IDENTITY

TALK IN THE TOWER®

The Future of Identity

Innovative and user-centric identity management –
Building trust and confidence

Publication Task Force 2

TABLE OF CONTENTS

PREFACE

Identity – Talk in the Tower

IDENTITY – Talk in the Tower®[1] is the platform for open, ongoing, and cross-border discussion on the future of identity. Launched at the Tower Lounge in Berlin, Germany, in May 2012 – a location chosen because its panoramic views highlight the need for fresh perspectives – the platform is designed to encourage creative thinking around identity issues in our fast-changing digital age.

As new technologies shape ever more complex information ecosystems, public interest in and concern about the impact on identity deepens. What actually determines identity in the digital era? How can people control and protect their identities? Who sets the rules for data privacy, anonymity, and transparency in a networked world? How can identity management drive innovation? Such questions are proliferating, and by bringing together a wide range of experts – academic, commercial, and technical – the platform is helping to stimulate an interdisciplinary exchange of out-of-the-box ideas about how to answer them.

Philosophers, lawyers, and social scientists are sharing their thoughts on new concepts, projects, and technical approaches with business leaders, IT specialists, and entrepreneurs. Moreover, the collective knowledge and insights of these leading decision-makers is helping to form a bridge between practical and abstract thinking. The discussion aims to gain a clearer understanding of what is happening to our identities, now and in the future, as well as to come up with concrete proposals for technological innovation. It seeks, in addition, to identify the legal requirements and political actions that will enhance security, to fill in knowledge gaps, and to define the areas where different stakeholders can profit from sharing ideas.

In working groups known as Tower Task Forces, expert participants break the potentially vast subject of identity into its constituent aspects, investigating in greater detail topics and issues previously identified by respected leaders and thinkers in so-called Tower Talks.

This report represents the work of one such Task Force, which has examined the Control of Identity, with a focus on how innovative, user-centered identity management can help. The report does not pretend to offer a scientific analysis of this important topic, but rather to provide insights and ideas around identity management that will form a basis for further discussion in subsequent Tower Talks, and with a wider public.

Giesecke & Devrient's engagement

As suppliers of end-to-end security solutions for both businesses and governments, identity and its protection are at the core of our business. Indeed, thanks to the technologies we produce, we are on the leading edge of the transformation that is driving interest in identity. Together with nationality, gender, culture, and the social environment, modern technologies are playing an

[1] *For further information, please visit our website https://www.identity-tower.com/*

increasingly critical role in shaping personal identity. At the same time, identity itself is becoming more and more important as a facilitator of modern life. Identities help enable financial transactions, for example. They also describe and define user attributes in social networks and administrative processes. And you can't travel far — on the Internet, or physically – without them.

Founded more than 160 years ago as a producer of banknotes, G&D now also supplies travel documents, ID systems, and health-care cards to governments worldwide, as well as providing banks, mobile network operators, original equipment manufacturers, and others with mobile security applications, especially for telecommunications and electronic payments.

These systems, by definition, need to be secure. Which is why trust, security, and competence have been our watchwords ever since our foundation. We apply our many years of experience to develop system solutions for security technologies, thus offering individual freedom and mobility across both national and virtual borders.

At the same time, we consider ourselves responsible for providing answers to important social questions. We are committed to taking responsibility for our actions and their impact on society. In fact, we are hard-wired for Corporate Social Responsibility (CSR), in all its aspects.

We believe that responsibility requires dialog; that dialog, indeed, inspires confidence – hence our ongoing discussions with a variety of external stakeholders. We launched the IDENTITY – Talk in the Tower initiative as part of our CSR program, drawing in external experts to further an interdisciplinary and international discussion around identity: the impact of technology, the norms and values that influence identity, and the key issues of its regulation and control.

Identity, in short, is a topic of increasingly critical importance to us, to our customers, and to the wider public. We are pleased that we can contribute to this crucial discussion as the initiator of IDENTITY – Talk in the Tower.

Participants

After the inaugural meeting of IDENTITY – Talk in the Tower, which took place in Berlin in May 2012, two Task Forces were established in September 2012. Task Force 1 is focused on the role of machines and technological change in forging new concepts of identity. Task Force 2 is focused on the control of identity and identity management.

Meanwhile, in September 2013, we started a third Task Force to focus on the risks and opportunities of Big Data. This report represents the results of Task Force 2's deliberations to date.

A comprehensive discussion of identity requires an interdisciplinary approach. This is why the Task Force participants represent such a broad range of professional interests – including

lawyers, social scientists, IT and communications specialists, and regulators. In order to ensure a truly international perspective, we also applied regional criteria to their selection, though European views predominate.

Each Task Force participant is an expert in his or her particular field, with unique perspectives on the control and management of identity. For detailed profiles of the participants, please see page 59.

EXECUTIVE SUMMARY

This report seeks to explore developments in the control of identity – how users can profit from or confront the challenges of identity management innovations, as well as (crucially) how public trust and confidence in them can be secured.

It begins by endeavoring to define identity in the context of the digital age. Digitalization has transformed our social relationships and thus, of course, our identities. Indeed, we now have multiple identities, depending on the multiple contexts in which we operate.

Acknowledging that individuals need to be empowered to take better control of their identities, the report discusses how innovations in identity management perform in that regard. It examines the concept of identity management, describing the principal players – public institutions and private companies, as well as the end user whose perspective is in the focus of this publication – and exploring (by reference to publicly available studies and surveys) the widely differing attitudes to online privacy and data management across geographies and cultures.

The core of the report is an investigation of four use cases, chosen by our Task Force participants, each of which reflects different cultural contexts for identity management innovation.

The palm vein authentication technology used by the authorities administering the Graduate Management Admissions Test (GMAT®) in the US provides an example of biometric identification. The program of the Unique ID Authority of India (UIDAI) offers a case study of a large-scale national electronic ID system. The UK Identity Assurance Programme (IDAP) illustrates a federated approach to identity management. And the example of eVoting on the mobile phone (not yet in use anywhere) explores the logical consequences of trends toward eGovernment and eAdministration.

In the second part of the report, our Task Force participants discuss the implications of the use cases from philosophical and social, legal, and technological perspectives.

They offer no hard and fast conclusions or specific recommendations, but seek rather to analyze the aims and likely outcomes of these initiatives to manage identity, both positive and negative. We hope that the diversity of views expressed will make a significant contribution to the ongoing public debate.

INTRODUCTION 1.

Focus: Identity 1.1

Identity is, of course, a broad concept. It has cultural, religious, biological, occupational, and gender aspects, among many others. Different academic disciplines use the term to describe different phenomena, depending on their specific area of interest. For psychologists, for example, "identity" usually describes personal identity, or the things that make a person unique, whereas sociologists often employ the term to describe social identity, or the various group memberships that define each individual. Digitalization has had a dramatic effect on both identification and authentication thanks to the multitude of identification methods and media that digital technologies have spawned – user name and password, biometrics, mobile devices, and social networks.

Most technical descriptions of identity, that of the International Organization for Standardization (ISO)[2], for example, use the categories "what you have" (ID card), "what you know" (password), and "what you are" (biometric, such as fingerprints). These categories help you to identify and authenticate yourself. The European IT Security Standard EN 14890 describes **"identification" as "the unique association of a set of descriptive parameters to an individuum within a given context." The same standard defines "authentication" as the "verification that an entity is the claimed one" or – as defined by the ISO – the "provision of assurance in the claimed identity of an entity."**[3]

Rather than address what might be called the "softer" aspects of the digital revolution's impact on identity – how our religious beliefs or family background influence the identities we assume, for example – this report focuses on the control of identity in the context of identification and authentication. The report seeks, above all, to understand how identity can be managed in the interests of the end user. However, in order to understand the user's needs and behavior, the first part of the publication will also include recent surveys on individuals' online behavior and their thoughts about private and purely descriptive information – information posted by an individual on a social network, for example.

Focus: The Private End User 1.2

The private end user — the individual citizen or consumer — is the report's principal concern. It recognizes, however, that other players — public institutions such as health-care providers and tax authorities, as well as private companies such as Internet service providers — are key to identity management in the digital age.

The report cites a wide range of metrics and research around relevant social trends and patterns, but because the data is so heterogeneous, the authors do not claim that it presents a definite and comprehensive picture.

---

[2] *ISO/IEC 24760-1:2011*

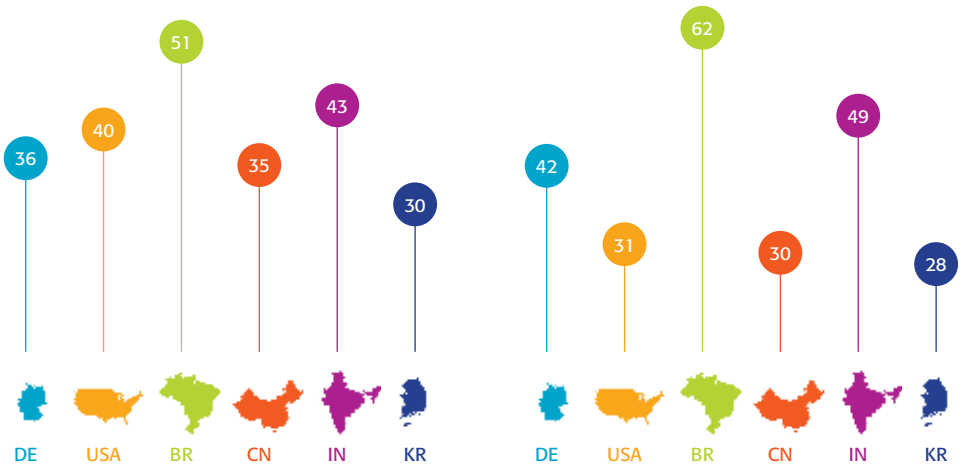
[3] *ISO/IEC 18014-2, IT Security Standard*

End User

1.2.1

As online interactions increasingly integrate with our everyday lives, we are using the Internet for a growing number of activities. From shopping and reading to banking and paying bills, from booking tickets to chatting with friends, more and more of what we do takes place online. And naturally enough, we expect the same levels of service in this virtual world as we require in the real one: simplicity of access and ease of use, and, of course, security. Protecting our privacy – our claim to determine for ourselves when, how, and to what extent information about us is communicated to others – is also of paramount concern.

The establishment of trust between end user and service provider is fundamental in this context. Yet despite the creation of a global Internet culture, whose users seem to share many of the same perspectives on new technologies[4], when it comes to the key components of trust – privacy and security – there remain significant differences across geographies and cultures *(see **Fig. 1**)*.



Source: Future Study MÜNCHENER KREIS 2013

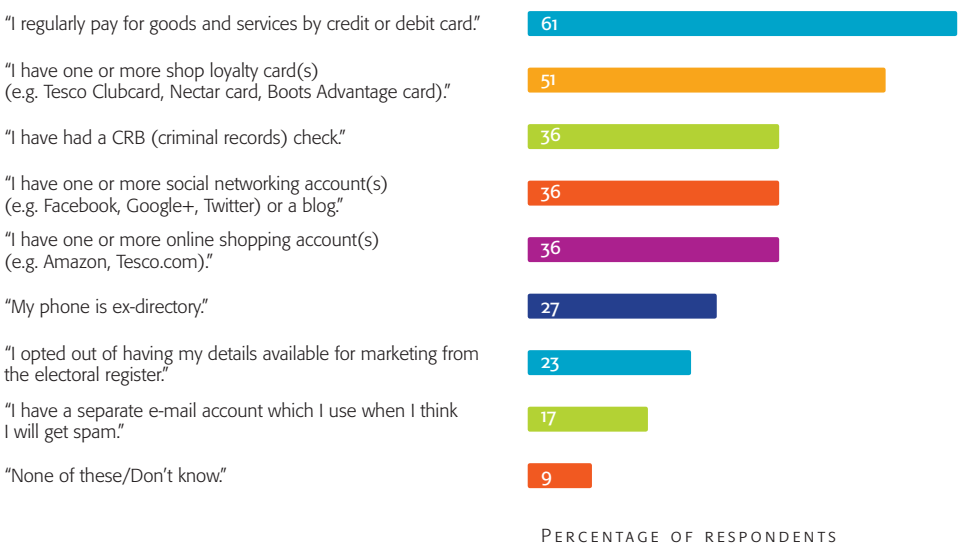
Fig. 1
Privacy and Security: A Diversity of Views
More than half of Brazilians minimize the amount of personal data they put online and a sizeable majority requires transparency about its use. In South Korea, by contrast, people are significantly more relaxed.

With the exception of Brazil, for example, whose citizens seem exceptionally sensitive to Internet disclosure, most non-Europeans (including US citizens) appear remarkably unconcerned about how much of their personal data goes online and how it gets used.

[4] *http://www3.weforum.org/docs/WEF_GITR_TheNewInternetWorld_Report_2011.pdf*

Meanwhile, our digital footprint (everything that is on the Internet about us) continues to grow – thanks largely to our penchant for shopping *(see **Fig. 2**)*. Whatever the reason for surfing the Internet may be (research, chat, or commerce), the action reveals a lot about our personal identity – even if the data we willingly surrender is not always considered "personal" *(see **Fig. 3**)*.

DIGITAL FOOTPRINTS CREATED BY TODAY'S CONSUMERS



Source: Deloitte. Data nation 2012: Our Lives in Data

Fig. 2
Revealing our Identity
A majority of consumers in the UK leave tracks via their credit, debit, or loyalty cards. Online shopping accounts and social networks are also significant markers.

Europeans, for example, don't consider data about their careers, friends, or attitudes to be anything like as personal as financial, medical, passport, or fingerprint data. And a similar pattern emerges when US citizens and the citizens of India are included *(see **Fig. 4**)*.

To be sure, the global data show that people also want to retain control over less obviously security-sensitive data – family photos and videos, for example – and that they don't want information about their salary to pass into unknown hands. Yet even such relatively "harmless" data can be linked in the digital world to reveal a user's identity (though most people don't realize it). Furthermore, the metrics reveal a contradiction between people's willingness to reveal their identity via social networks *(as shown in **Fig. 2**)* and their desire to retain control over the family-related data that they display on such networks *(as shown in **Fig. 4**)*.

In general, end users expect the service providers to whom they entrust their data to manipulate it only in the user's interest. However, country-specific insights show that the degree of trust in those service providers varies across cultures *(see **Fig. 5**)*.

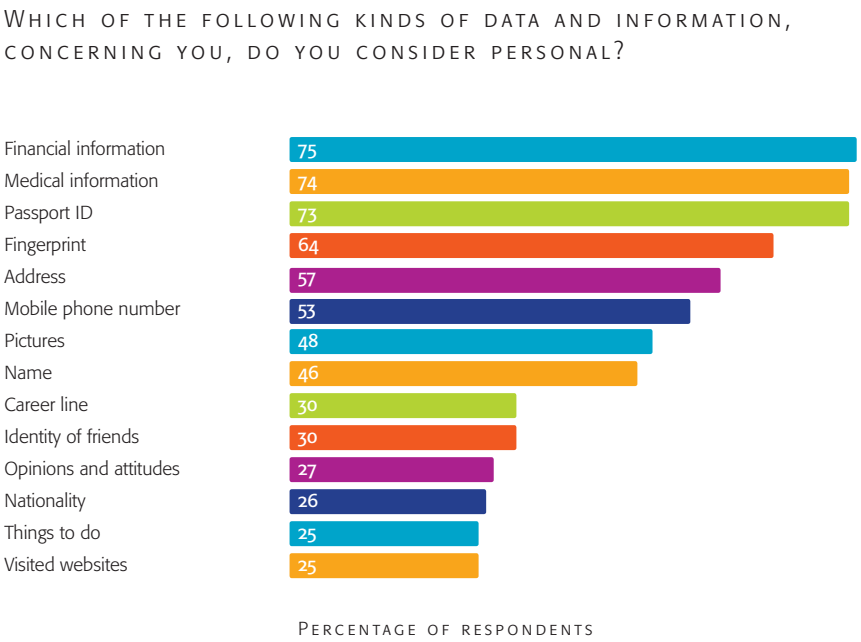


Fig. 3
Defining the Personal: Europe
Europeans consider financial, medical, and passport data highly personal. They are less concerned about revealing their opinions, behaviors, and nationalities.

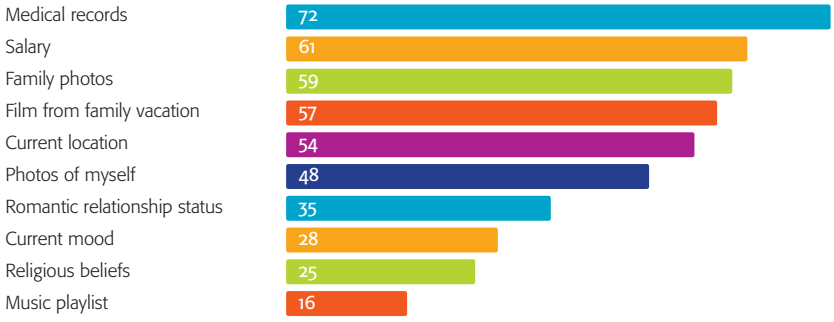
Americans, for example, have significantly less confidence in government than people elsewhere. In fact, just 46 percent of US citizens believe that public authorities can be trusted to handle their data responsibly – strikingly fewer than the three quarters of Chinese citizens or 69 percent of Germans who confirm their confidence in the state.

By contrast, more than half of US citizens seem happy to entrust their personal data online to banks, and almost as many have confidence in the online ordering services that rank rather low on trustworthiness in other countries. Americans are concerned, however, about identity theft – especially when it might entail negative financial consequences *(see **Fig. 6**)*.

