilio Mordini	CSSC	Participant
Tom Murray	The Hastings Center	Participant
Lisbeth Nielsen	National University of Singapore	Participant
Alexander Nouak	Fraunhofer	Participant
Karolina Owczynik	Zuyd University	Participant
Alain Pannetrat	CNIL	Speaker

Carole Pellegrino	SAGEM	Participant
Chris Pounder	Amberhawk	Speaker
Rafaella Puggioni	John Cabot University	Participant
Max Snijder	EBF	Speaker
Michael Thieme	IBG	Moderator
David Wright	Trilateral Research & Consulting	Participant

Subsequent to the face-to-face meeting of the Policy Forum, IBG implemented the following online resources:

- the official HIDE Outsourcing Policy Forum subpage (http://hideproject.org/events/pf-outsourcing_of_surveillance.html);
- a public bulletin board (<http://forum.hideproject.org/viewforum.php?f=11>); and
- a custom Wiki (http://wiki.hideproject.org/twiki/bin/view/Main/WP4_TestingReframing/PF3_Outsourcing/WebHome).

These resources host presentations from nine subject matter experts, as well as the minutes from the face-to-face meeting in London. Policy forum members have also collected, supplied, and updated the online resources with background documents, position papers, relevant news reports, and related articles. This method of exchanging information has especially facilitated communication, interchange, and debate between the forum's experts. It is supplemented by the occasional use of a Policy Forum email listserv.

The forum has also reached out to existing listservs (e.g. – the [biometrics] Yahoo group) to encourage participation and debate in the online forums. Over seven different, provocative threads for debate have been opened on the public bulletin board, alone. Additionally, the Policy Forum has summarized the proceedings and key takeaways from its face-to-face meeting in *Dialogue*, the official HIDE newsletter.

The Policy Forum's next steps include continuing to reach out to data protection authorities and subject matter experts who could not attend the face-to-face meeting. Some of these individuals had indicated interest in the subject of outsourcing and expressed a desire to see the outcomes and conclusions from the face-to-face meeting. Their independent review and commentary on the Policy Forum's conclusions and key recommendations is always desirable.

The Policy Forum will also concentrate future efforts on soliciting feedback from the broader, more general public. This will help the Policy Forum further develop and

clarify its position, leading to a more coherent and consistent set of positions amenable to all forum members and participants.

POLICY FORUM OPINIONS, POSITIONS, AND RECOMMENDATIONS

Using IBG’s background document and draft position paper as a starting point, participants at the face-to-face meeting of the Policy Forum weighed the benefits and costs of the trend toward outsourcing biometric systems and personal detection technologies. Participants pointed out that significant ethical questions arise when the public sector outsources its functions or procurement activities to the private sector, especially when the private outsourcer lies outside the traditional national boundaries and jurisdiction of the public sector contractor. This is largely because of the special responsibilities and authorities held by public sector entities who wield legal, not consumer-driven, mandates.

Governments, for example, have the authority to collect, process, maintain, and store sensitive personal data from their citizenry. They also have the responsibility for ensuring national security and defending their citizens’ individual rights. Reliance on the private sector and its free-market principles and economic incentives for these activities could result in dangerous degrees of risk-taking or compromise as to the “acceptable” costs of data loss or theft; this is especially problematic when the private sector may be less open than the public sector about how it handles and deals with personal data.

Recognizing the above, Forum participants discussed considerations such as:

- differences between domestic public-to-private (onshore) outsourcing and international public-to-private (offshore) outsourcing;
- tension between the desire for cost savings and the risk of stolen or impounded data; and
- standardization of data protection across the European Union and the broader world.

One of the major challenges identified by the forum participants is the discrepancy across the EU in approach and attitude towards data protection and outsourcing. Bojana Bellamy of Accenture pointed out that, for systems integrators dealing with several different countries, these discrepancies create inefficiencies and headaches due to the need to constantly modify and tailor Accenture's approach for each nation.

Presentations from Antonio Caselli and Antonella Canetta (Garante per la Protezione dei Dati Personali), Kirsten Bock (Independent Center for Privacy Protection Schleswig-Holstein), and Alain Pannetrat (Commission nationale de l'informatique et des libertes) revealed different attitudes and approaches towards biometrics, outsourcing, and data protection. France's CNIL, said Pannetrat, adopts a very cautious approach that almost never allows biometric data to be processed by outsourcers for access control needs, even when those outsourcers are in France. Germany's ICPP, by contrast, is more open to outsourcing products and services, provided they meet standards rendering them eligible for a European Privacy Seal (EuroPriSe) Trust Mark. However, the ICPP privacy seal is not suitable for use across the entire EU. Furthermore, the EuroPriSe seal is currently only voluntary.

