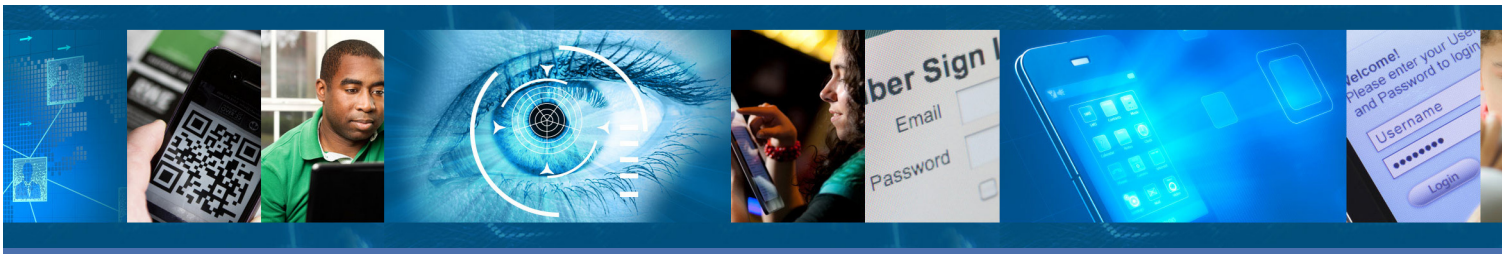
Partnership for Conflict, Crime & Security Research

IMPRINTS
Public responses to Identity Management practices & technologies

Identity Management (IM) Future Threats and Opportunities Policy Seminar

Monday 9 June 2014 at RUSI London



Opening Presentations

Welcome

Dr Tristram Riley-Smith - External Champion for Partnership for Conflict, Crime & Security (PCCS) Research (formerly Global Uncertainties Programme)

Dr Tristram Riley-Smith welcomed attendees, explaining that Policy Seminars like this were designed to support his mission to help research deliver impact by making a difference in the real world (e.g. through illuminating the thinking of policy-makers).

IMPRINTS[1] is an important project within the PCCS Research portfolio that Dr Riley-Smith champions[2]. IMPRINTS is a comparative and multidisciplinary research project, exploring how British citizens respond to influences to engage and/or disengage with the Identity Management (IM) practices, services and technologies of the future.

IM matters because identity matters, sitting at the heart of practically every conflict in the world. But this has been made all the more topical because of the technological transformation affecting the lives of everyone around the world:

- in 2011 the OECD said that digital IM will be fundamental for the full realisation of the economic and social potential of the internet; we won't have trusted social and commercial interaction without trusted identities;
- in 2013, the UK Government's Foresight report on the future of identity, highlighted ***"the emergence of hyper-connectivity (where people can now be constantly connected online), the spread of social media, and the increase in online personal information"*** as ***"key factors which will interact to influence identities".***

There is intense activity at the level of governments and corporations to develop new and better ways of IM. For instance:

- Estonia is a world leader in **e-government**, with a mandatory national E-ID card launched in 2002, serving as the access card for all of Estonia's secure e-services, ranging from logging into bank accounts from a home computer to i-voting, from accessing government databases to check your medical or tax records to picking up e-Prescriptions;
- the UK has organised its e-government service through assured identity providers: citizens wanting to use online government services need to register with selected providers like Digidentity, Experian, Mydex, the Post Office or Verizon.

Meanwhile, industry is exploring a host of different forms of ID management, ranging from the RFID chip inserted under the skin to Motorola's idea of an identity pill that would swallow each morning, turning your body into an authentication instrument to interact with the internet of things (from your 'phone to your fridge or car).

---

1 "Identity Management - Public Responses to Identity Technologies and Services".

2 The Partnership for Conflict, Crime & Security Research (formerly known as "Global Uncertainties Programme") has six research themes: Terrorism, Ideologies & Beliefs, Transnational Organised Crime, Chemical, Biological, Radiological and Nuclear Proliferation, Threats to Infrastructure, and Cyber Security. A seventh - Conflict & Conflict Resolution - has now been added.

