

HIDE System Interoperability Focus Group 2 – Minutes

On December 7, 2009 from 10am-3pm, HIDE partners met with several subject matter experts for the second meeting of the HIDE project Focus Group (FG) on System Interoperability. The meeting was held at Kings College, Guy's Campus in London, UK.

Participants:

Michael Thieme, IBG

Mary Collins, IBG

Dr. Paul McCarthy, CESAGEN

Dr. Simon Dobrisek, University of Ljubljana

Silvia Venier, CSSC

Xuebing Zhou, Fraunhofer IGD

Bénédicte Havelange, European Data Protection Supervisor (speaker)

Katarzyna Cuadrat-Grzybowska, European Data Protection Supervisor (speaker)

Dr. Caroline Wardle, SAMURAI Project (speaker)

Catherine Edlin, SAMURAI Project

Dr. Philip Tresadern, MOBIO Project (speaker)

Sapna Capoor, AGNITIO (speaker)

Philip Statham, CESG, Retired (speaker)

Dr. Caroline Wardle is a Visiting Professor of Computer Science at Queen Mary, University of London. She joined Queen Mary in 2007 after retiring from the National Science Foundation (NSF) in the U.S.A. Dr. Wardle's research and teaching interests have ranged over broad areas of computer science, software engineering, information systems, the ICT workforce, women in computing, and computer ethics.

Sapna Capoor is the Director of Corporate Development and Strategy (Global Markets) at AGNITIO, a voice recognition company. She has authored numerous studies and white papers on different aspects of the biometrics industry. She has worked with clients on biometrics/security based projects ranging from product development strategies to entering new geographic markets.

Since 2008, Dr. Philip Tresadern has been with the Imaging Sciences group at the University of Manchester, developing facial feature localization methods for image normalization in biometric authentication systems. He is currently working on the MOBIO Project.

Bénédicte Havelange and Katarzyna Cuadrat-Grzybowska work for the Policy and Information Unit of the European Data Protection Supervisor. They coordinate of the EDPS' activities related to EU large-scale IT systems and to border management/immigration/asylum issues. Their main tasks at the EDPS are organizing the coordinated supervision of EURODAC (EU database on asylum seekers), drafting legal opinions on EU legislative proposals, providing advice on EDPS policy, following up on the development of new EU large-scale IT systems (i.e. SIS II, Visa Information System, Customs Information System).

Philip Statham spent his career working at Government Communications Headquarters (GCHQ) the UK Government Signals Intelligence Agency and its information assurance division CESG. As the CESG Biometrics Programme Manager, he founded and chaired the UK Government Biometrics Working Group. Additionally, he served on the Home Office Biometric Assurance Group and provided advice on biometric security and security evaluation to the UK Government ID Card program. He continues to participate in international biometric standards work as a UK National Body representative to the ISO SC 37 Biometric Standards committee and as an SC 37 liaison officer to SC 27 on biometric security evaluation methodology standards.

Michael Thieme opened the meeting with a brief overview of the HIDE project and led round table introductions of all present. The structure of the FG consisted of five presentations each followed directly by a brief discussion period.

Presentation 1: Dr. Caroline Wardle, SAMURAI Project

The first speaker, Dr. Caroline Wardle, presented on the SAMURAI Project - **S**uspicious and **A**bnormal Behavior **M**onitoring **U**sing a **N**etwo**R**k of **C**Ameras for **S**ituation Awareness Enhancement. SAMURAI is an FP7 program led by Queen Mary University of London with seven other partner organizations. The program seeks to leverage existing CCTV cameras all over the UK and develop additional mobile and sensor capabilities to facilitate intelligent surveillance at critical public sites.

Dr. Wardle walked the group through a typical control room with eighty feeds being monitored by only one or two operators to demonstrate the enormous data overload encountered by security professionals. The SAMURAI project aims to tackle this data overload and improve operational effectiveness to enhance global situational awareness and help security analysts avoid missing vital information. Other goals of the project include gathering video evidence that holds up in court and developing tools to review footage and conduct post-event analysis. Currently, SAMURAI is focused on detecting and monitoring persons, vehicles, and luggage. Research challenges include networking multiple cameras, developing anomaly detection algorithms and person-in-the-loop learning, tracking of moving targets in multiple views, and global data fusion and visualization.