And with good reason: according to one recent survey, thanks to dramatic jumps in the two most severe types of fraud (New Account Fraud and Account Takeover Fraud), the incidence of identity fraud increased in 2012 for the second consecutive year, affecting 5.26 percent of American adults[5].

[5] *2012 Identity Fraud Survey Report; Javelin Strategy & Research (www.javelinstrategy.com), February 2013*

WHAT WOULD YOU BE CONCERNED ABOUT SHARING ONLINE IF YOU HAD NO CONTROL OVER WHO COULD SEE IT?



PERCENTAGE OF RESPONDENTS

BASE | 3,818 Internet users in US, UK, Germany, Sweden, and India

Source: 2012 Consumer Privacy in an Online World (Ericsson)

Fig. 4
Defining the Personal: Global
Almost three quarters of global respondents worry about sharing medical data when they cannot control who sees it. But they are quite happy to reveal their religious beliefs.

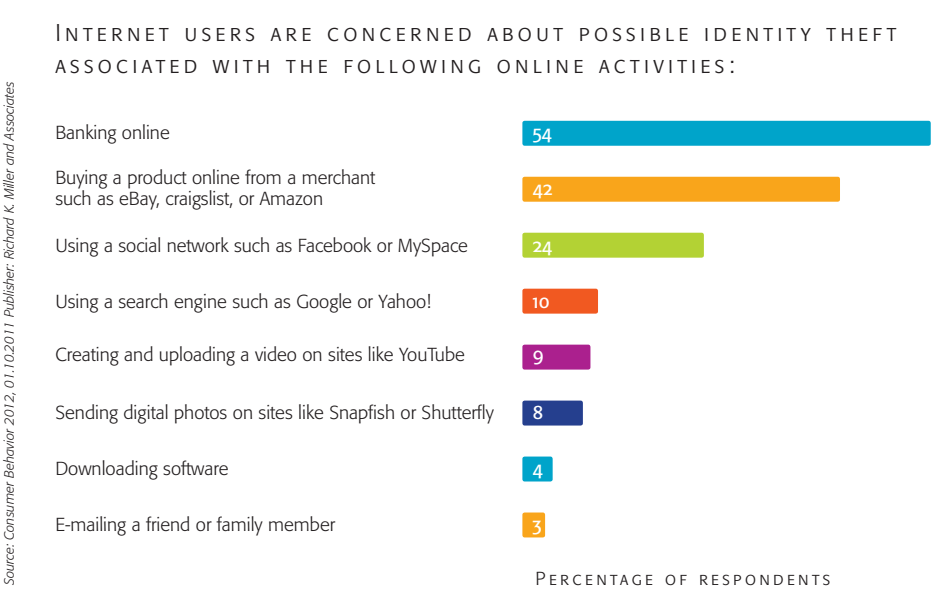
WHICH OF THE SERVICES THAT PROCESS YOUR PERSONAL DATA DO YOU HAVE CONFIDENCE IN AND BELIEVE THEY HANDLE YOUR DATA RESPONSIBLY?

%	Germany	Brazil	India	USA	China	South Korea
Government processing	69	52	59	46	75	69
Customer card programs	16	23	36	23	21	16
Social networks	9	17	37	16	21	9
Online banking	56	34	49	51	62	56
Ordering online	30	22	21	41	29	30
None of them	13	9	3	16	3	13

BASE | 18–34 years: n=715 | 35–49 years: n=613 | 50+ years: n=486 | multiple answers possible

Source: Future Study MÜNCHNER KREIS 2013

Fig. 5
A Question of Confidence
Public institutions are more trusted than commercial entities in five out of six countries. Only US citizens trust their banks more than their government to handle personal data responsibly.



Source: Consumer Behavior 2012, 01.10.2011 Publisher: Richard K. Miller and Associates

Fig. 6
Online Identity Fraud
Americans are most concerned about the impact of identity theft on their pocketbooks. The threat to personal reputation concerns them less.

Government, Public Authorities **1.2.2**

As stated above, the principal focus of this report is on the control of identity for individual end users. However, since the state and its subordinate administrative units offer services required by law, and in many countries these services are no longer paper-based but administered online, the security of such services is critical to the establishment of end user trust. The state, in short, needs to offer online authentication systems that citizens can rely on. Such systems are not only relevant for legal and income tax processes and certifications, but also for passports and other official documents. Most states have introduced machine-readable or biometric passports compliant with standards established by the International Civil Aviation Organization (ICAO). These documents help make travel faster and easier. But governments must also ensure that the authenticity and integrity of the personal data they contain can be guaranteed. The same is true of ID cards and related documents. In many countries – particularly those in the less-developed world – electronic identification systems are enabling such modern governance structures as voters' registries and access to public welfare services.

Private Companies **1.2.3**

Similarly, as identity providers, private companies play a key role. However, in contrast to government systems, those deployed by commercial providers are market-driven. The security measures used are chosen because of their economic viability.

Security and authentication measures vary widely: from the banking sector and services, which are linked to payments and have high security standards equal to those used in government services, to social media platforms with simple password authentication.

Central authentication systems for the commercial provider's own services, and where systems security is monitored in compliance with its own standards, are widely established. Moreover, decentralized authentication, which merges information about the user from a variety of other services, is being developed. But both types of identity management are designed from the service provider's perspective – not that of the user. In order to make online service provision scalable for all, there is clearly a need for a user-centric approach to identity management[6].

"Control of Identity": The Need for Innovation 1.3

Individuals clearly need to be empowered to take better control of their identity – to know what is happening to their personal data, and to have the means to handle their identity securely off-line and online.

The management of credentials for identity ownership is an essential aspect of identity management. Right now, as we accumulate more and more identities in diverse contexts, and interact with a growing number of remote identities[7], the management of the names and credentials for these identities simply does not scale.

Indeed, some of us feel we are suffering from "identity overload." In some circumstances, "pseudonymity" and "anonymity" may help (see box). But there is clearly a need for further innovative solutions that respect the different contexts in which individuals are confronted with identity management issues.

In this report, which represents the results of the Task Force's work to date, four use cases reflecting different cultural contexts will be under review for innovative identity management. Some are already available in a few jurisdictions but lack wider implementation; some are about to be introduced; and some are future scenarios.

The report first provides detailed descriptions of each of these four use cases, before our Task Force members contribute to an interdisciplinary assessment of them.

Pseudonymity and Anonymity
Pseudonymity allows a user access to a resource or service without disclosing his or her user identity. In contrast to anonymity, which removes the association between an identifying data set and the data subject so that data once linked to an individual can no longer be related to that person, the user creates an ambiguous parameter – the pseudonym (a fantasy name, for example) – that doesn't directly identify them but can be used for dedicated communication purposes; in a chat room or forum, for example.

---

[6] *See also Audun Jøsang http://folk.uio.no/josang/im/*

[7] *A remote identity are the credentials of a user stored by a remote located device. Remote eVoting, for instance, refers to voting through the Internet, a web-based service, applications, or even mobile devices such as smartphones or eIDs. Please see chapter 2.4 for further details*

THE USE CASES

2.

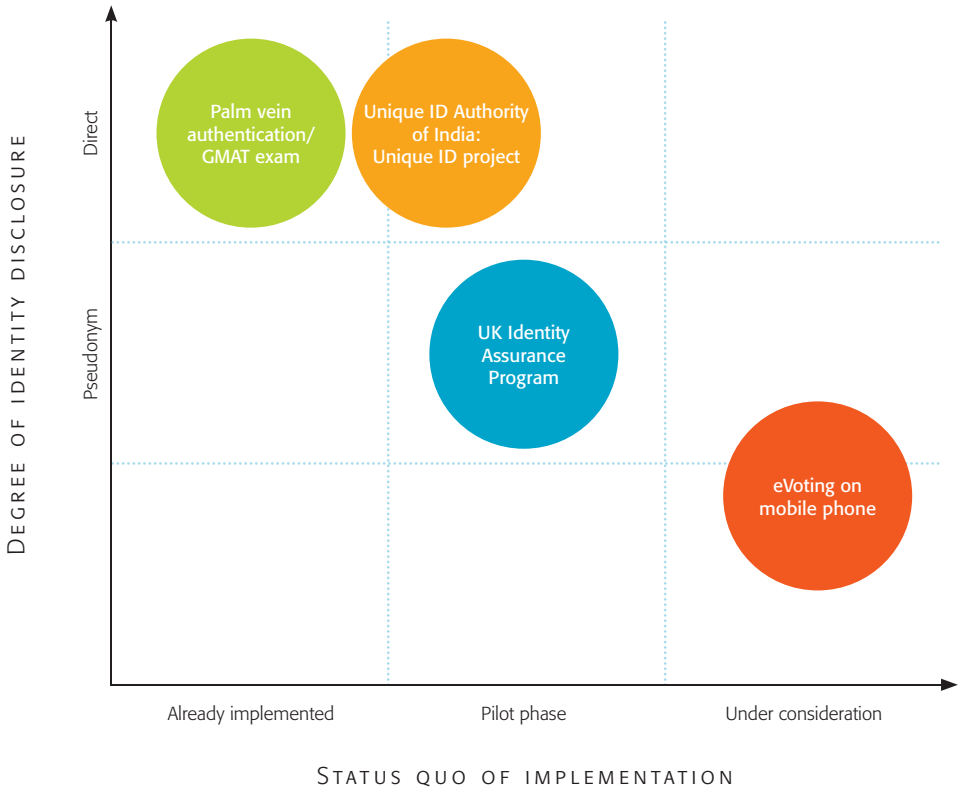


Fig. 7
Four Use Cases: Four Identity Management Systems
The x-axis shows the progress of implementation (already implemented; in pilot phase; or under consideration).
The y-axis shows the extent of identity disclosure (anonymity, where there is no association between the data set and data subject; pseudonymity, where an ambiguous parameter is created that doesn't directly identify the user; or direct identification where identity is authenticated one to one).

Fig. 7 describes four different use cases that reflect four possible identity management systems:

- Palm vein authentication: an example of biometrics, in use in the US in the Graduate Management Admissions Test (GMAT) examination
- The Program of the Unique ID Authority of India: an example of a unique identifier
- The UK Identity Assurance Program: an example of federated identity across accounts
- Mobile eVoting: an example of a key government service going mobile

These four use cases do not, of course, represent the full scope of existing systems; nor do they claim to give a comprehensive picture. Our international expert group chose them as representative examples of the diversity of identity system development globally, and because they have potentially wide applicability.

Palm vein identification, for example, has had a rather small proportion of the biometrics ID market *(see **Fig. 9***, below, which shows data from 2009). But since it offers an especially secure means of identification – palm vein patterns are invisible and virtually impossible to forge – and is sometimes felt to be less intrusive than, say, fingerprinting, it is catching on fast.

Similarly, the electronic registration of citizens (exemplified here in India) is on the rise. Users' desire for convenience and their struggle to manage different online identities are reflected in the UK use case. Participating in parliamentary elections by using only a mobile phone, though not yet in use anywhere[8], is becoming an increasingly realistic option as its convenience becomes clearer.

Palm Vein Authentication/GMAT Exam: Biometric Authentication in Everyday Life **2.1**

Specific to each individual user, biometric identity cannot be easily passed on to others. Moreover, it requires special technologies, which match a distribution of the data collected to specific checkpoints, for verification purposes.

Biometric recognition methods can be either biological/physiological or behavioral (*see **Fig. 8***).

Most such systems remain, in general, too expensive for mass-market use – with some exceptions. Biometric authentication is common, for example, in the identification of company employees, and in some countries in banking: in Japan and Brazil, for example, some bank tellers use palm vein authentication. By the end of 2011, indeed, 25 percent of ATMs in Japan were equipped with finger vein technology; and in Brazil around 11 percent of ATMs had converted to palm vein biometrics.

The biometrics industry is putting more biometric authentication methods into commercial use (*see **Fig. 9***).

Systems using behavioral characteristics require complex technologies, though as they become easier to use, they are likely to become more common. In any event, people appear to be increasingly open to the application of biometric authentication. A majority of Europeans expressed support for the use of biometrics in criminal identification and for ID documents and passports in one recent survey, though slightly less than half were in favor of such technologies replacing PIN numbers for bankcards[9].

---

[8] *In the 2011 [Estonian] parliamentary elections it was possible to use a mobile phone to identify oneself for eVoting. Because one doesn't need an ID card reader in the computer – a mobile phone with the respective SIM card acts as both card and card reader – this is especially convenient. However, the voting procedure still requires a computer. http://estonia.eu/about-estonia/economy-a-it/eVoting.html*

[9] *http://www.biometricupdate.com/201307/majority-of-europeans-support-biometrics-for-id-cards-or-passports-steria-survey/*

Overview of biometric recognition methods:

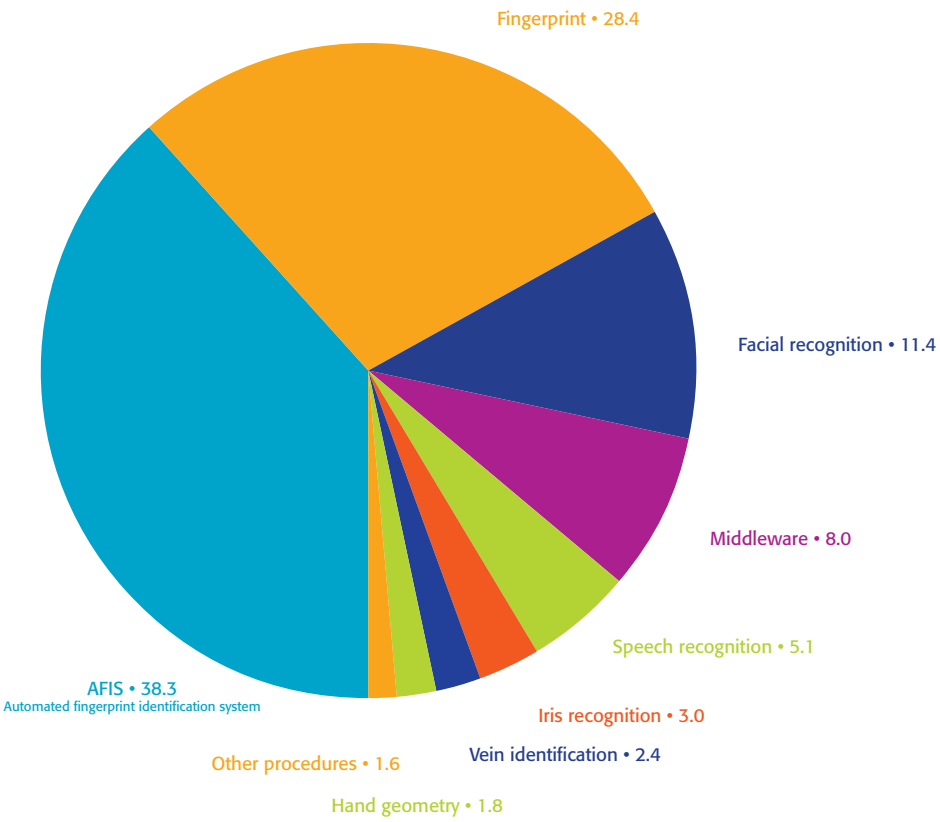
Biometrical identification	Characteristics	Representation of biometrical characteristics
Basis: Physical characteristics		
Finger image recognition	Pattern of epidermal ridges on the finger tip	Image of the finger lines, classification, special characteristics (minutiæ)
Hand recognition/ Vein identification	Dimensions and form of fingers and ball of hand as well as vein image	Length of fingers, hand profile, surface of hands and fingers
Facial recognition	Facial image and geometric characteristics	Transformational approach: covariance analysis of facial images; attribute approach: attributes like nose, eyes, etc. and their specific geometrical sizes and placement
Iris recognition	Pattern of the tissue around the pupil	Texture analysis
Retinal recognition	Pattern of the blood vessels in the central ocular fundus	Texture analysis of the circular scan of the retina/of the blood vessels behind the retina
Basis: Behavioral characteristics		
Voice recognition	Voice	Given text or independent solutions
Signature recognition	Writing habits	Speed, pressure, increasing speed of writing process
Keystroke recognition	Rhythm/speed of typing	Pressure time and intermediate times of pressing keys is measured
Optical speech recognition	Facial/body expressions	Analysis of motion sequences during the speaking of agreed texts

Original Source: Behrens, M. and Roth, R. (2001). Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven, DB Research • Source: 2012-04 Der vermessene Mensch (DB Research)

Fig. 8
Biometrics in Action
Anatomical characteristics are predominantly face, hand, and eye recognition. Behavioral characteristics include voice recognition, signature analysis and typing speed.

Our biometric use case focuses on palm vein authentication. While currently a small proportion of the overall market, its advantages from both a privacy and security perspective, as explained above, suggest that it is likely to become more widely used in the future.

DISTRIBUTION OF SALES IN THE BIOMETRICS INDUSTRY



PERCENTAGE SORTED BY TECHNOLOGY, 2009

Source: 2012–04 Der vermessene Mensch (DB Research) • Original Source: International Biometric Group

Fig. 9
The Biometrics Market
Data from 2009 show that systems using anatomical characteristics are in commercial use in various forms, and two in particular – Automated Fingerprint Identification Systems (AFIS) and authentication based on fingerprints – account for two thirds of the market. But with the exception of voice recognition, systems using behavioral characteristics are not yet widespread.

Use Case: The Graduate Management Admissions Test (GMAT) in the US

2.1.1

The Graduate Management Admissions Test (GMAT) is the most important test in the US for graduates seeking admission to the country's business schools. More than 1,500 universities and business schools currently use the test, and it is a criterion for admission in more than 5,000 programs worldwide. Administered by the General Management Admission Council (GMAC), an education corporation under New York State law, the GMAT has adopted palm vein authentication in all of its test centers as a secure means of ensuring the legitimacy of candidates. On arrival at the test center, each candidate has both palms scanned by a sensor that records the unique pattern formed by the palm veins.