But we don't know enough about the desires and taboos of the intended users of these new technologies. What do consumers and citizens want? How can we design new ID technologies that will resonate with them and make them secure and confident in the handling of their personal data? This is the topic for today's seminar. We will hear from a world class research project, IMPRINTS, that was selected in a sandpit competition three years ago (with key stakeholders from the government and the corporate sector): this research brings together the expertise of four universities and ten researchers from human computer interaction, psychology, design studies, political science and communication studies. It has been financed by the Engineering and Physical Sciences Research Council.

Outputs from IMPRINTS will help shape the issues and assist those working in this area - whether this is on policy, design or commercialisation. There is also an important ethical dimension to be considered with introducing any IM system, and Dr Riley-Smith cited another PCCS Research project, which is developing a Framework for Responsible Research & Innovation in ICT (see: http://www.responsible-innovation.org.uk/torrii/).

Introduction to the IMPRINTS Project

Professor Liesbet van Zoonen - Professor of Media and Communication at Loughborough University

Research Challenges and Approach

Professor van Zoonen initially set the context for the IMPRINTS project, emphasising the complexity of public attitudes to IM by reference to the **Privacy Paradox** where, for example, people in the UK reject identity cards but appear happy to use *Loyalty* cards; in other countries, like The Netherlands, there is concern over electronic patient records but people share many personal details on Facebook; while there is a fear of identity fraud in general, people are very careless with their personal data.

A common mistake of researchers working on IM tools and practices is to assume that users apply reason and common-sense as they go about their daily routines. It is the case that IM technologies are more readily accepted if they are easy to use, efficient and deliver added value; but this doesn't solve the privacy issue.

The IMPRINTS research project has taken a different approach to existing studies by focusing its questions on the **effects of culture** on perceptions of IM, exploring the way in which taboos and desires affect the way that people feel about future identity technologies. Experts and "early adopters" of new technologies have been consulted, prototypes and performance artworks have been commissioned, and scenarios have been developed to help policy-makers, designers and developers think about the future of IM.

E-Identification is one of the themes investigated, in light of the need to develop better and faster e-government services. The Belgian and Estonian governments, among others, are using this technology so that their citizens can be authenticated before they access government services. In doing so, they make use of **Biometrics** - an IM approach that is best known as a way of controlling refugees and countering terrorists. Biometrics policy in the UK and US appears to be focused on security and preventing threat; but Biometrics could be used for supporting a large number of public (as demonstrated by those European governments).

Popular culture and film has also been considered in the context of how Identify Management is represented. In Britain, the prevailing narrative is around identification for surveillance purposes, with the state seen to be controlling the individual. This view can be traced back to George Orwell's *1984* - with all subsequent narratives being a variation on that theme.

IM has also inspired artists. Some are working to develop technologies that are more appealing, but other artists have adopted a critical stance, creating make-up and hair designs that counter facial recognition and intelligent CCTV systems, rendering identification difficult if not impossible.

Professor van Zoonen referred to work being undertaken by big corporations in relation to IM technologies. She mentioned the development of smart ink tattoos as well as work on implanted RFID chips (although some US states have already legislated against employers using such devices on their employees).

The IMPRINTS researchers have used a number of different techniques to gather public attitudes to IM, including:

- Focus Groups;
- Cultural Probes (where artifacts are given to participants under circumstances that elicit responses that throw light on their thoughts and values);
- Q-Sort (where participants are given a range of statements and asked to rank them);
- Survey Games (developing games about IM and the future).

Research Findings

There seems to be little concern among the public about **current** IM practices and procedures: it is not a pressing issue and few problems were reported. However, access to novel IM processes is socially stratified: it is mainly the elite who are gaining experience of these technologies, especially those who travel widely and regularly.

Many of the participants in this research also struggled to identify a need or benefit for **future** forms of IM, although the more familiar people are with the technology the more popular it is. Personal taste plays a large part in this: those wish to be seen as 'cool' are more likely to adopt innovative tools and techniques. But context is also important: for instance, many people saw the benefits of IM applied to health.

A key conclusion appears to be that there is no "pull" from ordinary users for new IM technologies - these are very much being "pushed" by proponents (e.g. in Government) and developers. There is, furthermore, a great deal of ignorance and uncertainty about what future technologies may be able to offer. The IMPRINTS research discovered that if this level of indifference and/or disinterest is to be overcome, future IM systems are going to have to deliver **convenience, control and choice** to the citizen, in order to generate a positive interest in - even a desire for - the technology.