Dr. Wardle then raised several ethical considerations relevant to SAMURAI. She made the claim that, because all surveillance projects involve human subjects, they all must consider privacy and data protection issues of utmost importance. Dr. Wardle particularly emphasized the concept of **dual use** – the idea that technology originally developed for commercial or civil applications can potentially be appropriated for use in government or military applications.

Dr. Wardle explained that the EU requires an ethical checklist to be completed for each project it funds. The checklist contains a variety of common ethical considerations, including the issue of dual use. Based on her review of many of such forms throughout her professional career, Dr. Wardle reported that very few projects, if any, indicated that dual use was an ethical concern. She put forth the argument that, despite being often overlooked by scientists and program managers, dual use is an important consideration that is relevant to *all* technology projects. Dr. Wardle then opened the floor for questions and further discussion.

Thieme asked if SAMURAI is planning to implement a biometrics component at any point. Dr. Wardle said biometrics is not currently within the scope of the program and any future retrofitting of a biometric system (such as face or gait recognition) would be very complicated to incorporate. Dr. Simon Dobrisek commented that biometrics is really a subfield of pattern recognition and therefore relevant. Among technologies used for behavioral analysis of abnormalities, machine learning, data mining, and pattern recognition are the main technology categories. Thieme referenced a previous contribution from Emilio Mordini, who has suggested that biometrics can be used as a classification tool to assign persons to certain groups – as an example applicable to SAMURAI, people acting suspiciously in airports. Dr. Wardle said the project has two phases: stage 1 is actually building the system, and stage 2 involves refining and calibrating it.

Thieme then revisited the issue of dual use and opened a discussion on its relevance to SAMURAI. He noted that in the US, military funding is the primary driver for research, and as such, technologies developed for anti-terrorism purposes are now finding broader applications in the civil market. Dr. Wardle commented that directionality is important when considering ethical implications of dual use. Technology movement from military to civil applications is more permissible than the reverse – when technology developed for civil applications is repurposed or appropriated by the government.

A debate then ensued as to why dual use has not been as widely discussed as other ethical issues, both in literature and in practice. Dr. Wardle believes a key issue is that many scientists and researchers generally do not have very much general ethical training at all, and are typically more concerned with advancing development of new technologies rather than worrying about potential misuse. Dr. Dobrisek

made the analogy of a knife that is created to slice bread but can also be used to kill – he suggested all technology can involve similar unintended use problems.

Dr. McCarthy suggested a reason for why so few of the mandated ethical forms contained a check next to “dual use” – checking a box suggests that a project may be unethical rather than showing foresight and careful consideration. Scientists will often default to leaving a box blank to avoid complications and out of fear of not being funded. Dr. Wardle conceded that, but also asserted that promoting ongoing discussion of ethical issues can increase awareness and lead to legislation. Returning to the knife analogy, she referenced laws regulating the length of blades permissible to possess. Laws like these, while not all-encompassing, can help curb the use of technology in an unintended and abusive fashion.

Presentation 2: Sapna Capoor, AGNITIO

Sapna Capoor gave a presentation on AGNITIO, a voice recognition company, and several case studies and recent deployments. AGNITIO was founded in 2004 and has developed five main voice recognition solutions primarily geared towards law enforcement and intelligence applications. Voice recognition is a unique biometric in that it is the only biometric that can be collected remotely (i.e. through a phone or audio recording device) and it is relatively easy to integrate because of existing telephone and voice-over-IP infrastructure.

Capoor then outlined AGNITIO’s deployment with the Guardia Civil in Spain. AGNITIO built a comprehensive voice database to be used as an investigatory tool. All biometric samples (fingerprint, face and voice) are collected during booking. A detainee can refuse to participate in any part of the process, though fingerprint and photo records can be enforced by a judge. Voice recording cannot be mandated at this time, however a defendant’s lawyer cannot legally object to voice sampling if it is ordered by the judge at a later stage in the trial. To date, refusals to enroll in the system have been rare. Detainee voices are only recorded during specific crimes due to practical constraints such as length of enrollment time, data storage requirements, and system processing time. Voices are also enrolled from cases and investigations – either by recording or in person.

The database is integrated with SIGO-Delincuencia (Ministry of Interior database of criminals) and SAID (Spanish AFIS) and is used as an investigatory tool to identify speakers from intercepted telephone calls. Most cases involve terrorism, drugs, and/or organized crime. Telephone interceptions are similar to the concept of latent fingerprints – voices captured in the course of a crime investigation such as bomb threats or kidnapping calls.