The procedure, which requires the candidate to hold their palm several inches above the two-inch-square sensor for several seconds, is claimed to be relatively swift and simple. Because it cannot be copied, it is also said to be more accurate than a fingerprint. In addition, palm vein pattern readers use system-specific digital encryption, thus ensuring that the patterns cannot be used for identification purposes by anyone else in any other context. (In fact, because biometric data are considered especially sensitive, the recording of such data requires special protection under law; see Culture of Privacy box.)[10]

Culture of Privacy: Privacy of Design

Privacy by Design is a framework developed by Canada's Information and Privacy Commissioner, Dr. Ann Cavoukian. It advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation. In October 2012, Privacy by Design was recognized as the global privacy standard in a landmark resolution of the International Conference of Data Protection and Privacy Commissioners. The incorporation of Privacy by Design into privacy legislation will be a key issue in future debates around privacy and digital management. The proposed EU data protection legal framework, for example, has included the concept in Section 23.1. In the US, the Federal Trade Commission favors it.

- Does palm vein technology offer better protection against misuse of biometric data? Since palm veins do not leave traces on surfaces they carry less risk of "function creep," as Achim Klabunde points out, p. 51

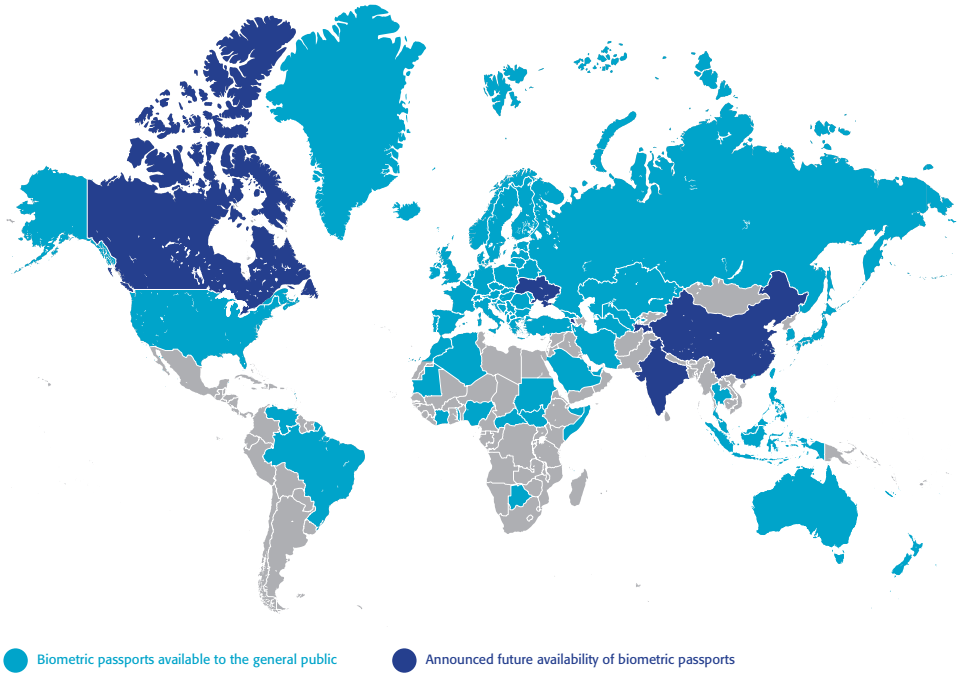
- Is biometric authentication really necessary for taking a test? Alessandro Mantelero argues that "the collection and processing of biometric data has to be adequate, relevant and not excessive," p. 35

[10] *See EU Proposal for a General Data Protection Regulation, Article 23. On Privacy by Design see also Peter Schaar, "Privacy by Design" (2010) 3(2) Identity in the Information Society 267-274; Ann Cavoukian, "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era' in GOM Yee (ed), "Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards' (IGI Global 2012) 170-208; Ann Cavoukian, "Privacy by Design: Leadership, Methods, and Results," in S Gutwirth and others (eds), "European Data Protection: Coming of Age" (Springer, 2013) 175-202*

Unique Identifier: Authority of India – Unique ID Project 2.2

The electronic recording of citizens, as well as the use of electronic identification documents, is on the rise worldwide. Indeed, according to the International Civil Aviation Organization (ICAO) 93 countries – almost half the membership of the United Nations – have issued ePassports, and 345 million citizens globally are using them (*see* ***Fig. 10***).

Distribution of sales in the biometrics industry



Source: Linköpings universitet: http://www.ida.liu.se/~TDDD17/lectures/slides/tddd17-auth3.pdf

Fig. 10
Biometric Passports – An (almost) Global Phenomenon
Most European citizens already carry biometric passports and many can use them to access government services. The rest of the world presents a rather mixed picture.

There are, to be sure, some parts of the globe where the authorities are not yet even planning to issue biometric passports. In Africa, for example, citizens in only a few out of the continent's 55 officially recognized states carry them. In South America, only Brazil and Venezuela have issued biometric passports. In Asia, too, there are several exceptions.

India, however, is advancing rapidly toward a national electronic ID system that, if successful, could provide a prototype for ID management programs worldwide.

Use Case: The Program of the Unique ID Authority of India (UIDAI) 2.2.1

The Unique ID Authority of India (UIDAI) was established in 2009 to help provide all of India's 1.2 billion people with an official identity. The principal goal of the program is to fight the corruption that bedevils poverty alleviation in the sub-continent – "to ensure inclusive growth by providing a form of ID to those who don't have any identity."[11]

The program creates a unique, 12-digit number – known as AADHAAR, or foundation, in Hindi – that each Indian citizen can use to open bank accounts, register mobile phones, or access basic services such as welfare and housing.

The numbers will be stored in a centralized database and linked to both basic demographic (name, birthdate, gender, address) and biometric (photograph, ten fingerprints, images of both irises) information. The biometric information will be used to "de-duplicate" the database, ensuring that each individual is assigned only one number, though when biometric data is missing or unreadable, the demographic information will perform the same function. After the initial enrolment phase, the UIDAI is to act primarily as an authentication service, verifying matches between numbers and biometric data. The AADHAAR can also be connected to a mobile phone number or e-mail address.

The project aims both to prevent persons receiving benefits from government programs more than once, and to allow people who previously could not receive any support due to lack of a proof of identity to be able to benefit. For the private sector, meanwhile, the AADHAAR system is designed to provide access to banking services for a section of the population so far excluded from the system because they cannot prove their identity.

The enrolment process for AADHAAR includes the registration of demographic data (name, date of birth, address, etc.) and, where possible, of ten fingerprints and two iris scans.

The UIDAI and the National Population Register (NPR) operate the enrolment centers; a unique ID number is issued once the Central Identity Register (CIDR) processes the data. The UIDAI anticipates a delay of 60 to 90 days, but longer periods are not excluded. The individual does not receive any token or document, just a simple letter stating her or his unique ID number. As of August 2013, nearly 400 million individuals were enrolled.

Some people argue that a single, centralized database is vulnerable to attack. The UIDAI insists that both the limited amount of information collected and the fact that such information can only be used for identity authentication will help ensure security. But there are no such restrictions on the UIDAI's public and private sector partners — insurance companies and banks among them.

The Indian program is nevertheless attracting a great deal of attention in other countries. Nigeria, for example, has just announced plans to create a civil database, based on the UIDAI's, leveraging the African country's experience to date in using biometrics to ensure financial inclusion

[11] *It is not to be confused with a parallel program, the National Population Register, which seeks to create national ID cards*

and in elections. Recently proposed legislation in the US, meanwhile, would extend the uses of a biometrically verified social security number for verifying employment eligibility[12].

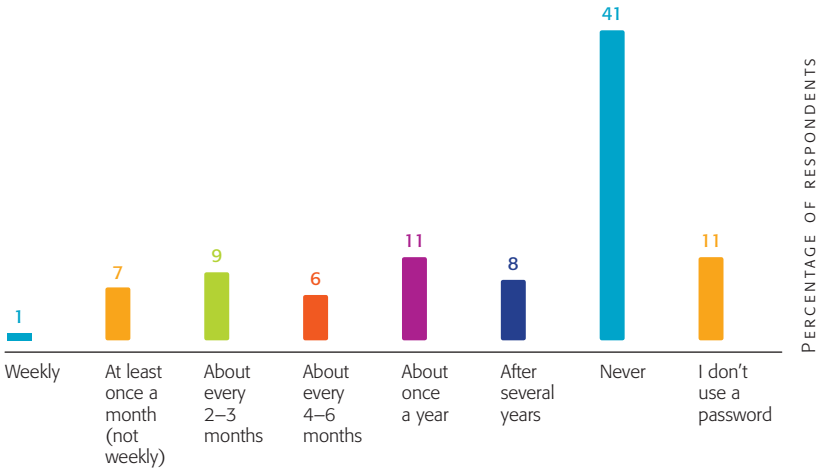
- Travis Hall points out that – from a user's perspective – a single identifier provides a potential "key" through which various aspects of a person's life can be strung together in inappropriate ways, p. 32
- The UIDAI program clearly violates the principles of proportionality and minimization of data collection, says Alessandro Mantelero, p. 35
- Jan Zibuschka emphasizes that the UIDAI program offers strong authentication since "the unique identifier has been linked to several biometric attributes of a user," p. 43

Federated Identity Across Accounts: UK Identity Assurance Scheme

2.3

Re-using already active personal access data from existing online accounts to access eGovernment portals raises significant questions about password security – especially as many users do not change their passwords with any frequency (*see* ***Fig. 11***).

How often do you change your most important passwords and security numbers on your own initiative (for electronic devices and services)?



Source: BITKOM February 2010, Germany (14+), / Forsa Darstellung © Statista

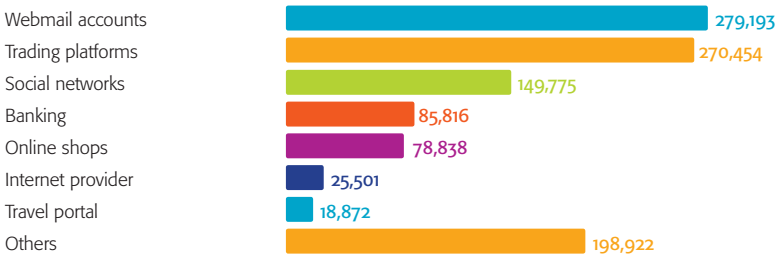
Fig. 11
Password Fatigue
Almost half of Germans never change their online passwords. Only about 20 percent change their passwords either annually or after several years; and just 25 percent change their passwords weekly or over several months.

[12] *http://uidai.gov.in/*

The data in ***Fig. 11*** is three years old, but we can only assume, given the recent proliferation of profiles requiring passwords and user names, that "password fatigue" remains high – which is worrying, considering the incidence of online identity theft (*see* ***Fig. 12***). The December 2012 cover story in Wired magazine in the US, for example, was themed "kill the password," claiming that password use carries security risks[13].

Source: Bundesamt für Sicherheit in der Informationstechnik Darstellung © Statista Germany; 2010

PLATFORMS IN GERMANY IN 2010, WHERE MOST IDENTITY AND PASSWORD THEFTS OCCURRED



NUMBER OF STOLEN IDENTITIES AND PASSWORDS

Fig. 12
Online Identity and Password Theft
Most theft occurs in webmail accounts, trading platforms, and social networks. Banking and online shopping appear to be better protected.

Banking and shopping online are probably more secure because they are directly related to payments. Many more people use social networks, of course. And they may be significantly more relaxed about securing them.

It would seem, indeed, that most people prefer to keep things simple, using "social sign-in" procedures that leverage existing login information from a social networking site to sign into third party websites, rather than memorize multiple passwords (*see* ***Fig. 13***).

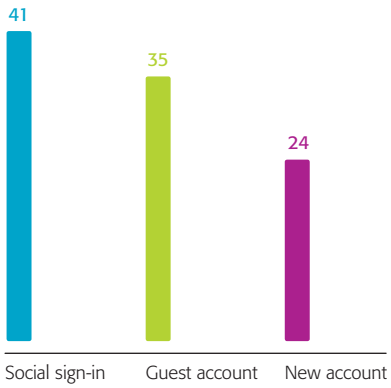
When it comes to re-using social sign-in procedures to access government services, however, some people – notably in Germany, but also in the US – are significantly more ambivalent (*see* ***Fig. 14***).

In emerging nations, by contrast, people seem significantly more relaxed. Security concerns may simply be lower in such countries, of course.

And their citizens' relative lack of concern may also reflect a greater openness to new technologies.

[13] *http://www.wired.com/magazine/20-12/*

WOULD YOU USE SOCIAL SIGN-IN IN ORDER TO AUTHENTICATE YOURSELF ON A WEBSITE, OR WOULD YOU RATHER CREATE A GUEST OR NEW ACCOUNT?



PERCENTAGE OF RESPONDENTS

Source: Janrain, Blue Research Darstellung © statista

Fig. 13
Keeping Things Simple with Social Sign-in
Nearly half of Americans prefer to use the social sign-in option to authenticate themselves. About one third would consider access via a guest account, which allows the user to remain anonymous and requires no personal data to be made available to the platform operator. Creating a new account is the least popular option.

"I WOULD LIKE TO BE ABLE TO USE THE PERSONAL PROFILES I ALREADY HAVE (E.G. FACEBOOK OR LINKEDIN) TO ACCESS ELECTRONIC SERVICES FOR CITIZENS, FOR EXAMPLE TO REQUEST A NEW DRIVER'S LICENSE OR REGISTER A CHANGE OF ADDRESS."

PERCENTAGE OF RESPONDENTS "STRONGLY AGREE"

BASE (regular Internet users)	GERMANY strongly agree	BRAZIL strongly agree	INDIA strongly agree	USA strongly agree	CHINA strongly agree	SOUTH KOREA strongly agree
	n=306	n=301	n=301	n=303	n=301	n=302

Source: Future Study MÜNCHNER KREIS 2013

Fig. 14
Ambivalent Picture
In China, India, and Brazil simplicity of use trumps security concerns. But in Germany and the US, citizens are more reluctant to access government services using their existing personal profiles.

In the UK, meanwhile, the government is forging ahead with an Identity Assurance Programme (IDAP) that claims to overcome privacy and security concerns by avoiding the need for a centralized database.

Use Case: The UK Identity Assurance Programme (IDAP)[14] 2.3.1

The Identity Assurance Programme (IDAP)[15], which is embedded in a strategic cost-cutting service delivery plan and is linked to ICT reforms and cyber-security goals, aims to provide a single point of access for all online government services, from welfare applications to passports and vehicle tax. It is a core element of the "digital by default" policy of the Government Digital Service within the Cabinet Office. It is designed to facilitate identity assurance schemes to enable trusted transactions online that allow "business and devices ... to assert identity safely and securely online in order to better access and transact with public services" and to transform government services, making them "more efficient and effective for users."

The initiative arose, at least in part, from the failed attempt to introduce a universal, government-controlled biometric ID card. It is informed by the federated model of identity assurance suggested over a decade ago by the New Labour Directgov scheme. The underlying privatization aim was to create a "trust eco-system" using trusted private sector identity service providers to authenticate citizens' online access to government services. The arguments put to the public for this include user convenience to combat login and password "fatigue," efficiency, and putting citizens in control of their identity and privacy. The absence of a central database is underlined.

Announcing the system on 15 August 2011, the Cabinet Office stated that building public trust in federated online services would avoid duplication and inconvenience arising from entering the same data several times over to access different services. Welfare benefit claimants would be able to "choose who will validate their identity by automatically checking their authenticity with the provider before processing online benefit claims."

In 2012, the Identity Assurance program sought to enable sufficiently trusted secure and convenient access to eGovernment services through identity assurance schemes. The first is to be run through private sector bodies including the credit agency Experian, Mydex, Verizon, Digidentity, and the Post Office. By October 2014, the Government expects the system to be fully functional with data storage entirely outsourced to private "certified providers," retaining only the responsibility for providing a single point of user access via its revamped portal. Delayed implementation has led to the scheme becoming less ambitious.

The original intention was for the Department for Work and Pensions (DWP) to steer the program via the introduction of a controversial universal credit system for some 21 million welfare benefit claimants. A more modest rollout replaced this in 2013 with company car drivers and employers filling in staff expenses form P11D for HM Revenue & Customs. Other services will follow dismantling of government inter-departmental data-sharing arrangements — between HM

---

[14] *The text on the UK Identity Assurance Programme was kindly contributed by Prof. Juliet Mayer-Lodge, a member of the Expert Group of the Privacy Committee of the Biometrics Institute. Her brief comments are strictly in a personal capacity*

[15] *https://www.gov.uk/government/publications/identity-assurance-enabling-trusted-transactions*

Revenue & Customs (HMRC) and the UK Border Agency, for example — and as the market in citizens' personal data and identity assurance expands.

The IDAP is part of an eGovernment reform to create Application Programming Interfaces (APIs) allowing third parties to present content and effect transactions on the government's behalf. The overall goal was to shift from "public services all in one place" (closed and unfocused) to "government services wherever you are" (open and distributed).

The government claims that the system will deliver multiple benefits in terms of privacy and security, as well as combating identity theft. Citizens will be able to choose from a pre-selected range of "trusted non-government organizations," such as credit reference agencies and employment services providers, authorized to verify their identity, without sharing personal data. The British public remains ambivalent and trust has to be built.