Furthermore, security is going to be an issue, with the growth in biometric systems raising people's concerns about governance issues. It is clear from the IMPRINTS research that the public expect those who are responsible for establishing governance policy - in order to regulate these technologies - to give careful consideration to the following:

- Data Segregation: data (linked to identity) should only be used for a specified function, and must be kept separate, for that purpose;
- Proportionality;
- Informed Consent and Opt-In procedures;
- Digital Legacy;
- Fear of Commercialisation;
- Desire for Monetisation.

One key conclusion from this research is that **one size does not fit all**. Any future IM technology must be scalable and accessible to many different kinds of people.

Breakout Sessions

Session A: Design Issues in IM

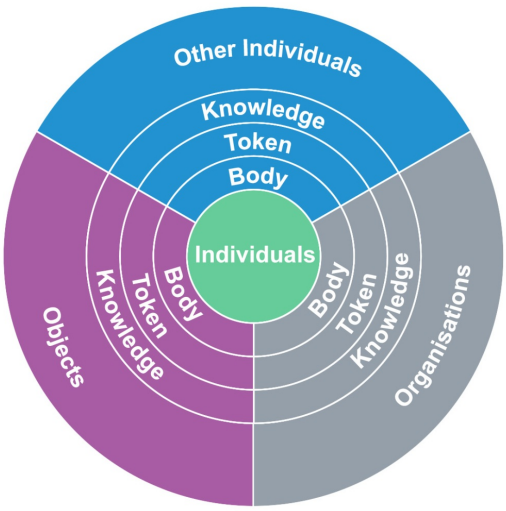
Led by Sandra Wilson and Lilia Gomez Flores (IMPRINTS)

The design-focused strand of IMPRINTS took place over three years:

- Year 1 was about sourcing scenarios of IM in art and design.
- Year 2 included a series of hackJam competitions - where designers from diverse backgrounds came together to identify solutions for IM.
- Year 3 was dedicated to finalising prototypes.

This session considered the **process of design** (in particular hackJam, and cultural probes) and **design outcomes** (featuring ways to design individual expression, mass personalisation as opposed to mass production, and incorporating personal narratives into wearable technologies). Key products from an International Design Competition were also shared with participants.

The Process of Design



There are three fundamental forms of IM: ***knowledge*** - i.e. passwords & PIN-codes; ***tokens*** - e.g. paper based and smart wearables; and ***body*** - i.e. biometrics. It was suggested that the first of these will become less important in the future (not least because of the practical difficulties in holding secure and confidential knowledge systems in our heads). Meanwhile, there are opportunities for tokens and biometrics to work together, and this is becoming increasingly common: for example, a smart wearable scarf can carry identity information (as a token) that is only activated if it recognises the heartbeat of the wearer.

IMPRINTS had taken these fundamentals and subjected them to innovation through a ***hackJam***, where participants were brought together in groups and given a series of challenges and materials to work up IM designs. This is how they were recruited:

We are looking for universities, colleges, businesses, hackerspace groups and individuals to organise a ***hackJam*** to shape the future of identity management. Hacking is a cultural phenomenon that borrows, appropriates, re-evaluates and manipulates to alter everyday objects, experiences and rules. Jams are about groups of people coming together to use a design based approach to problem solving employing creativity and innovation to address specific challenges. These hackJams then will bring together the re-appropriation of ***existing identity management scenarios*** with the creativity and dynamism of jamming to generate fresh and innovative responses to future identity management practices. We think these hackJams are ideal for level 5 and postgraduate students exposing them to a live international research project and providing them with an opportunity to take part in the very real cultural phenomenon of hacking and jamming.

One notable insight from this process was the importance of natural gestures. For example, it was suggested that shaking hands could be one way to communicate identity, especially if such hands would exchange information, through, for instance, smart ink or smart dust.

IMPRINTS has also deployed an **Identity Kiosk** at a number of public events, to help gather public attitudes to IM with the help of video games and interactive exhibits. A number of interesting insights derived from this:

- people were reluctant to touch the finger-print pad that was exhibited, despite being reassured that it was ***not*** collecting any data; in fact, people grew more reluctant to place a finger on this inert system after they had been told that this was a way that information could be collected;
- there was both a generational and a cultural difference in attitudes to ***"chipping"*** (i.e. having an identity chip inserted under the skin):
  - younger people are interested but the older generation is resistant;
  - the USA is more accepting of the idea than the UK.