Dr. Wardle was concerned with possible scope creep – AGNITIO’s voice database maintained by the police could be exploited for commercial purposes. For example, a person may be required to provide a voice sample for background checks before receiving a loan. Capoor noted that such systems would necessarily have strict data protection protocols in place, and that it is important to review the legal context on a case-by-case basis, as legislation can vary widely by country.

Capoor also suggested that there are pros and cons to any biometric deployment, and that while it is possible that an individual’s identity may be compromised, such cases are the rare exception and not the rule. She believes it is important for biometric solutions providers to establish the benefits of biometric systems to help justify potential risks taken on by users.

Thieme commented that voice biometrics have been historically developed in the context of improving customer service and to replace call operators with an automated system. The forensic application demonstrated by AGNITIO is a much more recent use case. Voice biometrics appear to have taken the opposite trajectory of fingerprints – which have traditionally been used for law enforcement purposes and later expanded to commercial and civil applications.

Thieme suggested that risk perception associated with voice may be due to the fact that people are not as familiar with it as a biometric modality. Because face and fingerprints have been around for longer, people feel somewhat more comfortable with the risks associated with providing them. Capoor also

believes that perceptions towards voice in the United States are relatively negative due to unsuccessful early deployments of older technology that is not as robust as current techniques.

As voice continues to develop and become more widely deployed, standards and legal frameworks will need to be updated to accommodate unique aspects of the technology and how it impacts privacy. Capoor briefly discussed relevant work in progress to develop a standard for voice models and a secure voice biometric template. Current data is stored in encrypted .wav files. The goal is to produce a non-proprietary, sanitized audio format to insure the content of what a person is saying is protected.

Dr. Dobrisek raised ethical considerations based on the performance of 1:N voice systems. He commented that relying purely on voice biometrics in court cases is very dangerous – the error rates associated with short samples are too high to justify convictions beyond reasonable doubt. Capoor agreed, and asserted that convictions should never be based purely on voice or any other biometric data but rather a combination of evidence. She did note, however, that the presence of voice data is often enough to compel settlements and suggested that the technology can be leveraged by law enforcement as a deterrent.

Dr. Wardle brought up the issue of spoofing. Thieme relayed findings from past research and testing conducted at IBG in which recorded voice samples were easily recreated and able to be spoofed. However, the simple addition of a behavioral component – such as changing the text of the sample each time – would be enough to strengthen a system sufficiently against playback vulnerabilities. He also noted that while voice may be easier to spoof than a modality with a more dynamic interaction, such as fingerprint or iris, this should not undermine deployment of such systems. Capoor also mentioned that AGNITIO has developed some anti-spoofing capabilities to address asynthesized attacks, though she did not go into further technical detail.

Zhou commented based on her experience with data protection work that a major challenge is the ease in which face images are acquired and can be compromised – voice as a modality is susceptible to the same problem. Dr. Dobrisek also noted that criminals are often ahead of developers in terms of spoofing. There are many techniques which can be used to encrypt the voice stream or change the quality of voices within recordings, such as by adding or manipulating acoustical voice vectors. Dr. Dobrisek questioned the point of deploying a technology that may catch a few inexperienced crooks but burdens several million people, especially when the major culprits are able to defeat the technology and escape detection.

Statham stressed the importance of clearly outlining how technology should be used in advance in an effort to anticipate possible attacks or misuses. He believes technological advancements should not be blocked simply because there is a chance for abuse but rather planned thoughtfully in a context-specific fashion. Dr. McCarthy agreed, but was skeptical that the benefits of such systems are clear enough to justify wide-scale deployment.

Presentation 3: Dr. Philip Tresadern, MOBIO

Dr. Philip Tresadern presented on the MOBIO (Mobile Biometry) project and related privacy and ethical considerations. The MOBIO project is an FP7 program that investigates the use of biometrics for securing private data that can be accessed through mobile devices. The motivation for the project stems from the increasing accessibility of the internet in recent years. Improved communication and display technologies have facilitated a shift towards mobile connectivity. People use their mobile phones for accessing email and online calendars, as well as internet banking and shopping on the move. Most of these applications require users to verify identity before granting access to private data. Traditionally, this has been achieved by usernames and passwords, but because passwords are easy to steal and may be forgotten, the MOBIO project explores the use of biometrics for personal device access.