- "Only if both parties trust each other can identities be shared in what we may call an equilibrium of trust," says Johanna Sprondel, p. 30
- Achim Klabunde refers to a recent survey showing that UK citizens had high trust in the government scheme, but low confidence in the expected private parties involved in it, p. 51
- Does the use of identity provided by private organizations increase the chances of misuse? In the context of eCommerce, Rocco Panetta points out that identity thieves misuse consumers' personal information in various ways, p. 41

Government Services Going Mobile: eVoting on the Mobile Phone 2.4

Our fourth and final use case concerns eVoting via the mobile phone. Because mobile devices offer users a high degree of convenience and flexibility, their potential for accessing eGovernment services of all kinds — including participation in political elections — is plainly considerable. However, there is also considerable variation in both the scope of eGovernment services currently available worldwide, and in users' attitudes toward using mobile devices to access them.

Consider, for example, ***Fig. 15***, which shows the extent to which eGovernment services are used across six different countries, and the proportion of people in those countries who access such services via mobile devices.

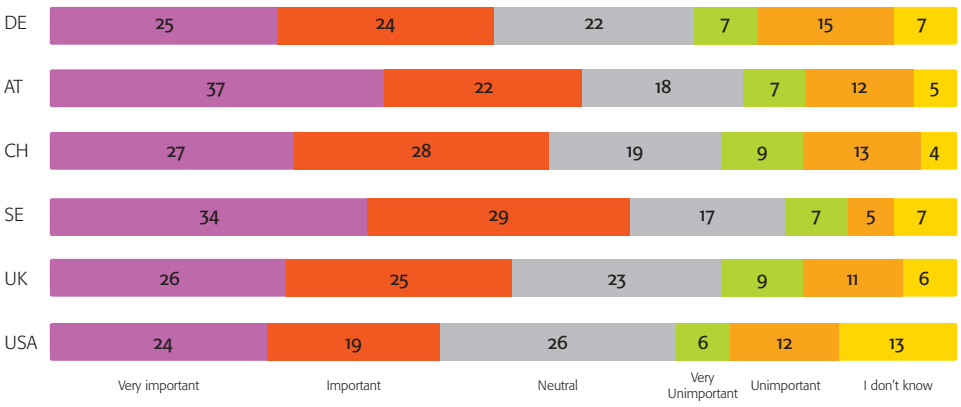
India and China are well ahead in using mobile devices to access eGovernment services, with Brazil close behind. Germany, however, lags behind even the US: a reflection, no doubt, of the government's historical reluctance to drive services online (though the recent passage of eGovernment legislation is likely to accelerate adoption).

	Germany	USA	Brazil	China	India	South Korea
Use of eGovernment						
All respondents	30% n=1,213	31% n=1,218	37% n=1,215	54% n=1,207	62% n=1,211	43% n=1,214
18–34 years	27% n=365	27% n=416	34% n=561	56% n=495	63% n=620	31% n=454
35–49 years	32% n=412	34% n=370	40% n=369	55% n=422	68% n=396	47% n=441
50 + years	31% n=436	35% n=432	39% n=285	49% n=290	46% n=195	54% n=319
Use of Mobile Government						
All respondents	35% n=214	40% n=218	60% n=254	54% n=567	62% n=543	43% n=397

Source: Future Study MÜNCHNER KREIS 2013

Fig. 15
eGovernment Services and Mobile Access
Significantly more people use eGovernment services in emerging nations than in the developed world. They are also more open to accessing those services via mobile devices.

Which importance will mobile phones and other mobile devices have on carrying out visits to government offices?



Base | All respondents: AT, SE, and USA

Source: E-Government Monitor 2012

Fig. 16
Future importance of mobile phones and other mobile devices for carrying out visits to government offices.
Shows the results of a 2012 survey that asked people in five European countries (Germany, Austria, Switzerland, Sweden, and the UK) as well as in the US how important mobile access devices are likely to become in the future.

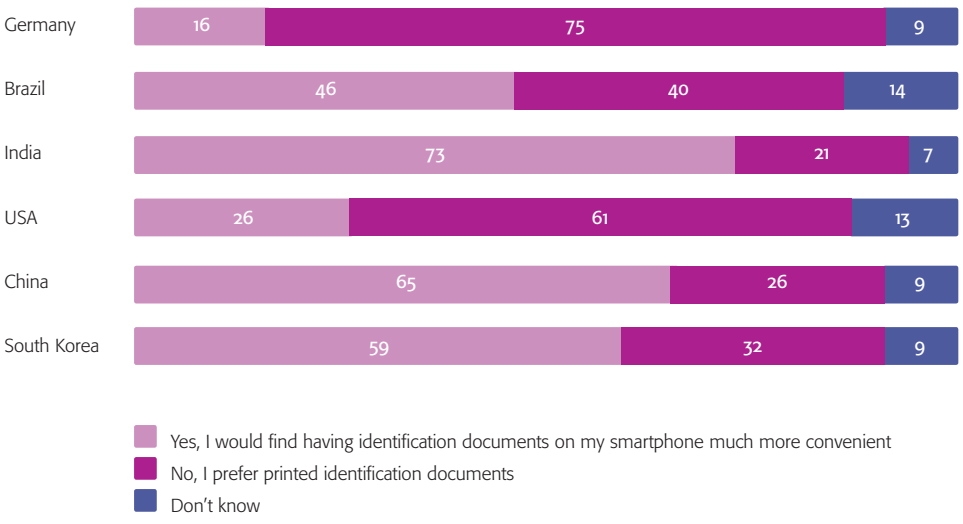
Sweden, of course, has been a leader in mobile phone use for years. And the relative lack of enthusiasm elsewhere may reflect the fact that in some countries eGovernment services are still designed for access via personal computers, not mobile phones.

Citizens in developed countries are also more skeptical than those in emerging nations about the merits of storing and carrying "virtual" IDs electronically in their smartphones, rather than in paper or plastic form (*see* ***Fig. 17***).

Virtual ID – Countries

Could you imagine using your main official form of identification (ID card, driver's license etc.) virtually on your smartphone instead of a physical document?

%



Base	Germany	Brazil	India	USA	China	South Korea
	n=306	n=301	n=301	n=303	n=301	n=302

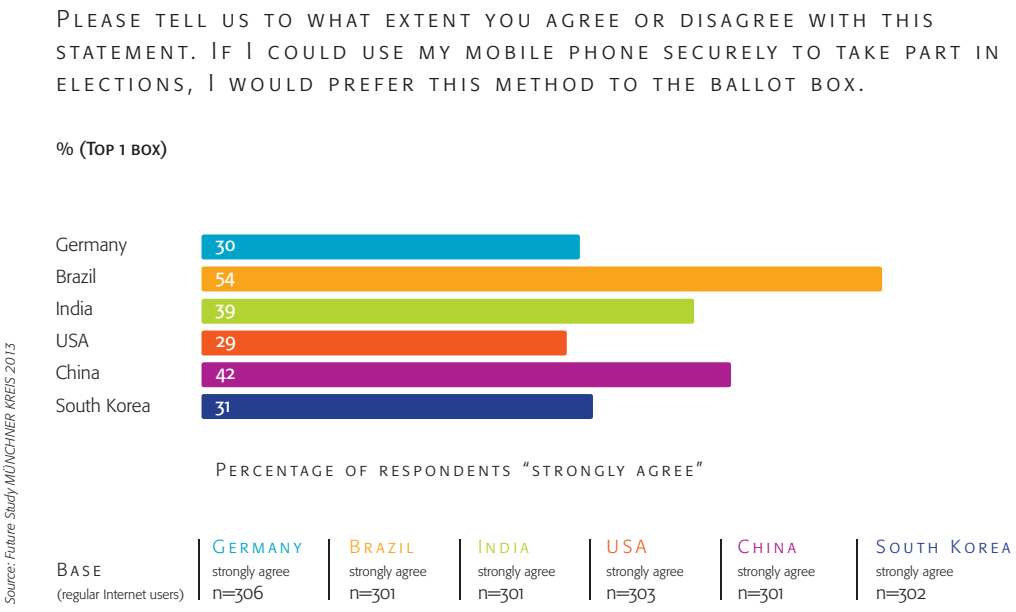
Source: Future Study MÜNCHNER KREIS 2013

Fig. 17
Virtual ID – the Role of Smartphones
In India, China, and South Korea people would be happy to store their ID documents in their phones. In the US and especially in Germany, people still prefer printed documents.

Electronic voting describes a system that enables people to vote electronically. This definition[16] encompasses both voting in the polling station through electronic mechanisms that may include the use of an electronic ID and remote voting through the Internet, a Web-based service, applications, or even mobile devices such as smartphones.

Mobile voting is considered to be the use of mobile phones for voting. Recent considerations include the use of eIDs to support the mobile authentication process.

"Electronic identity" (eID) is a means for people to prove electronically that they are who they say they are and thus gain access to services.



Source: Future Study MÜNCHNER KREIS 2013

Fig. 18
Receptivity to Mobile eVoting
More than half of Brazilians would prefer to use their phones to participate in elections. In Germany and the US, only a minority would be willing to abandon the ballot box.

Fig. 18 describes four different use cases that reflect four possible identity management systems.

In both Germany and the US, voting via the ballot box is, of course, a long-established tradition, which may explain the marked reluctance of these countries' citizens to switch to eVoting via their phones. But there are also other reasons why electronic mobile voting in parliamentary elections is not yet in use.

[16] *The definition is provided by Jorge Villarino*

Use Case: Mobile eVoting

2.4.1

While there is a rich literature on electronic voting and first proposals regarding the use of smart devices for the secure implementation of such schemes, the application of eID cards or mobile phones for electronic voting purposes is not yet common in practice.

This may be due to the fact that not all citizens are equipped with secure smart cards (such as eID cards) yet, and that the business case for the creation of such infrastructure solely for voting purposes needs to be better communicated. With the advent of nationally standardized electronic identity card projects this problem may disappear, making it likely that the use of such eID cards as the nPA (German identity card) in combination with a mobile phone as secure electronic voting methods will be further investigated. Technological developments are also likely to help.

In the near future, for example, Near Field Communication (NFC) capable mobile phones with secured displays and keypads could serve as trustworthy readers for eID cards. And soon mobile phones may even have so-called trustlets©[17] that incorporate virtualized eID cards into mobile phones. For voting purposes, the mobile phone would connect to the network via Over-The-Air (OTA) services or WLAN and the voting server would run the voting software. In Estonia, meanwhile, where online voting has been possible since 2005, the authorities emphasize that online voting is meant to supplement, not replace, traditional methods. Moreover, although citizens could vote from their mobile phones in the 2011 parliamentary elections, they still required a computer with Internet access to complete the process.

So how might mobile eVoting work in practice?

Phase 1: Would be a set-up phase in which the electoral authorities would determine a common key system for enciphering the ballots cast.

Phase 2: Would concern voter registration. Each voter would receive a unique credential, generated by the (virtual) eID card and guaranteeing uniqueness and anonymity.

Phase 3: Would allow the voter to use his or her mobile phone to complete the ballot form. A secure local connection between the mobile phone and the user's eID would be established in order to store the ballot securely inside the ID card (a step that would only be necessary if eID rather than virtual ID were used).

Phase 4: Would concern transmitting, or sending, the vote and the ballot to a central bulletin board. In order to avoid fraud or skimming attacks, the user would have a second PIN.

Phase 5: Would concern counting the votes. Each voter's unique credential would eliminate duplicates, the ballots would be decrypted with the system established in Phase 1, and the decrypted ballots would be tallied to obtain the final result.

---

[17] *Applications that are stored and processed in a specialized secured department of a mobile device*

In the early stages of implementation, such a voting system could be used in the context of elections to sporting bodies, or in local elections because acceptance levels are expected to be higher. The use of mobile devices for parliamentary elections would be an additional — and very likely hotly debated — step.

- From a technical point of view, mobile eVoting fulfills the highest security standards, argues Gisela Meister, p. 45
- Jorge Villarino points out that a key element is trust and confidence in the voting process. Lack of trust might increase in the case of remote voting systems, p. 37
- Achim Klabunde concludes that "such systems should only be operated in environments where voters' trust in the organization conducting the vote is high and where there is little risk of interference or tampering," p. 51

IMPLICATIONS OF THE USE CASES 3.

The second part of this report comprises the comments of our expert Task Force participants. In contrast to the largely descriptive and neutral first part, it represents a wide diversity of individual views, not all of which concur. However, by presenting such diverse opinions it is hoped that the report will both highlight the complexity of the issues raised by the use cases, and stimulate further discussion and debate.

The expert comments are divided into three parts – philosophical and social, legal, and technological.

Implications of the Use Cases: Philosophical and Social Perspective 3.1

In this section, two of our Task Force experts – Johanna Sprondel and Travis Hall – discuss the implications of the use cases from a philosophical and social perspective.

Taking the English moral philosopher John Locke's definition of identity — self as consciousness — as her starting point, Sprondel's focus of interest is in establishing a balance between trust and control as a condition for Internet identity. Hall, meanwhile, discusses how privacy and inclusion interact, and borrows from the insights of media studies to show how, just as the meaning of signs is never truly fixed, the connotations of an ID document can be "multifaceted, contradictory and fluid."

Balancing Trust and Control as a Condition for Identity in the World Wide Web 3.1.1

By Johanna Sprondel

From a philosophical perspective, it's difficult to come up with a succinct definition of identity, let alone one that includes a perspective on the Internet. This may partly be due to the fact that the question of identity traditionally touches on the very core of humanity and is therefore closely connected to concepts of personhood. As a result, the question of identity has been strongly influenced by religion, and has been a concern in fields as diverse as political theory, gender studies, postcolonial studies, psychology, phenomenology, and many others.

One might, however, take John Locke's 1698 position as a starting point and say that identity (the self) is always founded on consciousness: that it is about being the same person, conscious of our thoughts and actions, in the past, present, and future.[18] This perspective allows us to state, in regard to the Internet and identity, that no matter how many mobile devices I carry, how many online personas I create, what I call myself on Facebook or in a chat room, for the understanding of the concept of personhood (and it is the identity of a person that is at issue when we discuss

---

[18] *John Locke: An Essay Concerning Human Understanding, II, XXVII "On Identity and Diversity," 1698*

identity in this context) it is vital that I am able to make a relationship between all these different identities – that I can identify with them.[19]

Of course, just because someone knows my online persona, my name in a chat room, in an eMarketplace, or on Facebook, they still do not know a great deal about who I (the person behind these identities) am. For purposes of security and authentication this might arguably be considered something desirable; a factor welcomed by those who deal with me, and one that could make some transactions easier for me. But how does it generate the necessary equilibrium between trust and control? The key idea behind many authentication and security processes is that identity is the basis on which certain estimates, concessions, and restrictions are made. From simple processes like logging into one's e-mail account, to more complex processes of identification and authentication such as online banking or eShopping that actually require proof (by a test-payment, a copy of my ID, address check, etc.) it is essential to ensure that the user logging in is the person owning the account. This, at any rate, is the intention and it raises the issue of trust as well as control.

Let us first consider control. The Oxford English Dictionary defines "to control" thus: "To check or verify, and hence to regulate (payments, receipts, or accounts generally): orig. by comparison with a 'counter-roll' or duplicate register; […] To exercise restraint or direction upon the free action of; to hold sway over, exercise power or authority over; to dominate, command." Two things become clear from this definition. First, that control implies a limitation; only if certain conditions are fulfilled may actions follow. In terms of Internet use this means that only if I can prove that it is really me who is trying to log in may I take actions granted to me by my contractual partner – and only if I am sure that the contractual partner is who I think him to be should I share certain information. Second, control also implies power, sway, and authority. A contractual partner may execute or direct certain actions. And this is where trust becomes an important issue. All parties involved should want to make sure that they are dealing with the person they think they are dealing with, so what we want to ensure is that the person logging into my account is trusted to be me. My identity has to be proven by a login and password, given to me by the contractual partner, or chosen by me in agreement with that partner (in an act of control, we might say). At the same time it is the user/account holder who trusts the institution that offers the service: that when sharing my personal data with them and unveiling my identity to them I actually believe that they run the service I am logging into. Only if both parties trust each other can identities be shared in what we may call an equilibrium of trust. And we may state the same for control: as soon as one party acts deceptively about their identity, or control is exercised in an inappropriate way, this equilibrium becomes unstable.

The abuse of control can have many faces — fraud, skimming, fake accounts among them — not all necessarily intended by any of the contractual partners. That is why security as well as high standards of authentication should be of vital interest to all users of the World Wide Web. Indeed, only if trust and control are intended, and exercised in such a way, by all parties involved, as to ensure equilibrium, can we speak of identity in the Internet in terms of its core meaning: the instance that brings together consciousness of our past, present, and future thoughts and actions.

---

[19] *An extreme example for this may be found in the world of Second Life: Second life rape victims report about severe traumata, having fully identified with their avatars/online personae*

Privacy and Inclusion

By Travis Hall

Privacy

Identification is central to both the protection and degradation of privacy. While much ink has been spilled on the subject, two particularly useful conceptual tools help us grapple with the role of identification and its limitations in broader discussions of privacy issues: Privacy as Contextual Integrity and Privacy as Obscurity.

Helen Nissenbaum developed the concept of Privacy as Contextual Integrity to describe the general harms that occur when privacy is violated. Her definition enables us to transcend the public/private sphere dichotomy, which no longer really describes either the way in which we conduct our lives or the way in which privacy is valued (are Google searches "public," for example?). Instead, Nissenbaum argues that in "observing the texture of people's lives, we find them not only crossing dichotomies, but moving about, into, and out of a plurality of distinct realms," i.e. contexts.[20]

When people discuss violations of their privacy their concern is with the proper flow of information within and between these contexts. You would not, for example, share the same kinds of information with your doctor as you would with your employer, even though you can reasonably be required to share information with both that could be considered "private." According to Nissenbaum, "What most people care most about is not simply restricting the flow of information but ensuring that it flows appropriately."[21] Thus, identity is both a set of informational objects that have appropriate or inappropriate flows, as well as significant keys through which various contexts can be tied together (again, appropriately or inappropriately).