The research found that there were three key issues in the design process, with a major conclusion being the need for IM to **focus on, and be responsive to, the individual**.

1. personal expression - for example, scarves, reflecting persona taste, carrying identity data;
2. mass personalisation - common identity tokens can be personalized, as is currently possible with a cover for your Oyster card, or a personal image on your bank card; ***Dundee has designed jewellery that can contain chips with medical information;***
3. Importance of the narrative - we like to be recognised on the basis of our life stories (e.g. personal security questions like the name of our first pet, or the street where we grew) rather than in terms of our PIN; such narratives are slowly becoming a part of IM systems.

Design Outcomes

A range of IM ideas was presented, including:

- **The Ping Garment** - this hooded jumper incorporates a link to the owner's Facebook: it can be programmed to update their Facebook status (e.g. registering that I'm going out when I put the hood up).

- **Nymi** - this company manufactures a bracelet that recognises the wearer's heartbeat, confirming his or her identity which is then transmitted as a signal - acting as a password to a number of devices.

- **Sixth Sense** - a necklace, which is both a camera and projector - the camera uses face recognition to identify the person in front of the wearer and this data can then be projected on to them.

- **Gun fire recognition** - a microphone located in a public place picks up gun-fire and identifies where the noise came from: this directs a camera towards a specific location, using face recognition tools to try to identify the assailant (sending these details to the police).

- **Smart wear** - a form of identification which includes GPS and heart rate data (something that could be used by armed forces when deployed in battle).

- **QR Coded Scarves** - where a fashion item has incorporated into its design a QR (Quick Response) Code, with a unique set of dark dots arranged, against a light background, within a square box, acting as an identity token.

In discussion, the question of resistance to IM was raised. Activism has not emerged in formal protest yet, but an online video was shown, which provides guidance on how to avoid facial recognition systems.

Session B: Diversity Issues in IM

Led by: Pam Briggs (IMPRINTS)

In the session Diversity Issues in IM, participants explored the issue that IM has a number of stakeholders including government and industry but the users are often forgotten when it comes to policy making and creation of new technologies.

Certain groups of users can be marginalised in the design process and so this research focussed on the design of universally acceptable identity technologies. The reported research described a series of focus groups and workshops with various community groups including:

- People with mental health illness;
- People with disability;
- Older people;
- Refugees;
- Teenagers.

It was difficult for many participants in these sessions to envisage what the future would be like - their references often tended to be fictional (especially films). Nevertheless, this process led IMPRINTS to identify a number of important principles - even necessary conditions - for successful IM. These are listed in the Table below, framed against issues of **Legitimacy**, **Competence**, and **Choice.**

Legitimacy	Data segregation	Adopt a principle of proportionality and only store data that is essential for the service or organisation. Establish clear lines of accountability for data use.
	Data Integrity	Implement good data checking procedures. Where viable, provide a mechanism for people to update their personal data.
	Data Access	Ensure a clear data access policy and procedure. Provide information about who has access to personal information, and about why, when and how the data will be used.
Competence	Trust	Consider trust in both the technologies and the people involved in designing and modifying the service. Establish an audit procedure to minimise potential for data loss.
	Reliability	Consider post-implementation issues around everyday use and issues of scale. Who takes responsibility for effective service delivery? Who is accountable for failure?
	Security	Provide transparency about system vulnerabilities - make people aware of risks and what could happen in the event of an online attack.
	Safety	Consider human vulnerabilities and physical hazards - make any health risks transparent.
Choice	Inclusion	Consider legal and governance frameworks to protect individuals - offer alternative solutions and informed consent. Have awareness of new social norms and recognise actual rather than idealised use of systems in the real world.
	Exclusion	There may be a range of barriers to technology use - physical, financial, psychological - design to maximise accessibility for all. The provision of alternatives will encourage more widespread adoption.

Session C: Cultural Issues in IM

Led by Liesbet van Zoonen (IMPRINTS)

In this session, a 10-minute video was shown, with excerpts from film and television. All excerpts were representations of past, present and future forms of IM e.g. story-telling, passports or implants.