The nature of mobile implementations presents some practical constraints on data storage and processing power. However, newer phones are coming equipped with high-end processors that can

process information captured through increasingly sophisticated sensing devices (cameras and microphones), making development over mobile platforms more feasible.

The MOBIO project investigates bi-modal authentication using two data streams – face and voice – which are fused to provide more robust performance. The problem of detecting faces has been solved – digital cameras all come standard with reliable face detection algorithms. However, one of the research challenges which MOBIO attempts to conquer is finding landmarks within faces. Using data that varies by subject, lighting, pose, and expression, Dr. Tresadern and his team localized facial landmarks and generated statistical models of shape and texture. The face models are then unwarped, accounting for variation in shape and lighting, to generate 2D images for comparison. The compiled research database contains images and video from 100 subjects.

Dr. Tresadern then outlined several key project considerations related to privacy and data protection. He grouped the concerns into two main categories: misuse of data, and misuse of technology.

Misuse of Data

Misuse of data deals with questions such as who has access to the data, how it is controlled, and whether or not the same data may be obtained without consent of the user.

Some biometric data is already being stored in centralized databases such as face images from passports or driver's licenses. The Driver and Vehicle Licensing Agency in the UK recently received media attention for losing large amounts of data. If data is stored on a centralized database, deployers must consider what measures are in place to ensure the data is not transferred to a memory stick/CD/laptop that could consequently be lost or used for unintended purposes.

The alternative to centralized repositories of biometric information is to retain all data on the mobile device itself. However, this poses risks of data theft if the phone is ever lost or stolen. Dr. Tresadern also pointed out a counter-argument that most mobile phone users are very careless anyway for storing various personal details on their mobile phone without even password protection. Mobile internet access only aggravates these issues.

In a biometric system, it is unacceptable to store raw data, not only for privacy reasons but because, in most cases, not all of the data is relevant. Data is usually processed to extract features that can be used for matching and then encrypted. For a system to work properly, two faces, for example, cannot map to the same vector – this would mean that the user is compromised and imposter attacks would be possible.

An additional consideration is determining what data needs to be sent to the server. Transmitting biometric data allows the opportunity for interception and copying. However, conducting all processing directly on the phone or mobile device and simply sending an accept/reject instruction to the server may open the door to mimicry by hacking.

Given that voice biometric data can be easily recorded, impostors may be able to use such recordings to gain fraudulent access. Many science fiction stories have involved bypassing biometric systems by removing the required body part (eyes and fingers, commonly) from the subject. Evidence suggests this has occurred (albeit on a very limited scale) in real life. A system that permits this kind of fraud presents a serious threat to the safety of the users.

Dr. Tresadern then considered other traditional means of authentication. One common criticism of passwords is that they are easily lost or stolen. However, they can also be easily concealed, unlike some biometrics (the face, in particular). Passwords and PINs can also be changed at will if they are compromised. This is not the case with biometrics – once they are compromised, they lose all value. One way to address this problem is to introduce a random perturbation to the biometric data before it is used. Therefore, if the system is compromised, only the hash must be regenerated, and the data remains secure.

Dr. Tresadern asserted that when researchers or deployers collect data to be released to the public, they have an obligation to those providing data to protect their identity. He outlined some of the considerations and efforts made by the MOBIO team to minimize the amount of personally identifying information linked to the subjects in their research database.

Misuse of Technology

Misuse of technology concerns the effect of applying or the potential to apply similar technology for other tasks to which the user did not consent.

Because of the prevalence of security cameras, automatic identification in surveillance applications is a major concern. Face recognition on such a large scale raises serious issues with respect to false positives (i.e. wrongful accusation). Dr. Tresadern demonstrated why a system that works well for a small number of users may result in false positives when scaled up to many users. Any persons with faces similar to a perpetrator on a watchlist are at risk of false suspicion.

Location tracking is another potential concern. There are a variety of ways in which signals from mobile phones can be used to track individuals. GPS technologies provide even more accurate means of pinpointing location. Dr. Tresadern stresses the importance of careful reading of any agreements that discuss what data phone companies may collect and distribute without consent.

The face modality presents unique ethical concerns because of the fact that faces can convey information such as gender, age, race, religion, and health, among other characteristics. A system could be designed which automatically classifies within these variables and discriminates accordingly.

Presentation 4: Bénédicte Havelange and Katarzyna Cuadrat-Grzyvbowska, European Data Protection Supervisor

Havelange and Cuadrat-Grzyvbowska gave a joint presentation on their work at the European Data Protection Supervisor (EDPS) and relevant system interoperability and privacy considerations.