For example, a fingerprint in and of itself is a meaningless smudge, but it can link an individual to a crime scene, a job application, or a medical record. At times these links are desirable, but the danger is in information that is necessary and good in one context being linked to another through the common identity. It is for this reason that identification technologies often fall into one of two distinct categories — profiling (race, gender, buying habits, etc.) or identification (name, government issued number, etc.) — and it is claimed that the technologies are "privacy protective" because they do one thing, but not the other. Indeed, technology companies often argue that because no name is linked to a profile or vice-versa, no violation of privacy can occur; the contextual flow of information remains appropriate.

The palm vein technology utilized by the GMAT can be seen as a generally privacy-positive technology, as it grants legitimized authentication (are you who you say you are?) without providing a link to other contexts. Unlike fingerprints, palm veins cannot be left behind for forensic use or for fraudulent purposes; and unlike iris scans or facial recognition technology, they cannot be collected from a distance (and thus potentially without the knowledge or consent of the individual concerned).

---

[20] *Helen Fay Nissenbaum, Privacy in Context : Technology, Policy, and the Integrity of Social Life (Stanford, Calif.: Stanford Law Books), 4*

[21] *Ibid*

This concept of privacy raises problems for the UK and Indian ID programs, however. While both claim to be mere authentication services that do not allow for function creep (or the use of data collected for one purpose in other, unrelated uses), a single identifier nonetheless provides a potential "key" through which various aspects of a person's life can be strung together in inappropriate ways. This concern is often raised in regard to government services collecting information for social welfare purposes that may also be used for security/policing purposes, or sold on to private companies.

Another concept that has recently become more important in privacy debates is that of "obscurity."[22] Discussions of Privacy as Obscurity also recognize that it is often not the hiding of information that protects privacy but rather its selective and strategic revealing. It is possible, for example, to avoid being identified while walking down the street if you wear a ski mask, but the act of wearing a ski mask on the street draws much more attention (most likely negative) than the possibility of being recognized. In other words, when people are "in public" what they desire is not privacy in the more traditional sense of remaining wholly anonymous or having all information regarding themselves hidden, but rather that they remain obscure — part of the crowd, and not singled out for special attention.

Identity, then, is both central to maintaining privacy and limited in its application. Remaining obscure means not being constantly identified or singled out for special observation or treatment; but it also means that the possibility of identification is less of a concern than the potentially negative ramifications of being categorized or profiled in an undesirable way. As Big Data collection and analytics continue to take hold, the actual risks of breaching the contextual flow of information may come less from the possibility of knowing a person's name, and much more from the myriad other bits of data that can single them out for discriminatory treatment. Paradoxically, it is often those who are NOT identifiable that are targeted for discrimination or ill treatment.

India's Unique Identification (UID) project, in common with most other ID programs, has rules for "exception processing" to ensure that individuals who do not easily register in the system due to physical traits that hinder biometric enrollment are nonetheless included. Yet to be marked as an exception inevitably leads to greater difficulty in the normal course of business; and it is often through marginal difficulty that bureaucratic exclusion and neglect occur.

Inclusion

In the promotional materials produced about the Indian ID project, the concept of "inclusion" is given particular prominence. The Indian government describes "inclusion" through identification as both "social" and "financial." And in discussing the use of biometrics for identification in elections, the term "political inclusion" is also used. The use of this terminology appears straightforward. Lack of identification is a barrier to participation in sectors of modern society. Without it, one cannot open a bank account, gain access to certain financial or social goods (for example, my local public pool is free for residents but requires an ID), and its absence can mean disenfranchisement or harassment.

---

[22] *See: Flynn Brunton and Helen Nissenbaum, "Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation," First Monday 16, no. 5; Woodrow Hartzog; Frederic Stutzman, "The Case for Online Obscurity," California Law Review 101, no. 1*

It should be noted that while the sociologist and surveillance studies scholar David Lyon has argued that identification is by definition a form of "social sorting"[23] (i.e. that the act of identification is always one of creating hierarchical categorizations), these forms of discrimination (in the broad sense of the term) can also be beneficial and positive for both society as a whole and for those being identified. It is also necessary to point out, however, that this is by no means a natural state of being. Societies have existed for centuries without modern systems of identification, and significant portions of the world's population do not have stable documentation of their identities. Moreover, the programs that require identification create barriers for those who lack it.

Some of the insights of media studies are helpful in unpicking this argument. Identification is not normally thought of as a form of media, but it does consist of particular types of information technology that convey a specific type of communication — the identity of the individual. Fingerprinting is a type of printing, as are ID cards (although often with photographs included), and facial recognition or iris scanning are merely algorithms applied to photographs and video. More importantly, however, identification is a means by which the relationship between the individual is represented and mediated vis-à-vis other individuals and institutions.

Thus, the ethical ramifications of an identification program depend primarily on the relationship between the individual and the institution, though, like all other media, these programs can also subtly shape, distort, and reconfigure these relationships in new ways. Key to this formulation is the assumption that identity is not something that is naturally always or already present but rather a constructed, relational process that is grounded in historical and cultural praxis. Identification, in other words, is the creation of signs that play central roles in the creation and maintenance of relations that are abstract and disjointed in both time and space.

Signs are never truly fixed in their meaning, and the connotations of an identity document can be multifaceted, contradictory, and fluid. This means that the products of identification regimes often take on much greater significance than their initial purpose and scope. Take, for example, the driver's license in the United States. Although only meant to certify the ability to operate an automobile legally, it has come to signify a ritualized transition into adulthood. In other words, identification programs are often accepted or rejected not on their technical or procedural merits but rather due to the culturally contextual significance that attaches itself to the program or technology. Inclusion and exclusion are both, therefore, procedural goals of the institutions creating identity programs. India, for example, argues that it is trying to include residents in its social welfare programs while excluding those who are defrauding the system. But these bureaucratic measures never occur in a political or cultural vacuum.

What it means to be identified, and whether or not this is a means of acceptance into a community or rejection from it, is a matter of contestation and struggle. As can be seen in the recent court battles in the United States, the role of identification in voting is particularly fraught. The introduction of any kind of eVoting, particularly with mobile phones, would depend less on the technological capabilities and more on the social infrastructure and cultural or political sensitivity of the project. As stated above, it is typically through the introduction of marginal difficulty that

---

[23] *David Lyon, Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination (London; New York: Routledge)*

identity systems discriminate and exclude, and this is particularly concerning when it comes to enfranchisement. Digital access may create ease of use and security for some, but at what price? It is important that rights are granted equally. The relative easing of access for some, even if access does not change for others, can be discriminatory.

Implications of the Use Cases: Legal Perspective 3.2

In this section, three of our Task Force experts – Alessandro Mantelero, Jorge Villarino, and Rocco Panetta – discuss the legal implications of the use cases.

Mantelero considers the use of biometric data in personal identification systems and examines the conflict between opposing needs (data protection, security, profiling) and their interaction, examining the legal constraints designed to balance the needs of the digital economy and government with the fundamental rights of individuals (as recognized by the European Union). Villarino, meanwhile, focuses on the legal and political challenges of eVoting and examines, in addition, the developing regulatory environment around eCommerce.

In addition, Panetta discusses identity issues in regard to eCommerce, which has no direct relationship with the use cases, but is nonetheless an important issue, especially from a legal and political perspective.

Biometric Personal Data 3.2.1

By Alessandro Mantelero

Biometric data (see chapter 2.1) can be used to identify people in a unique way because they are based on the digitalization of one or more parts of an individual. Three elements characterize biometric data and the identification systems based on this information:

- Universality: the biometric element that exists in all persons
- Uniqueness: the biometric element must be distinctive to each person
- Permanence: the property of the biometric element remains permanent over time for each person.

The use of biometric data dramatically reduces the risk of identity theft. At the same time, however, it is based on elements that the individual cannot usually change, so it is difficult to avoid being tracked or to exercise self-determination without recourse to legal protection. Moreover, such devices as drones, video-surveillance systems, and sensors are able to collect information without the knowledge of the data subjects. Meanwhile, governments or private companies can impose the adoption of biometric identification systems as a condition of access to their services (see the Indian case, above).

For these reasons, and in light of the future EU General Data Protection Regulation, accurate data protection and privacy impact assessments should be carried out before the adoption of any biometric technology.[24] The European data protection authorities identified the following fundamental factors to take into consideration in order to realize this assessment:

- The possibility of adopting less intrusive means to achieve the desired purposes
- The prevalence of data protection over cost reduction or the efficiency of the system
- The adequacy of the biometric data collected as a means of satisfying, in a proportional way, the need for personal identification.

Generally speaking, constitutional rights and data protection principles do not hamper the use of biometric data. However, in accordance with the principles of proportionality, necessity, and minimization of data collection,[25] the use of these technologies is only admitted where the collection and processing of biometric data are adequate, relevant, and not excessive. At the same time, whenever possible, and in order to respect the right to self-determination in regard to personal information, the data controller should offer alternative solutions to the data subject who does not accept identification by biometric technologies.

The relevance of individual self-determination also limits the extensive use of individual consent to collecting biometric data, since consent is only legitimate if it is freely given and informed.[26] It is also worth emphasizing that consent "shall not provide a legal basis for processing, where there is a significant imbalance between the position of the data subject and the controller."[27] For these reasons, extensive biometric identification systems, which have been developed in countries such as India, are in conflict with the fundamental rights and regulations of the European Union. The AADHAAR, India's Unique Identity (UID) program, clearly violates the principles of proportionality and minimization of data collection,[28] as it is a massive biometric data collection involving each of India's 1.2 billion citizens, by providing them with a unique, 12-digit ID number and an ID card linked to the data. This system will be used not only for eGovernment purposes, but also for banking transactions via mobile apps and for eCommerce. The project, if completed, will create a centralized biometric database and will be the largest identity biometric program in the world — hence the criticism it has received, both in India and abroad.[29] Awareness of the limits to the use of biometric data is even more necessary in the context of European Horizon 2020[30] politics and as smart cities and smart communities projects, characterized by the use of multiple monitoring devices and sensors, are developed. It is important to avoid an approach focused only on technology without an adequate assessment of the legal implications of the adopted solutions. Principles such as Privacy by Default and Privacy by Design (see box "Culture of Privacy: Privacy by Design" on p. 17) should become part of any such projects and integral to the cultural background of the new generation of technologists.

If the value of data protection is underestimated, such projects and strategies run a double risk, legal and economic, due both to the power of control and sanction exercised by data protection authorities,[31] and to the need to redesign the technological model adopted — a costly option.

---

[24] *The first regulations on privacy impact assessment were introduced in the 1990s; for a comparative analysis of the different regulations, see David Wright and others, "PIAF A Privacy Impact Assessment Framework for data protection and privacy rights," September 21, 2011 www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf accessed March 3, 2013. It is worth emphasizing that privacy impact assessment and data protection assessment do not coincide, as the concepts of right to privacy and data protection are different. However, the tools and procedures used to identify the potential privacy risks can be useful in order to better define the procedures and methods of the data protection impact assessment*

[25] *See Directive 95/46/EC, Article 6 and EU Proposal for a General Data Protection Regulation, Article 5. See also European Court of Human Rights, Grand Chamber, S. and Marper v. The United Kingdom, (Applications nos. 30562/04 and 30566/04), December 4, 2008. The principle of minimization implies that the retention period of biometric data should be no longer than necessary for the purposes for which the data have been collected*

[26] *See Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on July 13, 2011 http://ec.europa.eu/justice/data-protection/Article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf*

[27] *See EU Proposal for a General Data Protection Regulation, Article 7 (4)*

It should also be noted that the restrictions on the use of biometric data adopted in the European Union concern not only data collected in the member states of the EU, but also biometric information on European citizens that is collected abroad.[32]

Finally, where the use of biometric data is permitted under EU law, it is important to limit the number of persons involved and to adopt a data-protection-by-default approach in designing the architecture of the system of identification and its level of security. Indeed, the European data protection authorities, on several occasions, have pointed out the risks related to the creation of permanent centralized biometric databases. And there is an overall need to balance the development of useful devices and technologies with respect for legal requirements, fundamental rights, and informational self-determination.

Identity and eVoting

3.2.2

By Jorge Villarino

Electronic voting (also known as eVoting) might be defined as the way we name a system to vote electronically — both voting in the polling station through electronic mechanisms which might include the use of an electronic ID, and remote voting via the Internet, a Web-based service, applications, or even mobile via smartphones. (In Estonia, which could be considered the leading example of electronic voting, only Internet-based remote voting is included in the definition.)

From a more technological perspective, however, eVoting includes: electronic voting machines, optical scan devices, election authority-run kiosks, telephone voting, WAP mobile telephone voting, SMS voting (text messaging), digital television, and Internet voting (remotely or in a polling place).

There is no global or European legislation regarding electronic voting, and no legal study can be drafted comparing geographical areas. However, there are some key aspects regarding the right to vote that could be considered universal: the vote must be free, equal, direct, and secret. Such features are included in most modern constitutions and must therefore be guaranteed by any voting system, including electronic. Indeed, some key democratic institutions, including the Council of Europe, have already worked hard on this question and their recommendations should be taken into account.[33]

Legal and political challenges of eVoting

Since voting can be considered the foundation of democracy any innovation in the electoral system, even purely technological, should be thoroughly considered and carefully implemented. Identity is a core aspect of the voting system and digital ID has been implemented in many countries. Public services in some countries are also provided through so-called eAdministration

---

[28] *See also the Facebook case on facial recognition feature, http://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf*

[29] *See Standing Committee on Finance (2011-12), Ministry of Planning. The national Identification Authority of India Bill, 2010, Presented to Lok Sabha on 13 December, 2011 Laid in Rajya Sabha on 13 December, 2011 http://164.100.47.134/lsscommittee/Finance/42%20Report.pdf; R. Bowe, India's gargantuan Biometric database Raises Big Question, September 27, 2012 https://www.eff.org/deeplinks/2012/09/indias-gargantuan-biometric-database-raises-big-questions*

[30] *The EU Framework Programme for Research and Innovation: http://ec.europa.eu/research/horizon2020/*

[31] *See EU Proposal for a General Data Protection Regulation, chapter VI, section II. See also Article 34*

[32] *See Directive 95/46/EC, Article 4 and EU Proposal for a General Data Protection Regulation, Article 3(2)*

[33] *Council of Europe, "Proposal for a Council of Europe activity on eVoting standards," http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Work_of_eVoting_committee/03_Background_documents/98IP1(2002)11_en.asp#TopOfPage*

and there are ambitious projects at all levels, European and national. However electronic voting poses specific challenges. Among the most relevant:

- Different legislation in different countries: As already mentioned, there is no unique legislation regarding the right to vote. In some countries, including Belgium, Cyprus, Austria (in general elections), and Greece, voting is mandatory. The recognition of foreigners' right to vote also varies from one country to another.

- Data protection: What kind of data should be required for voting? Data protection regulation in the EU establishes that data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.[34]

- The use of ID cards for voting: Should we use electronic ID cards for voting? One of the most advanced countries in the world regarding eDemocracy is Estonia, which does use ID cards for that purpose. But what about foreigners? In most countries the right to vote is a citizen's right. The Indian AADHAAR scheme, for example, which is being implemented by the Unique ID Authority of India (UIDAI), provides unique identification to non-citizens and therefore a specific system should be provided to prevent – if necessary – those non-citizens from voting.[35] On the other hand it could be difficult to use non-governmental identity systems in elections. The UK Identity Assurance Programme, for instance, which gives citizens the option to access mobile and Web-based services offered at gov.uk with a non-government-issued credential they already use with other approved entities, might not be acceptable. More than just a legal issue, this is also a sociological and cultural problem. Identity for voting (and other features such as anonymity) must be granted by a governmental provider.

- Guarantees: The right to vote is a fundamental right enshrined in most modern constitutions, as well as in international treaties on rights and liberties, and it is governed by strict mechanisms (one person one vote, representatives of the electoral authority, representatives of political parties in polling stations, secrecy of vote, etc.). These mechanisms will have to be provided in an electronic voting system as well, but in some respects their implementation will be challenging. Only through an appropriate technological system could guarantees be enforced. And as established by the Council of Europe, all technical requirements should fully reflect the relevant legal and democratic principles.[36]

- Confidence and trust: A key element is trust and confidence in the voting process. In an electronic voting system, confidence in the system (even if that system works well) might be adversely affected by so-called "black-box software." Most people will have no idea how the electronic voting system works or even understand how the voting machines work.

Lack of trust might increase in the case of remote voting systems. Voters might not have sufficient technological skills, especially if the voting system works with different interfaces. Moreover,

---

[34] *Section 6.1b) of the Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

[35] *Explanation of the AADHAAR PROJECT. http://uidai.gov.in/what-is-aadhaar-number.html*

[36] *Council of Europe, "Certification of eVoting systems Guidelines for developing processes that confirm compliance with prescribed requirements and standards," February, 2011 http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf*

confidence in traditional voting systems will always be higher. Users might doubt that their anonymity is safe in an electronic system (the process is not "visible" to non-technicians, whereas a paper-based process offers the advantage of physical perception).