It was shown how these narratives provided a ***"horizon of imagination"*** against which people think about future IM developments. It was particularly noteworthy that in each of the excerpts analysed, identity technologies are used to **control** the individual - ***there was not one positive message about IM - it was always a threat.***

Professor van Zoonen also showed that popular culture and sci-fi draw on a small number of **classic themes** about identity, especially fears about of **identity fraud** and **identity confusion,** raising much bigger questions about our humanity and identity. For example, where IM

technology interfaces with our body, this raises the question ***what makes us human?*** How could this technology affect the way that humans are perceived?

The key message for policy-makers, designers and companies working with IM is that this well-established cultural heritage or context needs to be taken into account: it affects the environment within which new IM developments will be received: they could produce tensions and tap into deeply-felt existential fears.

In discussion, it was noted that there are indeed historical British attitudes to idea of the state controlling the individual; the only time this had been tolerated was in times of emergency or war. In Germany, resistance to adopting IM technologies has come predominantly from **East** Germans, with their recent unhappy history of intrusive state control.

The breakout session considered whether there were any positive messages about IM technologies in popular culture. It came to the conclusion that the more likely place to find positive messages was in art, design and corporate scenarios of future technologies. It was recognised that a particular cultural framing of a new IM technology could influence its acceptance: a distinction was made between the different discourses between the use of new technologies in the UK and US (for security purposes) and in the EU (for service purposes), with the latter seemingly leading to more acceptance among the public.

Session D: Biometrics and IM

Led by: Professor Aletta Norval and Dr Elpida Prasopoulou at University of Essex (IMPRINTS)

There is a growing number of biometric applications in IM, and these are being used in a wider range of settings.

Over the last decade we have witnessed a shift from a situation in which biometrics are primarily used in a security context (such as finger printing at border control posts), to one where fingerprints and retina scans are incorporated into personal devices. For example, face recognition is now extensively used in on-line social networks; and new forms of biometrics, such as the analysis of one's gait or brain waves are being introduced in consumer electronics, ranging from headbands to fitness products to enhance the customer experience by tracing their mood. Many of these technologies are being diffused into everyday life. However, significant concerns about security, privacy, identity and citizenship remain.

Professor Norval and Dr Prasopoulou have focused their research on public understandings of biometrics. In contrast to user research conducted by industry, which tend to focus narrowly on the usage of particular technologies, this IMPRINTS explores how students (lay experts) understand biometrics and how they see what is generally considered to be a zero-sum trade-off between privacy and security.

Current work in government and industry assumes that the diffusion of biometrics to wider areas of everyday life is a positive process, where the context in which the biometric is employed does not change perceptions of biometrics. Government reports assume that once citizens are accustomed to their uses, they will adopt biometrics in everyday-life contexts. However, academia and civil society are highly critical of this diffusion, raising concerns over surveillance, privacy and citizenship.

This suggests to the IMPRINTS team that a different approach to the spread of biometrics is required. They start from the assumption that the ***framing*** of biometrics - how it is given its meaning - matters; we need to understand how it is presented and understood by both the government and industry, since this affects public understandings.

These framings set limits to what can be said and done through and with biometrics, shaping both forms of governance and the possibilities of public contestation. To understand this, Professor Norval and Dr Prasopoulou analysed the contexts in which biometrics emerged, and the arguments that were made for its increased use. Governments were interested in security and control in a post 9/11 era, in facilitating economic growth and ease of movement and in contributing to e-government. Industry, by contrast, was interested in technological advances to securing identity, protecting personal data and safeguarding society.

The Q-method was used to capture public understandings of biometrics. The overarching question informing this study concerned the uses of biometrics in everyday life. The respondents were asked to sort a set of 50 statements according to whether they agreed or disagreed with them, and to justify their choice where they strongly agreed or disagreed with statements. They conducted an online study with students (lay experts), which included students from the UK, the EU and further afield.

The ranked statements were sourced from government and civil society reports, academic articles and specialised press. The core themes identified included:

- Identity;
- Empowerment;
- Surveillance;
- Accountability;
- Security.

The findings produced four distinctive viewpoints, which have been entitled:

- Privacy Advocates;
- Conservative Techies;
- Safety Champions;
- Casual Adopters.