Havelange opened with a brief overview of the landscape in the EU and the role of the EDPS. Data protection is considered of utmost importance in the EU; it has been defined as a fundamental right and is a pre-condition for establishing mutual trust between authorities. Data protection protocols are not only ethically relevant but they actually help make systems more effective and should not be considered an obstacle to deployment of new technologies.

The mission of the EDPS is to ensure the protection of people whose data are processed by the European Community institutions and bodies and to give advice on new legislation that has data protection implications. Havelange noted that it is very rare that their office opposes a certain system or technology, rather their opinions indicate that certain projects should be handled with care and may include recommendations for deployment. The three roles of the EDPS are supervision, consultation, and cooperation. The EDPS supervises the central parts of EURODAC, SIS II, VIS, and CIS and has issued numerous comments and opinions relevant to system interoperability issues (the most recent Opinion related to this topic was released 10 July 2009). The EDPS also cooperates actively with national data protection and joint supervisory authorities.

Havelange and Cuadrat-Grzyvbowska then discussed several key principles of data protection:

- **Purpose limitation principle:** collection of data must be justified by explicit, clear, legitimate purpose
- **Proportionality principle:** superfluous data need not be collected; all data should be stored no longer than necessary
- **Data quality:** accuracy and quality checks must be performed routinely to ensure that data is reliable and up to date
- **Transparency:** data subject must be informed of the purpose of collection and usage of data

- **Security:** appropriate measures should be taken to prevent accidental or unauthorized access, alteration, dissemination, destruction, or loss of data
- **Data subject's rights:** the right of subjects to access (directly or indirectly), rectify or erase their data must be considered; such rights can actually increase the quality of data in the systems

Cuadrat-Grzyvbowska then provided some additional thoughts about the future of data protection within the context of new programs and legislation. The Lisbon treaty and Stockholm Programme will both have an effect on the legal and political landscape in Europe.

Havelange expressed some general comments on the concept of interoperability. It can sometimes be difficult to create legislation and policy regarding system interoperability because there is no universal definition. Interoperability is not purely a technical issue, moreover, just because something is technically possible, it does not make it necessary. For example, merging databases is not always a good idea. Havelange stressed the importance of first determining exactly what is the goal of a particular program and plan accordingly. She also warned that technology is almost never dismantled once it's been deployed, which is another reason to proceed with caution.

System interoperability can help avoid the risks associated with double storage – the fewer copies of sensitive information in existence the better. However, it also increases risk of function creep and merging of databases with different purposes. Havelange also worries about using biometrics as a primary key because of its statistical nature – biometrics will never be 100% reliable. Dr. Dobrisek suggested that a primary key is a way to locate someone physically. He explored the idea of using biometrics as a type of key-keeper which secures data unless law enforcement or the government needs it. For example, if a person defaults on a bank loan, only then is the bank granted access to his/her address, otherwise there is no need for them to have information which ties individuals to a physical location.

Thieme asked if the EDPS makes any distinction between practical functionality and just the possibility for interoperability. He noted that standards are built to facilitate openness, but this could be seen as a potential drawback if one opposes system interoperability because of the potential risks associated with it. Havelange conceded it is difficult to know the future and provide recommendations to cover all scenarios but that their office will sometimes advocate that certain systems are never made interoperable, though this is rare.

Havelange advocated the need for case-by-case assessments, taking into consideration the data protection principles of necessity, proportionality, and purpose limitation. Open democratic debate should lead to clear and careful policy choices. Cuadrat-Grzyvbowska noted there is sometimes a disconnect between practical application and the legal process.

Presentation 5: Philip Statham, Biometric Standards – Security, Usability & Privacy

Statham presented on biometrics standards work relating to security, usability, and privacy. He discussed work done by subcommittees ISO/IEC JTC1 37 on Biometrics and ISO/IEC JTC1 27 on IT Security Techniques and also provided links to several current reports and standards drafts.