Electronic systems, furthermore, are managed by very few people, while traditional systems are controlled by a very wide electoral administration, some of them citizens. (Citizens control the process in poll stations on Election Day, and they usually perform the provisional counting.) In an electronic voting system only very few people would have access to the verification process and probably even fewer would be able to understand it from a technological point of view. Only a limited number of people would be involved in verifying votes and that could lead to fraud — the main threat to any electoral system.

On the other hand, public services in many countries are already accessed and managed through eAdministration tools. Indeed, such tools are much more widespread than electronic voting (see, for example, the UK Identity Assurance Programme). But is there a difference between eVoting and "ePublic Services"? Can experiences in eAdministration be used to argue in favor of the implementation of an electronic voting system? Why do people use electronic devices for banking transactions, for example, or for eCommerce experiences, and not for eVoting? The answer is neither legal nor technological. It has to be found in the political and sociological background of each country (see, for example, Figure 15, eGovernment Services and Mobile Access).

The potential of eVoting

This brief paper would not be complete if we just mentioned the barriers to electronic voting systems. There are also positive aspects. eDemocracy is not a new concept and in many countries people are calling for more direct participation in public decision-making.

It is, to be sure, very difficult to determine the level of participation if we were to use electronic voting. On the one hand, it would make it easier for some people to exercise their right to vote (especially if we used mobile or remote voting mechanisms). On the other hand, a significant proportion of the population would probably not be accustomed to dealing with electronic devices[37]. In Estonia, for example, only 15.4 percent of persons with the right to vote and 24.3 percent of participating voters gave their vote over the Internet in the last parliamentary elections (2011) — the first, by the way, in which mobile phones were used for voting[38].

Participation, however, has to be seen from perspectives other than those of the government. The implementation of electronic voting can contribute to achieving electronic democracy. Electronic voting would make informal or non-mandatory consultations easier, especially if a mobile eVoting system were adopted. Civil society would have the chance to participate actively in political processes and public decisions at local, regional, federal, and even international levels.

---

[37] This consideration will not be applicable to those countries where voting is mandatory, and in which the participation level will probably not be affected

[38] Statistics about electronic voting in Estonia can easily be found in the official web site of the Estonian National Electoral Committee, http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/

Furthermore, remote or mobile voting would enhance the participation of nationals who live abroad (in most countries it is quite a complicated process managed through embassies and consulates) because voting by mail would no longer be needed (except for remote places that might not have access to the Internet).

Mobile voting

Mobile voting, defined as the use of mobile phones for voting, further complicates the political and legal challenges. Problems of trust and confidence might increase because the process is even less "visible," except for technicians. There is also a big problem of acceptance. Figure 19 of this report shows that in countries such as Germany or the US no more than 30 percent of people would use their mobile phones to take part in elections, even if security were to be assured by the government or other public institution. In Estonia, where eVoting was implemented in 2005, it was not until parliamentary elections in 2011 that mobile phones were actually used for voting.

The use of mobile phones is of course well developed in areas such as eCommerce and eBanking. So from a technological point of view, their use in voting is certainly feasible. They are also highly flexible, which is a very helpful feature in areas such as informal public consultations, mandatory voting, and voting from abroad and in remote areas. They could, in addition, help stimulate civil society's (and especially youth) participation in elections, as well as in political decisions of special importance through consultative referendums.

For now, however, electronic voting or mobile voting could not be established as a unique way of voting; paper-based processes are still required as an alternative.

Conclusion

- Electronic voting systems could be implemented and would enhance participation in electoral processes, as well as in public consultations.

- Voting systems require a set of legal guarantees to prevent fraud, which is considered the main threat to any democratic process. Voting in democratic countries must be, at the very least, universal, free, equal, direct, and secret.

- The crucial guarantees are identity and anonymity, meaning that the person voting is the person entitled to do so (identity) and no one else can know how they have voted (anonymity). The main challenge for the implementation of eVoting is lack of trust. Public authorities must make an effort to explain how the system works from a technological point of view. At the same time, the electoral administration has to be able to control the whole process as a way of certification. Public certification is a key tool in the establishment of trust.

- Paper-based and electronic processes must coexist.

A Brief Digression: eCommerce and Identity 3.2.3

By Rocco Panetta

Although the selected use cases do not refer directly to identity systems in eCommerce, this is, nevertheless, an important identity issue – especially from a legal perspective – and will be briefly discussed in the following paragraphs.

eCommerce can boost markets and trade, improve efficiency and effectiveness (value creation), and transform business processes (value chain). Its relevance in our times, and the need to achieve a balance between technological development and the fundamental rights of individuals, has been recognized by the European Union. In fact, Directive no. 2000/31/EC on certain legal aspects of information society services (in particular electronic commerce) in the internal market was issued to establish harmonized rules aimed at ensuring transparency and information requirements for online service providers, commercial communications, electronic contracts, and the limitations of liability of intermediary service providers.

The directive enhances both administrative cooperation between member states and the role of self-regulation. Examples of services covered by the directive include online information services (such as online newspapers), online selling of products and services (books, financial services, and travel services), online advertising, professional services (lawyers, doctors, estate agents), entertainment services, and basic intermediary services (access to the Internet and transmission and hosting of information).

In addition, the proper functioning of the internal market in eCommerce is ensured by the so-called "Internal Market" clause, by means of which the information society services are, in principle, subject to the law of the member state in which the service provider is established. In turn, the member state in which the information society service is received cannot restrict incoming services.

The use of the Internet to purchase goods and services online is rather limited and mostly restricted to domestic commerce – a reflection, in part, of lack of trust in eCommerce transactions, due to fears that personal information could be stolen. Generally speaking, identity thieves misuse consumers' personal information both offline and online in the following ways:

(i) Misuse of existing accounts:
Identity thieves use victims' existing accounts, including credit card accounts, checking/savings accounts, telephone accounts (both landline and wireless services), Internet payment accounts, e-mail and other Internet accounts, and medical insurance accounts;

(ii) Opening of new accounts:
Identity thieves use victims' personal information to open new accounts, including telephone accounts (both landline and wireless services), credit card accounts, loan accounts, and checking/savings accounts;

(iii) Committing of other frauds:
In recent years, a number of member states have put programs in place to address ID theft. Such programs, which tend to have strong educational and awareness aspects, target broad audiences including consumers as well as key employees from the public and private sector and law enforcement. The challenges suggest that efforts to combat online ID theft have three key aspects:

(a) Prevention:
What stakeholders can do to lower the risk of their identities being stolen (e.g. ways to enhance identity security, ways to identify attempts and instances of identity thefts, and ways to limit the magnitude and scope of incidents);

(b) Deterrence:
What stakeholders can do to discourage parties from engaging in ID thefts (e.g. legal sanctions);

(c) Recovery and redress:
What stakeholders can do to facilitate recovery and redress of such harms as financial detriment, injury to reputation, and other non-monetary harms.

Moreover, in June 2012, the European Commission proposed new rules to enable cross-border and secure electronic transactions in Europe. The proposed regulation ensures people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available. It also creates an internal market for eSignatures and related online trust services across borders, by ensuring these services will work across borders and have the same legal status as traditional paper-based processes. This will give full effect to the major potential savings of eProcurement.

We hope that both elements of the regulation – ID and eSignatures – will create a regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities.

This will increase the effectiveness of public and private online services, eBusiness, and eCommerce in the European Union.

Implications of the Use Cases: Technological Perspective 3.2

In this section, three of our Task Force experts – Jan Zibuschka, Gisela Meister, and Achim Klabunde – discuss the technological implications of the use cases.

Zibuschka discusses technical security factors from the perspective of authentication. Meister systematically compares the security levels of the different ID management systems at issue in each use case. And Klabunde focuses on the privacy perspective.

Technical Security – Authentication 3.3.1

By Jan Zibuschka

According to the Oxford Dictionary, to authenticate means "(to) prove or show (something) to be true, genuine, or valid"[39]; in the present case to prove that a user really corresponds to a certain account, identifier, or the identity that he or she claims.

There are several well-established categories of credentials that can be used to authenticate a user, the so-called authentication factors:

- Something you know: A shared secret between user and service provider – e.g. a password, PIN, or name of parents[40] – that can be used to establish the user's authenticity.
- Something you have: A physical token, possession of which the user can prove to a service provider to establish his or her identity, e.g. a smartcard or mobile phone.
- Something you are: This group of possible authentication credentials refers to biometric properties, anatomical or behavioral characteristics that can be used to recognize and thus authenticate a user (e.g. palm vein authentication/GMAT exam).

In a concrete authentication scenario, one or several authentication credentials from at least one of those categories will be combined to reach an appropriate level of trustworthiness.

On the Web passwords are typically used, while chip and PIN is widely used in banking, representing a combination of something the user has and something he or she knows.

Palm vein authentication/GMAT exam: biometric authentication in everyday life

This use case employs biometric authentication based on the users' palm vein patterns. The specific authentication product used for the GMAT exams is Fujitsu's PalmSecure[41] technology, which claims a false accept rate of 0.00008 percent and a false reject rate of 0.01 percent[42].

Those values would indicate a very high level of reliability, but they are supplied by the vendor and do not take attacks into account.

Similar technology is reportedly also used in banks and hospitals. It is worth noting that earlier, alternative technologies including electronic fingerprinting, electronic signature, and digital image capture (two biometric methods and one token-based approach) were evaluated for the authentication process in the GMAT exam.

All in all, the approach taken is logical, as palm vein readings have several advantages over classical fingerprint biometrics. Specifically, it is not really possible to construct a dummy for impersonation purposes even if the vein pattern is used[43].

---

[39] *http://oxforddictionaries.com/definition/english/authenticate*

[40] *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204447/GPG_44_-_authentication_credentials_in_support_of_HMG_online_services_issue_1.2_May_2013_1_.pdf*

[41] *http://www.fujitsu.com/us/services/biometrics/palm-vein/palmsecure/index.html*

[42] *http://www.fujitsu.com/us/services/biometrics/palm-vein/palmsecure/index.html*

[43] *http://www.schneier.com/blog/archives/2007/08/another_biometr.html*

Unique identifier: Authority of India – Unique ID Project

The program of the Unique ID Authority of India (UIDAI) aims to produce a national database for India containing a unique identifier (AADHAAR) for each citizen, which is linked to demographic as well as biometric information. The program makes use of certified biometric devices such as fingerprint readers or iris scanners[44].

Using this system can achieve a very high level of security. The unique identifier has been linked to several biometric attributes of a user, so user authentication can be determined from various biometric properties including iris pattern and fingerprint, along with the user's knowledge of his unique identifier. All of this, moreover, can be performed under supervision by a third party (as biometric devices are needed that the concerned individuals probably cannot afford). Moreover, because the database is centralized, up-to-date information should always be available.

If the unique ID were used in isolation, authentication would be rather weak, though this usage is not part of the foreseen scenario, which is using the AADHAAR to authenticate users to banks using biometrics in the context of microcredits and micropayments[45].

Federated identity across Accounts: UK Identity Assurance Programme

In the context of federated identity management systems, authentication is typically out of scope. Rather than providing a full identity management solution for a specific use case, systems like OpenID are mainly concerned with identity transmission and assurance[46].

The UK Identity Assurance Programme (IDAP) puts concrete implementation of authentication in the hands of the identity suppliers (currently The Post Office, Cassidian, PayPal, Verizon, Digidentity, Experian, Ingeus, and Mydex[47]).

The IDAP does, however, provide an abstract discussion of authentication credentials within the system, and how they will be evaluated[48].

The so-called "inherent strength" of a credential is one aspect considered, and includes entropy as well as the exposure of the credential in the usage process. Organizational factors of the identity supplier providing the authentication credential are also considered, including fraud prevention and the quality of provisioning/management of user accounts, though these are out of scope for the present technology section.

It seems that while certain identity providers (e.g. Cassidian) can provide strong alternative factors (e.g. based on ECTC[49]), many of the accounts in the system (e.g. at Verizon or PayPal) will employ user authentication based on passwords, transmitted to a Web server via HTTPS. The framework[50] also foresees using tokens (examples given include mobile phones and utility bills, which could be employed by Verizon for example) and biometric information (examples given by the document[51] include personality and skin color).

---

[44] *http://uidai.gov.in/biometric-devices.html*

[45] *http://uidai.gov.in/aadhaar-usage.html*

[46] *http://lists.openid.net/pipermail/openid-security/2006-October/000560.html*

[47] *http://digital.cabinetoffice.gov.uk/2013/01/17/identity-beyond/*

[48] *https://www.gov.uk/government/upLevelofAssuranceds/system/upLevelofAssuranceds/attachment_data/file/204447/GPG_44_-_authentication_credentials_in_support_of_HMG_online_services_issue_1.2_May_2013_1_.pdf*

[49] *http://www.cassidian.com/de_DE/web/guest/ectc*

[50] *https://www.gov.uk/government/upLevelofAssuranceds/system/upLevelofAssuranceds/attachment_data/file/204447/GPG_44_-_authentication_credentials_in_support_of_HMG_online_services_issue_1.2_May_2013_1_.pdf*

As the examples indicate, the entropy requirements for isolated authentication credentials do not seem to be high from a purely technical viewpoint. (None of the aforementioned systems has any certification, though PayPal is working to strengthen its authentication system, for example in the FIDO alliance[52].)

Government services going mobile: eVoting on the mobile phone

The mobile phone use case is still in the proposal phase so, as in the general identity federation case, it is not entirely clear how the user will be authenticated during the individual steps of the voting process, or how the preliminary credential will be generated and transmitted to the user.

There is certainly a "physical token" aspect, as embodied by the mobile phone, the SIM card within the phone, and perhaps also future virtualized eIDs. This does not, however, answer the question how the user will authenticate to the provider of the voting credential, to the transmission channel, and, most importantly, to the mobile phone and its trusted elements.

Currently, PINs are typically used for that purpose. However, it is already becoming clear that future mobile phones will provide a higher level of security. Apple, for example, includes a fingerprint sensor in its latest model iPhone.[53] So this early phase proposal could potentially reach a very high level of authentication assurance (e.g. when combining a strong Public-Key Infrastructure [PKI] for transmission of credentials in the back end, biometrics to authenticate the user to the phone, and PIN to unlock the virtual eID after the phone has been unlocked).

Security Levels

3.3.2

By Gisela Meister

According to international OECD requirements[54], the security of ID Management systems and communications requires "the development and implementation of consistent policies to ensure the availability, confidentiality and integrity of identity data stored and exchanged by participants across private and public systems and networks."

A straightforward way of comparing the security of different ID management systems would be to apply already used and internationally agreed security metrics. Security metrics regarding so-called IAS[55] schemes, for instance, are referenced in the forthcoming EU regulation[56] and described in related EU-sponsored projects.

The scheme that has been most often applied recently is the European STORK project on cross-border interoperability of electronic identities, which is based on security levels defined by the European Network and Information Security Agency (ENISA)[57].

---

[51] *https://www.gov.uk/government/upLevelofAssuranceds/system/upLevelofAssuranceds/attachment_data/file/204447/GPG_44_-_authentication_credentials_in_support_of_HMG_online_services_issue_1.2_May_2013_1_.pdf*

[52] *http://www.fidoalliance.org/members.html*

[53] *http://9to5mac.com/2013/07/29/new-iphone-with-biometric-fingerprint-sensor-seemingly-confirmed-by-ios-leak/*

[54] *Ensuring Security, OECD , DSTI/ICCP/REG(2008)*

[55] *http://www.cassidian.com/de_DE/web/guest/ectc*

[56] *EU Regulation Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market/* COM/2012/0238 final – 2012/0146 (COD)*/*

[57] *Mapping security services to authentication levels, Reflecting on STORK QAA levels, European Network and Information Security Agency*

A forthcoming EU project, "Future ID," describes security levels for an ID platform on an implementation-oriented basis.

In contrast, international IT security standards as described in the IT Security Standards by the International Organization for Standardization (ISO/IEC)[58] can be applied on a more generic and use-case-independent basis.

The objective of this section is to describe and compare the security of the four use cases in this document by means of an underlying comparison scheme, or metric, that will help validate the ID schemes, and compare their security (by means of the linked metric).

For our purposes, and for more granular comparison, this security metric should consist of several security levels, which are both implementation neutral as well as token-based neutral.

We will focus on the ISO/IEC security metric, which is generic as well as token- and use-case-independent. An exhaustive description and several use cases are described in the IT security standard "Information technology – Security techniques – Entity authentication assurance framework,"[59] for which we will provide a suitable extract in the next section.

Other security metrics as defined by the STORK EU project[60] or the forthcoming Future ID EU project may be taken into account in further analysis, based on a more granular approach.

In the following we will adopt the terminology of international and European IT Security Standards (see also Terminology box for definitions).

---

[58] *ISO/IEC 18014-2, ISO/IEC 7498-2, IT Security Standard, IT Security Standard and Information Technology – Security techniques – Entity authentication assurance framework, ISO/IEC FDIS 29115, IT Security Standard, 2012; ISO/IEC = International organization for standardization, the European counterpart is CEN = European Committee for standardization, and on a national basis; for example for Germany the mirror organization is DIN = Deutsches Institut für Normung*

[59] *ISO/IEC FDIS 29115 (2012)*

[60] *Secure Identity Across Borders Linked Grant agreement (STORK) no.: 224993, "D2.3 – Quality authenticator scheme," February 27, 2009*

Terminology

Authentication

- The "Provision of assurance in the claimed identity of an entity"[61] or
- The verification that an entity is the claimed one[62].