Participants were intrigued by the idea of creating an EU-wide seal that would clearly indicate which outsourced products or services at least meet a minimum EU-wide standard for data protection. They decided that this concept merits further study and investigation.

Participants also recognized that the first step to achieving standardization across several nations was defining terms and roles in a consistent fashion. Chris Pounder of Amberhawk suggested a definitional framework (generally accepted by the forum participants), which involves three key players: the data protection authority, the data controller, and the data processor. The data protection authority sets standards and provides guidance to data controllers, such as governments, who are ultimately responsible for determining the desirability and purpose of an outsourcing activity. Data controllers, in turn, are responsible for selecting and vetting data processors, who handle that outsourcing activity.

Data protection authorities would do well to spend more time coordinating their efforts and policies, perhaps through the European Data Protection Supervisor or an ad hoc, independent body. This could be reinforced through European law in conjunction with custom. While respect for cultural differences and nuances is important and requires some degree of customization of policy, the increasing internationalism of many governments and private companies suggests a need for a similarly extensive, common approach.

Also, data protection authorities need to allocate more resources to educating the public about the sensitivity of biometric and other highly personal data and the risks

that outsourcing can bring. Such efforts to develop privacy awareness and acceptance of markers, such as a trust seal, will help the public better accept and distinguish legitimate data collection and outsourcing risks from questionable, inflammatory concerns. It will also build up the public confidence if data protection authorities enforce transparency.

Data controllers, for their part, need to learn the nuances, power, and potential for abuse of the technologies and services they are considering. Forum participants recommend that data controllers treat biometric and other personal data as particularly sensitive information that demand a greater degree of care and protection when being handled or transferred to an outsourcer than might be afforded to other types of data. Data controllers also have a responsibility to establish clearly worded, transparent contracts with their data processors so that it is clear what penalties may be involved in the event of improper data disclosure. Finally, forum participants urged data controllers to regularly conduct privacy impact assessments.

As for data processors, these recipients of outsourcing contracts need to develop internal mechanisms for ensuring that there is a culture of privacy compliance. This can be executed through internal audits, process control, and privacy by design. Data processors also need to have a good command of mitigation strategies for data loss or leakage. Means of anticipating potential breaches and measures for handling such occurrences need to be carefully designed and practiced, especially when sensitive biometric or highly personal data is involved.

Additionally, data processors will increasingly need to be as transparent as possible when it comes to explaining how they process and handle sensitive data. With the advent of cloud computing, the complexity of the Internet-based infrastructure behind the provisioning of cloud computing services cannot be permitted to serve as an excuse for lack of clarity in regards to how data will be protected and privacy will be assured. The complex processes may be abstracted in the cloud, but the safeguards must be specific and plainly evident.

Overall, Forum participants agreed that outsourcing the processing of biometric or personal data could be beneficial to governments, provided the data processors remained within the government's immediate jurisdiction or within "EU-compatible" countries. However, the key conclusion was that countries' positioning towards outsourcing (and the limits and reaches, thereof) need to be better coordinated and made more consistent across the EU. In the meantime, countries are advised to adopt the policies of the most stringent and data protective entity involved when outsourcing is in play. Only then can countries develop the requisite public trust needed to increase the political viability of outsourcing the handling of sensitive data.

ISSUES FOR FUTURE INVESTIGATION

The Policy Forum brought together disparate parties to begin the process of defining a common taxonomy and structural approach to outsourcing of systems that collect and process biometrics and other personal data. The Forum also highlighted several key issues and areas that remain to be analyzed and discussed in future Forum conversations and sessions. They are as follows:

- The dominant focus of the European Data Protection Supervisor (EDPS) is on supervising institutions and bodies of the EC, like the European Parliament and the European Commission. Should it take a more active and legally-empowered role in enforcing consistency across various nation-specific data protection authorities?
- In the event of a data breach that violates data protection obligations, who should be responsible: the data processor or the data controller? Should both share responsibility? If so, how would such liability be divided between the processor and the controller?
- Should data protection authorities take the role (as in the French model) of conducting prior authorization reviews of proposed data processing activities? Or should they (as in the German Schleswig-Holstein model) adopt a role more focused on independent verification and certification? Is there a different model altogether that would be even more appropriate for adoption across the EU?
- Who should maintain ownership of personal data throughout the outsourcing process? The data subject? The data controller? The data processor? The data protection authority?
- Should there be different policies for treating different types of data? Should biometric data be afforded more data protection than other personal data (such as birth dates, medical data, national ID numbers, etc.)? Or should policies be consistent regardless of the type of data involved?