Standards

Statham began with an overview of SC 37 TR 24714 Biometrics - Jurisdictional and Societal Considerations for Commercial Applications. Part 1 provides general guidance on a variety of topics including jurisdictional issues, accessibility, health and safety, usability, societal, cultural and ethical aspects of biometrics, and acceptance. SC 27 CD 24760 contains a Framework for Identity Management that defines concepts, requirements, and implementation issues for deploying identity management solutions and maintaining privacy. SC 27 WD 29101 focuses on requirements for managing and protecting Personally Identifiable Information (PII). Statham then mentioned SC 37 29144 – “The use of biometric technology in commercial identity management applications and processes.” This standard is still in its first working draft and pertains to life profile events. Statham also provided information on SC 37 29194 – “Guidance on the Inclusive Design and Operation of Biometric Systems.” So far, the draft

contains an inventory of medical conditions which may impact biometric vulnerability as well as some general advice on system requirements to deal with potential problems.

Statham then transitioned to SC 27 CD 24745 “Biometric Template Protection,” regarding biometric security and privacy issues. This pertains to the notion of renewable biometric references, a claimed solution to some common privacy concerns about biometrics. This technique was developed as part of the TURBINE project (TrUsted Revocable Biometric IdeNtitiEs). The key feature is anonymization of biometric data through translation to a (renewable) password. Such technology is commercially available from privID, though Statham noted some issues. It is unclear how privID’s technology deals with the problem of biometric variability – they have alluded to this but there is no clear indication of how it works. Additionally, Statham would like to know performance and error rates compared to other biometric technologies. Such technology is also not necessarily suitable for 1:N applications, and may present obstacles to interoperability because of its proprietary nature.

Statham then outlined three main recommendations from the Privacy Task Force for future standards work. The first step is to compile all relevant work and create a roadmap for the future. Second is development of a document which defines common terminology in the area of privacy and data principles. Lastly, establishing and maintaining a live means of sharing information and collaborating would facilitate ongoing privacy-related work.

Security

Security depends on the application and means something different for access control, beneficial services, and surveillance. Factors which affect biometric security include basic performance parameters, human interaction, and vulnerabilities. SC 37 29156 provides Guidelines on Performance Requirements for Security & Usability in access control applications.

With biometrics, there is a trade-off between False Accept Rate (FAR) and False Reject Rate (FRR). A low FAR is correlated with increased security, whereas a low FRR is correlated with increased usability. Failure to Enroll (FTE) rates also impact usability. With respect to passwords, length and randomness (entropy) are security factors, and represent the same trade-off between security and usability. With tokens, technical design and manufacture are security factors, but do not have any bearing on usability. All authentication methods have potential security weaknesses. Biometrics may be subject to spoofing, capture/replay, and database attacks. Passwords may be easy to guess or difficult to remember. Tokens can be lost or stolen. Both passwords and tokens are easily shared and subject to software and hardware attacks respectively.

Governments have developed risk models to assess the security of authentication methods. These have typically been aimed at protecting the agency, not individuals enrolled in the system. US Govt. M-04-04: E-Authentication Guidance for Federal Agencies categorizes harm and impact factors, provides assurance levels for which to rank the reliability of a system, and shows the links between risk and assurance.

Usability

Usability is a concern for all human/system interactions, not just for biometric systems. Additionally, usability problems with biometric systems may not be a problem with the biometrics. Statham cited as an example the Iris Immigration System in UK airports. The main challenge associated with deployment was in gate design and finding an optimal height for the sensor that accommodates as many people as possible.

NIST has defined several usability criteria for biometrics, including success rates (effectiveness), time on task (efficiency), time to learn a task (learnability), number of errors made over time (memorability), and user satisfaction level (satisfaction).

Multi-factor authentication offers the potential to optimise the trade-off between security and usability. The strength of one factor may be able to compensate for the vulnerability of another. For example, a modest password plus a biometric may provide the security of a strong password while also providing

good usability. However, establishing an optimum trade-off between the various factors of a multi-factor authentication mechanism can be difficult because the strengths and weaknesses are different in kind.

Dr. McCarthy continued the discussion regarding cultural factors and usability. He noted that because of different values across cultures, it is extremely difficult to establish a global definition for privacy or security. Statham agreed and said that while standards will define common concepts, it will be left to countries to create their own policies and determine compliance.

Thieme noted that the standards community was quick to define lots of terms and requirements relevant to interoperability but is now slower when it comes to issues of usability, security, privacy – this makes work like the HIDE project particularly relevant and useful. Other current privacy initiatives mentioned by the group include an EDPS partner group in Spain working on international privacy standards, the newly created TMB Privacy Steering Committee, and the Rising pan European and International Awareness of Biometrics and Security Ethics (RISE) project.