Identification

- The unique association of a set of descriptive parameters to an individuum within a given context[63]
- The process of recognizing an entity in a particular domain as distinct from other entities[64]

Security metric (Level of Assurance 1 – Level of Assurance 4) for entity authentication assurance, see *IT security standard "Information technology – Security techniques – Entity authentication assurance framework"*[65]

- Level of Assurance 1: There is minimal confidence in the claimed or asserted identity of the entity, but some confidence that the entity is the same over consecutive authentication events.
- Level of Assurance 2: There is some confidence in the claimed or asserted identity of the entity.
- Level of Assurance 3: There is high confidence in the claimed or asserted identity of the entity.
- Level of Assurance 4: There is very high confidence in the claimed or asserted identity of the entity.

[61] *ISO/IEC 18014-2, IT Security Standard*
[62] *ISO/IEC 7498-2, IT Security Standard; Application Interface for Secure Signature Creation Devices, CEN EN 14890, European Standard, 2011*
[63] *ISO/IEC 7498-2, IT Security Standard*
[64] *ISO/IEC 18014-2, IT Security Standard*
[65] *ISO/IEC FDIS 29115 (2012)*

According to IT security standard "Information technology – Security techniques – Entity authentication assurance framework"[66] at **Level of Assurance 1**, there is minimal confidence in the claimed or asserted identity of the entity, but some confidence that the entity is the same over consecutive authentication events. This level does not require the use of cryptographic authentication methods (e.g., cryptographic-based challenge-response protocol).

At **Level of Assurance 2**, there is some confidence in the claimed or asserted identity of the entity. Single-factor authentication is acceptable. Successful authentication is dependent upon the entity proving, through a secure authentication protocol (e.g., cryptographic-based challenge-response protocol), that the entity has control of the credential.

At **Level of Assurance 3**, there is high confidence in the claimed or asserted identity of the entity. This Level of Assurance employs multifactor authentication — at least two-factor authentication; claim of the credential by knowledge (PIN, for example) and by possession (secure authentication protocol).

At **Level of Assurance 4,** there is very high confidence in the claimed or asserted identity of the entity. This requires the use of tamper-resistant hardware devices for the storage of all secret or private cryptographic keys.

Additionally, all sensitive data included in authentication protocols are cryptographically protected, both in transit and at rest. At Level of Assurance 4, digital certificates (e.g., X.509, card-verifiable (CV) certificates) may be used to authenticate devices connected to a network of laptops, mobile phones, printers, fax machines, and other devices.

Selection of the appropriate level of assurance should be based on a risk assessment of the transactions or services for which the entities will be authenticated.

By mapping impact levels to levels of assurance, parties to an authentication transaction can determine what level of assurance they require and can procure services and place reliance on assured identities accordingly.

Mapping security levels to use cases

We introduced security levels in the previous section. We will now link this abstract classification to our four real-world use cases. The use cases are classified according to their "trustworthy" properties in ***Fig. 19***.

[66] *ISO/IEC FDIS 29115 (2012)*

THE USE CASES ARE CLASSIFIED REGARDING THE FOLLOWING CRITERIA

Use cases	Federal ID/ decentralized token-based ID	Identification/ authentication method	Technology scale	Security level
1. Palm vein authentication/ GMAT exam	Federal	Biometric authentication additional token-based authentication	Independent two-factor personal authentication with cryptographic protocol	LoA 3
2. UK Identity Assurance Programme	Federal	Password-based e.g. PayPal	Single-factor software token authentication	LoA 2
3. Remote eVoting on mobile phones	Token based	Hardware-based device authentication with E2E secure channel	Highly secure two-factor authentication, sensitive data are cryptographically protected	LoA 4
4. Indian eID program	Centralized	Software based on a unique ID number	No cryptographic protocol authentication based on ID	LoA 1

Fig. 19
Use Case Classification Criteria
Our four use cases are described by type and ranked according to authentication method, scale of technology used, and security level.

1. Palm vein authentication/GMAT exam in the US

Security concerns: One of the main objectives of the General Management Admission Council (the educational corporation that administers the GMAT exam) is to make sure that the person who is attending the program is undoubtedly the person whose scores are received.

1. Identity: In order to achieve this objective, GMAT has invested in technological security, adopting so-called "palm vein technology" in all its test centers worldwide.

The following additional security measures or restrictions are assumed:

2. Authentication is token-based in regard to the storage of biometric reference data, necessitating a two-factor authentication process.
3. The token does not necessarily consist of tamper-resistant hardware[67].

The resulting security level (with additional assumptions) = Level of Assurance 3 (see Terminology box).

2. The program of the Unique ID Authority of India

Security concerns: Use of a single identifier together with a single, centralized database. The UIDAI is insistent on the limited amount of information at issue, which will be used solely for authentication of identity. There are no cryptographic authentication methods (e.g. no cryptographic-based challenge-response protocol is required or further means of authentication, e.g. possession). The only authentication factor is knowledge-based, a unique ID.

[67] *If the token consists of tamper-resistant hardware, e.g. by means of a secured smart card, then the Level of Assurance 3 is to be replaced by Level of Assurance 4*

The resulting security level (with additional assumptions) = Level of Assurance 1 (see Terminology box).

3. UK Identity Assurance Programme

Security concerns: The UK Identity Assurance Programme aims to provide a single point of access system (SPOC) for people to sign into the gov.uk website that is being developed as a portal for all online government services, from welfare benefit applications to car tax, passports, and student loans. It is assumed that single software-token-based authentication will be performed through a secure authentication protocol (e.g., cryptographic-based, challenge-response protocol). The token is software based; in other words, it does not consist of tamper-resistant hardware.

The resulting security level (with additional assumptions) = Level of Assurance 2 (see Terminology box).

4. eVoting on mobile phone

Security concerns: In the case of contactless cards, Near Field Communication (NFC) capable mobile phones with secured display and keypad will soon serve as trustworthy readers for eID cards or for virtualized eID cards.

The mobile phone and ID card will constitute the vote-casting device, whereby the mobile phone is connected to the network via, for example, OTA (over-the-air) services or WLAN. The underlying authentication is a two-factor authentication by both PIN and a challenge response protocol to prove that the user is, for example, over the age of 18, and lives in a certain region or city.

The following additional security measures or restrictions are assumed: all sensitive data included in the authentication protocols are cryptographically protected in transit and at rest, and the sensitive data are stored in a "secure element," e.g. a SIM card inside the mobile phone, which would consist of tamper-resistant hardware[68].

The resulting security level (with additional assumptions) = Level of Assurance 4 (see Terminology box).

Conclusion

As stated above, the appropriate security level reflects how much security is required by the use cases; in other words, can they procure services and rely on assured identities? For further study, the mapping may be enhanced by using a different security metric, e.g. the metrics used by the EU STORK or the Future ID project.

---

[68] *If the mobile phone does not use secure elements for the storage of sensitive data, if for example it relies on a trusted execution environment, then the Level of Assurance 4 is to be replaced by Level of Assurance 3*

Privacy by Design in Identity Management

3.3.3

By Achim Klabunde

The implementation of technical solutions that guarantee on the one hand time-secure and effective identity assurance and on the other hand the respect for the fundamental right of privacy requires an operational and functional interpretation of both basic concepts. Their philosophical, social, and legal foundations are developed in previous chapters of this publication. Their technical implementation needs to take account of the conditions and mechanisms of the online economy.

Rocco Panetta's contribution to this publication illustrates the enormous importance that reliable, trustworthy, and effective identity services are expected to have for online businesses. Secure, effective, and privacy-preserving identity management systems are seen as key enablers of more complex, more critical, and higher value online commercial transactions, as well as public sector services. The potential privacy implications related to this function have been the subject of extensive research and analysis. The central role of identity service providers in online transactions could enable them to collect detailed and comprehensive data about the life and behavior of their users. Comprehensive and effective privacy safeguards must be part of identity assurance solutions. In line with the principles defined by the legal frameworks, they must be implemented through organizational and technical measures. In regard to technology, which is the concern of this section, the principles of Privacy by Design (see *Culture of Privacy: Privacy by Design* box on page 17 for definition) and Privacy by Default define an approach to implementing new systems where privacy is considered from the very beginning of development and where the more privacy-friendly solution is offered to the user as the first option.

Implementing a system according to the principle of Privacy by Design requires the analysis of privacy issues from the first phases of the development process. Data protection authorities recommend performing a privacy or data protection impact assessment (PIA/DPIA)[69] as one of the first steps of a new project. The PIA will identify the risks to privacy and help find mitigating measures and safeguards. Unlike a security risk assessment, where the potential damage to the assets and interests of the organization operating the system is the key driver, these risks are only secondary in a privacy impact assessment. The primary impacts assessed in a PIA concern the privacy, reputation, and other rights and legitimate interests of the individuals whose data is processed in the system. It is important that this difference in perspective is understood when a PIA is performed, to avoid concentrating on the indirect effects of a privacy violation on the interests of the system operator, e.g. financial damages claimed or reputational impact.

In order to translate privacy safeguards' functional and non-functional requirements for a technical system, an operational understanding of privacy is required. Most English-language dictionaries[70] agree on two meanings of the word "privacy": the first refers to a state of seclusion, physical separation from others, and the second concerns freedom from unwanted intrusion or disturbance in one's private life. The second meaning is the foundation for considerations of privacy in the context of individuals' rights. This was reflected in the 1890 article by Warren and

[69] *PIA project, http://www.piafproject.eu/*

[70] *C.f. i.a. http://www.merriam-webster.com/dictionary/privacy; http://oxforddictionaries.com/definition/english/privacy; http://dictionary.cambridge.org/dictionary/british/privacy*

Brandeis[71], which is often considered the first publication arguing that a legal right to privacy exists (under US law). The right to privacy (or private life) was later codified in legal instruments, e.g. the European Convention on Human Rights[72].

The social concept of privacy has developed since then. In his contribution to this publication,[73] Travis Hall introduced Helen Nissenbaum's notion of privacy as contextual integrity, requiring "appropriate information flows" rather than absolute restriction of information exchange.

In the legal domain, the German Federal Constitutional Court developed the idea of a right to "informational self-determination" from the general personality right in its 1983 landmark decision on a census law, which also puts an individual in a position of controlling which information about him is shared with whom, at what time, and for which purpose.

The technical consequences of these privacy requirements have already been considered in many research and development publications on identity systems. *The Laws of Identity* by Kim Cameron[74] contains privacy-preserving elements such as user control and consent (legality and transparency), minimal disclosure, and justifiable parties (data minimization). The requirements for privacy and identity have been further developed in European research projects, such as Prime[75], PrimeLife[76], and ABC4trust[77], as well as by work in the US[78] and Canada[79].

Some of the research projects also develop concrete requirements and possible technical solutions for the privacy-related features of identity systems. Nevertheless, in real-world implementations, additional conditions resulting from the context, the concrete application and purposes, and other aspects need to be taken into account and require thorough analysis of each case.

This can be illustrated to some extent for the use cases considered in this publication, even though a full analysis of each use case is beyond the possibilities of the current exercise.

Palm vein authentication/GMAT exam in the US

As an identity system, the Graduate Management Admissions Test (GMAT) system is well defined in regard to both function and the range of parties involved. Its main purpose is to ensure the legitimacy of the person who registered for the exams, and to reassure educational institutions and programs that they are granting access and support to persons whose ability, as defined by the tests, is certified by the Graduate Management Admission Council (GMAC).

These institutions may use other systems to establish the identity of potential participants. But one of GMAC's roles is that of an identity service provider, as it confirms properties of the individuals (test results) towards third parties (the educational institutions).

From a privacy perspective, the use of biometric methods is always creating particular privacy concerns. Unlike other credentials such as passwords or key cards, biometric characteristics are in principle inseparably and unchangeably related to an individual for his entire life. Palm

---

[71] *S. D. Warren, L. Brandeis; The Right to Privacy, in Harvard Law Review, Vol. IV, December 15, 1890, No. 5*

[72] *ECHR, Article 8*

[73] *See Travis Hall, p. 32*

[74] *Kim Cameron, The Laws of Identity, 2005, Microsoft, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf*

[75] *J. Camenisch, et al.; Privacy and Identity Management for Everyone. In ACM DIM 2005.*

[76] *K. Storf, et al.; Requirements and concepts for identity management throughout life, PrimeLife Deliverable H1.3.5*

vein pattern recognition technology as employed by GMAC has some advantages over other biometric technologies. In contrast to fingerprinting, for example, palm vein patterns are rarely used in other contexts. Furthermore, unlike dactyloscopic (fingerprinting) data, palm vein data has limited use in investigations in general, as unlike fingerprints palm veins do not leave traces on surfaces. Thus, purpose limitation is implicit in the choice of this biometric technology and later "function creep," as in other cases[80], is unlikely.

AADHAAR – Unique Identification Authority of India (UIDAI)

The political justifications for the AADHAAR project, which intends to issue a unique 12-digit identification number to each of the 1.2 billion residents of India, is to provide a basis for the inclusion of all Indian citizens in the administrative and economic system, and especially for participation in government support programs and to obtain benefits.

The system is intended help to overcome the shortcomings of the previously used systems and documents, none of which is considered sufficiently trustworthy and reliable, e.g. as some individuals are in possession of multiple identification documents, enabling them to participate in programs more than once, while, on the other hand, many residents have no or no individual ID documents, or are only registered as part of a family, so that they cannot prove their entitlement and receive no benefits.

The potential value of a database holding the fingerprints of more than a billion individuals would create a case for strong privacy safeguards. The basic design of the system's authentication interface, which will only confirm or deny a claimed identity and never provides any of the collected data, is in principle privacy friendly. But it is difficult to assess if the implementation of this design and the privacy safeguards of the entire system hold this promise, due to its complex structure.

It could be a challenge for the operating authority to ensure proper implementation of safeguards at all levels given that it is relying on private providers for many services, including for the operation of the CIDR, enrolment, authentication service agencies, and authentication user agencies. This dependence has been the subject of criticism.

Other controversies concern the legal status of the project, as the law establishing the system appears to have been pending in the Indian parliament since 2010 due to concerns expressed by the responsible committee. It should be noted that the law would provide some privacy safeguards, but it also allows disclosure of data on the basis of court orders or for national security reasons.

Regarding the operation of the system itself, it has been noted that an electronic know-your-customer (e-KYC) function has been implemented, transferring customer data from the AADHAAR system to the service point, which appears to be contrary to the simple Yes or No restriction in an authentication request.

---

[77] *J. Camenisch, et al.; Architecture for Attribute-based Credential Technologies; ABC4Trust D2.1*

[78] *Schwartz, Cooper, Hansen; Privacy and Identity Management; in IEEE Security & Privacy, March/April 2008*

[79] *A. Cavoukian, Privacy in the Clouds: Privacy and Digital Identity – Implications for the Internet; Information & Privacy Commissioner, Ontario, Canada, 2008*

[80] *EDPS opinion on EuroDAC proposal*

UK Identity Assurance Programme

In June 2013, the UK Cabinet Office published draft privacy principles for the UK Identity Assurance Programme[81], thereby opening a public consultation with a deadline of September 2013.

The principles had been prepared in consultation with a special advisory group, including privacy and consumer advocate organizations. The nine draft principles include elements from the laws of identity as well as data protection principles.

User Control
• Identity assurance activities can only take place if I consent or approve them

Transparency
• Identity assurance can only take place in ways I understand and when I am fully informed

Multiplicity
• I can use and choose as many different identifiers or identity providers as I want to

Data Minimization
• My request or transaction only uses the minimum data that is necessary to meet my needs

Data Quality
• I choose when to update my records

Service-User Access
• I have to be provided with copies of all of my data on request; I and Portability can move/ remove my data whenever I want

Governance/Certification
• I can have confidence in any identity assurance system because all the participants have to be accredited

Problem Resolution
• If there is a problem I know there is an independent arbiter who can find a solution

Exceptional Circumstances
• Any exception has to be approved by Parliament and is subject to independent scrutiny

The principles and the process for their adoption will be seen as part of a process to increase trust in the forthcoming framework. The outcome of the consultation will be an indicator of how far this objective can be achieved. Some need for improvements was indicated by a survey in summer 2013[82], which showed that UK citizens had high trust in the government scheme, but low confidence in the expected private parties involved in it. The final form and implementation

[81] *https://www.gov.uk/government/consultations/draft-identity-assurance-principles*
[82] *http://www.theguardian.com/public-leaders-network/2013/jul/22/government-identity-platform-private-sector*

of principle 7 (governance/certification) and the degree of transparency and credibility of the related process could be of crucial importance for the acceptance of the scheme.

Mobile eVoting

Voting systems have to comply with somewhat contradictory requirements. On the one hand, each voter must be identified and authenticated before he or she may cast a vote, and the vote must be collected so that it cannot be changed. On the other hand, the anonymity of the voter must be preserved as regards the substance of the vote.

In physical presence voting, these requirements are met by keeping track of voters in the register and collecting all ballot papers separate from any identifying element in a ballot box where they are secure from tampering or premature reading. The voting laws usually determine that a ballot paper that has been made identifiable by the voter (e.g. by signing it) must be considered invalid and must not be counted.

The design of this physical voting process allows observers to follow the entire voting process in a polling station and thus detect any irregularities, such as voters casting multiple votes or any tampering with the ballot box. Any citizen can make this observation, without any technical education or special background[83].

Existing electronic voting systems, usually used in similar processes as paper voting, have already been criticized for problems in their implementation[84] that prevent the same level of observation and assurance. While sophisticated mechanisms allow the separation of the secret vote and the documentation of the participation of a voter in a secure and tamper-proof way, the processes in the electronic devices are not accessible to direct observation and cannot be assessed without specialist knowledge.

Therefore, even a technically perfect electronic voting system could not ensure that an ordinary citizen would be convinced that no tampering has occurred during the election. This is even more the case for mobile systems, where observation would be even more difficult. Due to these risks, mobile eVoting systems should only be operated in environments where voters' trust in the organization conducting the vote is high and where there is little risk of interference or tampering, in particular for non-binding consultations etc. For votes of great importance, e.g. legislative elections, maintaining the credibility of the process is of fundamental importance.