All four groups clearly agreed with one statement, namely, that ***'In the wrong hands biometrics have the potential to violate privacy'***. Despite this agreement on the importance of privacy, distinctive viewpoints emerged that resulted from different valuations of the other core themes.

Privacy Advocates are concerned about the development and spread of new biometric technologies. They see biometrics as a powerful instrument in the hands of governments and corporations. They are particularly concerned about issues of data linkage, user control over data (when, where and by whom it was used) and consent (effects of the technologies on existing everyday practices.

Conservative Techies are cautious users. In contrast to ***Privacy Advocates*** they are positive about government uses of biometrics even though they are still concerned about privacy and

possibility of data leakage (for example, with regard to medical information). However, they are happy for biometric technologies to be used on condition the data is well protected. They are also positive about the use of biometrics for personnel management, for example hand geometry or fingerprinting to be used for capturing labour data. Again in contrast to Privacy Advocates, they are not supportive of the use of ***souveillance*** (surveillance from below) such as in the case of the use of smartphones to record police action.

Safety Champions, the third group, share similar concerns to ***Privacy Advocates***. They are preoccupied with the possibility of data linkage and the use of their biometric data for unrelated purposes. However they are quite favourable to the use of biometrics for border control and security purposes. They are also against surveillance and they tend to advocate an active form of citizenship to counter the need for surveillance. This group differentiates between the types of biometrics they were happy with - iris scanning was alright but fingerprint recognition less so because of its criminal associations. ***Safety Champions*** favour the use of biometrics for domestic uses and this is the only group that is not negative about the use of biometrics in online social media.

Finally, **Casual Adopters** have an instrumental view of biometrics, treating it as a technical solution to a variety of problems ranging from the difficulties of remembering multiple passwords to overcoming fraud and aiding immigration control. They express trust in existing technological solutions for biometrics and they also see certain biometrics, such as face recognition, as useful gadgets that are enjoyable to use.

It was concluded that different understanding of the role of digital identity in everyday life lead to different responses on the use of biometrics in various contexts. Each viewpoint had a unique understanding of privacy which also influenced their acceptance of biometrics and the contexts of use.

Closing Plenary Session

Chair: Professor Aletta Norval

Panel: Dr Tristram Riley-Smith and Isabelle Moeller

The final plenary session received feedback from the four breakout events, and there was an open-floor discussion about the policy implications of the IMPRINTS research. Set out on the following page in bullet-point form are the key messages and insights that emerged from this session.

There is one powerful and important message deriving from the IMPRINTS research and reinforced by this Policy Seminar:

The future use of IM technologies have substantial policy implications; Government and Industry need to take into account the user when formulating policy and creating the technology.

One size does not fit all with all IM technologies and processes, the human element must be taken into account.

- there are sometimes surprising levels of diversity, not only between different groups but also within specific: groups *it was surprising, for instance, that teenagers are not as enthusiastic as thought about some of the future IM technologies*;
- we possess multiple identities (represented not only by our biology and ethnicity but also by our membership of family, occupational, religious, political, and leisure-based communities;
- there are disadvantaged minorities (the disabled, the poor, the old and infirm) whose needs must be taken into account when designing and delivering IM services;
- it is important to recognise that in the "real world", we share our possessions and even - at times - our identities:
    - it is not uncommon for us to pass bank card and PIN to a trusted family members to get money from an ATM (e.g. when we are ill or busy);
    - if a fingerprint is used to access smart phones or tablets, it prevents us sharing usage.
- those involved in designing new IM technologies and systems should aim for mass personalisation rather than mass production: adapting solutions to accommodate individual differences, expectations, and needs.

The relationship between identity and personal data is a subject of real concern:

- citizens' views on biometrics centre on the question of privacy, given the very personal nature of biometric IM;
- the public seek reassurance on so-called "hygiene factors", relating to such issues as:
    - Data segregation;
    - Data integrity;
    - Competence;
    - Personalisation;
    - Use of the body for access authentication.

Given the strength of negative fictional narratives about IM, increased prominence needs to be given to a positive narrative around the use of such technologies.

- for example, in Australia after recent bush fires had destroyed homes and businesses, biometrics enabled people in affected communities to resume their way of life rapidly, as IM technology enabled them to prove who they were and then access the help they required.