Conclusion

Each of the use cases demonstrates a different perspective on the privacy issues related to identity services and a different technological environment for the design and implementation of privacy-friendly solutions. In order for Privacy by Design to become a standard engineering approach, methodologies must be developed to identify and address the privacy challenges across a wide variety of contexts.

---

[83] *http://www.welt.de/politik/Article3691578/Wie-vor-20-Jahren-das-Ende-der-DDR-begann.html*

[84] *M. Bishop, D. Wagner; Risks of eVoting, in: Communications of the ACM, November 2007, Vol. 50, No. 11*

CONCLUSION

4.

The digital age has transformed our social relationships and thus our identities. Within just a few years we have witnessed the multiplication of personal identities in different social contexts to an extent inconceivable in the offline world. At the same time, the practice of profiling users has made it possible to identify people without any specific, personally identifiable information. At the core of these new dynamics is information and its management; information that differs by reason of its sensitivity, economic value, quality, and nature, as recognized by both data protection laws and by case law.

The large amount of data collected by private and public entities for different purposes and the diverse nature of this information induce us to reflect not only on the usefulness of these new technologies, but also on their risks. Indeed, the law, which in many countries provides specific guarantees in relation to the collection and processing of personal data, requires us to do so. And it is also necessary in the interests of boosting a digital economy largely based on services that make massive use of personal information.

Identity is the *fil rouge* that holds together the different pieces of our digital lives, connecting our credit card purchases, our access to reserved areas, our use of public services, and much more. At the same time, identity also offers a powerful means of controlling people and tracking their activities (consider, for example, the Panopticon of Jeremy Bentham as an analogy)[85]; hence Johanna Sprondel's call for "an equilibrium of trust" as a condition for identity in the online world.

Gisela Meister suggested a systematic approach to determining levels of security across our four use cases, while Jan Zibuschka evaluated their authentication procedures. None emerges from this investigation as a "winner" – but picking winners was never the intention of this publication. We sought, rather, to show the range of innovation possibilities by describing real-life initiatives to manage identity, and analyzing both the positive and negative aspects of their aims and likely outcomes. It is, however, clear that building public trust and confidence in identity management innovations – with the users' perspective in the center – will be a struggle.

The report has exposed wide regional (and cultural) differences in attitude toward the key issues of privacy and security. One size will plainly not fit all. Yet end users everywhere demand convenience of access. The challenge for service providers – both public and private – will be to balance that universal requirement with a diversity of local differences. A tall order, especially since, as Travis Hall points out, "the relative easing of access for some, even if access does not change for others, can be discriminatory."

Service providers will also be challenged to convince end users that innovations are in their best interests. The report makes clear that high security standards will not be sufficient to allay concerns. When it comes to eVoting, for example, Jorge Villarino believes that paper-based and electronic processes must continue to co-exist. And Rocco Panetta's reflections on eCommerce underscore the critical role of policymakers and legislation.

---

[85] *Jeremy Bentham's Panopticon allowed a watchman to observe all occupants of an institution without their knowledge*

Moreover, as Achim Klabunde and other Task Force experts observe, the principles of Privacy by Design will need to be incorporated into ongoing innovations from the very first. The report also suggests that end user concerns about privacy and data protection are unlikely to diminish – to the contrary. More and more information is being shared between public and private sectors; and the increasing availability of Big Data analytics, coupled with the spread of eGovernment and eDemocracy projects, will raise new questions as well as highlighting old ones.

We still believe, however, that identity management in the digital age can be made both secure and convenient from the end user's perspective – despite the scale of the challenges in regard to the fair and democratic use of personal information. End users themselves will need to take responsibility, educating themselves about the issues raised by identity management innovations, their consequences – and opportunities.

Meanwhile, those providing such services will need to limit the risks to privacy if they are to maximize the opportunities that innovation brings. As Alessandro Mantelero summarizes the challenge: there is an overall need to "balance the development of useful devices and technologies with respect for legal requirements, fundamental rights, and informational self-determination."

Our use case choices were, of course, subjective; but as the expert comments make clear, by expressing a wide diversity of views, the Task Force participants have opened up a lively (and very timely) debate. We hope that this debate, and the challenges and opportunities it highlights, will make a major contribution to the broader public discussion.

TASK FORCE PARTICIPANTS

Hans-Jörg Frey

"Personal life and economic activities rapidly transfer into the online world. As a result, also the subject 'identity' gets a whole new meaning because it regulates the interaction of users, the economy, and the Government."

Hans-Jörg Frey has more than 18 years of experience in the IT and communication industry. He has worked with globally active companies such as Grundig AG, Siemens AG, BenQ Mobile GmbH, EPCOS AG, and Giesecke & Devrient GmbH. For the past 12 years, he has worked in various positions in product and portfolio management and successfully launched numerous products in the market. Some of these were launched in the course of major projects which were carried out in cooperation with Nokia and RIM. In 2008, Hans-Jörg Frey joined Giesecke & Devrient as a senior product manager. His areas of responsibility included authentication products for online banking applications and now applications for payment cards. Trend analysis and the thus resulting end customers' requirements taking into consideration the technical feasibility are some areas of Hans-Jörg Frey's expertise, with which he has contributed to numerous market studies within as well as outside the company. He holds degrees in Electronic Engineering and in Industrial Management.

Travis Rudolf Hall

"Identification is a foundational problem of governance, and is of increasing concern to the private sector. Identification technologies act as the mediators of the relationship between an individual and institutions over time and across contexts, and how they are designed affects and is affected by the nature of that relationship."

Travis Hall is a Visiting Researcher at the Humboldt Institute for Internet and Society, Berlin, Germany

- PhD in Media, Culture, and Communication, ABD, New York University, Dissertation Title: "Measured Life: Bureaucracy, Bodies, and Biometrics," Committee: Helen Nissenbaum, Benjamin Kafka, John Torpey (Spring 2013)
- IEEE Certified Biometrics Professional (Spring 2012)
- MA in International Communications (Summer 2003, American University)
- BA in International Relations with honors, summa cum laude (Spring 2002, American University)
- Research Assistant for Helen Nissenbaum (Spring 2012), New York University, conducted research on the FBI's Next Generation Identification project and the Department of Homeland Security's Secure Communities project, provided technical and policy expertise on biometric systems to immigrant and privacy rights advocates, attended various workshops and events on US government biometrics programs, presented findings to FBI's Advisory Policy Board and MURI Project Review team

Achim Klabunde

"Mathematically, identity seems to be a simple concept. However, in the real world, we interact in different social contexts and we need to control what we disclose about ourselves to whom and when to preserve our freedom. For technical identity systems, modeling this human requirement could still be a challenge."

Achim Klabunde is Head of Sector IT Policy at EDPS (European Data Protection Supervisor). He has been leading the IT competence team at the European Data Protection Supervisor since April 2012. From 2002 to 2012 he worked for the European Commission on issues related to trust, security, data protection, and privacy in regulatory and policy functions, e.g. regarding telecoms legislation or eGovernment. Before joining the EU administration, Achim Klabunde worked in the private sector as project manager and software engineer and gained experience in areas such as database design, network management, and business process reengineering. He holds a diploma from Bonn University where he studied informatics and communications research.

Alessandro Mantelero

"In the age of Big Data, innovative methods of analyzing large datasets lead to a wider reflection on identity management systems. How to balance the role of government and private sector in shaping future authentication systems? How to guarantee an adequate level of data protection and of anonymity?"

Alessandro Mantelero is Professor of Private Law at Politecnico di Torino (Department of Management and Production Engineering) and Faculty Fellow at Nexa Center for Internet and Society. Alessandro Mantelero graduated cum laude in Law at the University of Turin in 1998, with a PhD in Civil Law from the same university. He is author of numerous publications and is currently focusing his studies on data protection, ISP liability, and legal implications of cloud computing and Big Data. Alessandro Mantelero was admitted to the Italian bar in 2001. He is involved in different national and international research programs, is Project Member at the Network of Excellence in Internet Science and co-director of the Cloud Computing Governance Initiative for the Nexa Center. The Cloud Computing Governance Initiative was launched by the Berkman Center (Harvard University) and involves the following universities and research centers: Harvard University (Berkman Center), Politecnico di Torino (Nexa Center), Keio University, and University of St. Gallen. In 2012 he was Visiting Researcher at Berkman Center for Internet and Society at Harvard University.

Gisela Meister

"State-of-the-art smart cards as electronic identity (eID) cards can already be used for a visual and electronic verification of the citizen´s identity. Their electronic interface provides technical interoperability as well as privacy protection. The use of such eIDs as representatives of personal identity should be discussed from social and economic perspectives."

Gisela Meister is G&D's Standardization Director, coordinating all standardization activities within G&D. She is also the Head of R&D's Technology Consulting Department, which includes the responsibility for G&D's security evaluation projects. Gisela Meister has been employed with G&D since the end of 1989. She chairs the European standardization working group for digital signature applications on smart cards and actively contributed as Task Force Convenor to the development and harmonization of the European Citizen Card Technical Standard within CEN. Since 1994, Gisela Meister has been a member of the DIN national committee on Card Standardization and since 2006 she has been chairing the technical committee NIA 17.4 and acts as head of the German delegation of its international mirror technical committee within ISO/IEC. Gisela Meister has degrees in mathematics and economics from the University of Münster, received the SIT Fraunhofer Smart Card prize 2004, and is a member of several program committees regarding smart cards and security aspects, such as the BSI IT-Sicherheitskongress in Bonn, the Fraunhofer Smart Card Workshop in Darmstadt, the Chip to Cloud Conference in Nice, and the ID World symposia in Frankfurt.

Rocco Panetta

"Since the adoption of the Data Protection Directive (1995), the ability of organizations to collect, store, and process personal data has increased. Identity management systems are now widely used on the Internet, and they increase the need to protect the user's identity. In this context, self-protection gains in importance beside EU and national regulations. In other words: never enter your real data!"

Rocco Panetta is Managing Partner at Panetta & Associati. He is a commercial and regulatory lawyer specialized in TMT, Energy, Infrastructures, and Environmental Law. Former Head of Legal Department at the Italian Data Protection Authority and Italian Representative for the Art.29 WP at the EU Commission, he has extensive experience in private practice assisting both domestic and multinational corporations. Rocco Panetta has acquired significant and noteworthy experience in the TMT field since the start of the IT/Telecom revolution in the nineties. Previously appointed Secretary General, he has served as member of the Italian Environmental Impact Assessment Commission. Professional Memberships: Italian and Rome Bar Association; Advisory Board of the IAPP, York, USA; Advisory Board of the IEL, Dallas, USA; Scientific Committee of the IIP, Rome, Italy. Career: Ughi & Nunziante 1996–1999; Baker & McKenzie 1999–2001; Italian DPA 2001–2007; Environmental Impact Assessment Italian Commission Secretary General and

then Commissioner 2007–2011; Partner Panetta & Associati 2008 to date. Publications: editor of the Code of Renewable Energy 2010 and author of more than one hundred publications such as books and articles on telecoms, energy and the environment, and privacy law.

Johanna Sprondel

"According to John Locke's statement (dating back to 1689) in 'Essay Concerning Human Understanding' Book II Chapter XXVII entitled 'On Identity and Diversity' identity (the self) is defined as being the same person to the extent that we are conscious of our past and future thoughts and actions in the same way as we are conscious of our present thoughts and actions. Quite an idea when we take it to court in the digital age, 24/7 and around the globe online, no?"

Johanna Sprondel is currently a Visiting Scholar at Stanford University. Johanna Sprondel, born 1980, studied philosophy, political science, and comparative literature at the Universities of Freiburg, Zurich, Basel, and Strasbourg. She obtained her PhD in 2011 with a dissertation on the topic of myths in philosophy, literature, and history. She was a visiting scholar at the Zurich James Joyce Foundation and the DHI and is currently working as a postdoctoral researcher at the DFG Research Training Group Multilevel Constitutionalism at Humboldt-University, Berlin. Her current research focuses on the impact of digital media on the humanities. In 2013 she will work as a visiting researcher at Stanford University on her habilitation: "Hermeneutics 2.0 – Encounters of Experience and Comprehension in the Digital Age."

Jorge Villarino

"In a global and electronic world, digital identity has become one of the most important challenges for legislators around the world. If we do not establish an appropriate legal framework it might became a significant barrier for economic development, not just in the IT sector but in all economic branches. One of the main reasons for the data protection reform in the European Union has been consumers' lack of trust in the digital environment. Therefore an appropriate legal framework has become a main challenge to overcome this barrier. Privacy and security are major concerns for consumers and should also be the core objective of the legislators. Otherwise, economic development will not take advantage of IT improvements."

Jorge Villarino has a Law degree from the University of Saragossa (Spain). He has completed the Leadership Program for Public Management (IESE Business School) and the Executive Management Program for Executives (IE Business School). He has been working at the Spanish Senate for the last nine years, and now works as a Legal Advisor in the Justice Committee of the Spanish Parliament, where he is also the Director for International Relations. From an academic point of view, he has been working for the last four years as a PhD candidate at the University Abat Oliva

CEU (Barcelona, Spain) on a dissertation about the legal aspects of cloud computing and its impact on the right to privacy and freedom of expression. He teaches Internet Law in the International University of La Rioja (Spain). He has also taught several courses and seminars about Internet law (eCommerce, data protection, freedom of speech, cloud computing, intellectual and industrial property, and Privacy by Design), in public and private institutions such as the Madrid Bar Association, the Saragossa Bar Association, several domestic and international universities, the Spanish Chapter of the International Association of Software Architects (IASA), and Microsoft, among many others. He participated as a keynote speaker on Internet Governance in the last annual session of the American Society of International Law in Washington D.C. He is also a member of the Academic Council (Advisory Board) of Syntagma, Centro de Estudios Estratégicos [Center for Strategic Studies (www.syntagma.org)], where he has been working very closely with Professor García Mexía, one of the main Spanish experts in Internet Law.

Jan Zibuschka

"To be called user-centric, an identity management system should at least take users' preferences regarding IdM systems into account. IdM systems should also provide the highest feasible level of effectiveness with regard to security and privacy. Neither practical effectiveness of IdM systems nor stakeholders' preferences have been researched extensively."

Jan Zibuschka is a senior researcher at Fraunhofer IAO, Stuttgart. Jan Zibuschka has a long track record in both applied and basic interdisciplinary research in the identty management field, with a special focus on identity intermediation. He has participated in several national and international research projects dealing with security and privacy, such as the FP ICT projects PRIME, PrimeLife, and FIDIS. He has published in several relevant areas, including the design of market-compliant solutions for privacy-friendly intermediaries in location-based services and cost-efficient approaches for web identity management and single sign-on, as well as innovation management, civil security, and technology management. He currently pursues his interests in the German national project SkIDentity, aiming to build a viable intermediary infrastructure linking the German eID to cloud services. He also disseminates his findings in the European thematic network SSEDIC, shaping the research agenda for the future European eID. Jan Zibuschka is employed as Senior Researcher and Project Lead at Fraunhofer IAO, Stuttgart, where he is work package leader in the national SkIDentity project. Additionally, he is a deliverable leader in the EU-funded SECUR-ED project, and does industry consulting work in the security/privacy space. Currently, he is a visiting researcher at Norsk Regnesentral, Oslo, in the PetWeb 2 project. He is working on finishing his dissertation and tries to find time for identity-management-related research activities where he can.

SELECTED BIBLIOGRAPHY

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, 8 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

Barnard-Wills, David. Surveillance and Identity: Discourse, Subjectivity and the State. Farnham; Burlington, VT: Ashgate, 2012. Bygrave, Lee. Data protection law: approaching its rationale, logic and limits. The Hague; New York: Kluwer Law International, 2002.

Camenisch, Jan, et al. Privacy and Identity Management for Everyone. ACM DIM 2005.

Cave, J. et al. (Ed.) Data protection review: impact on EU innovation and competitiveness. Luxembourg: Publications Office, 2012 http://dx.publications.europa.eu/10.2861/87915.

Council of Europe, Committee of Ministers: Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for eVoting (Adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies).

Cavoukian, Ann. Privacy in the Clouds: Privacy and Digital Identity – Implications for the Internet. Information & Privacy Commissioner, Ontario, Canada, 2008.

Dudley-Jenkins, Laura. Identity and Identification in India: Defining the Disadvantaged. London; New York: Routledge Curzon, 2003.

Gates, Kelly. Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. Critical Cultural Communication. New York: New York University Press, 2011.

Gutwirth, Serge. Leenes, Ronald. De Hert, Paul. Poullet, Yves (Eds.) European Data Protection: Coming of Age. Dordrecht: Springer, 2013.

Lyon, David. Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. London; New York: Routledge, 2003.

Magnet, Shoshana. When Biometrics Fail: Gender, Race, and the Technology of Identity. Durham: Duke University Press, 2011. Nissenbaum, Helen; Brunton, Flynn. "Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation." First Monday 16, no. 5 (2011).

Nissenbaum, Helen Fay. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, Calif.: Stanford Law Books, 2010.

Schaar, Peter. Privacy by Design. (2010) 3(2) Identity in the Information Society 267-274.

Schwartz, Cooper, Hansen. Privacy and Identity Management. IEEE Security & Privacy, March/April 2008.

Solove, Daniel J. Schwartz, Paul M. Information privacy law. New York: Wolters Kluwer Law & Business, 2011.

Solove, Daniel J. Nothing to hide: the false tradeoff between privacy and security. New Haven [Conn.]: Yale University Press, 2011.

Solove, Daniel J. Understanding privacy. Cambridge, MA.; London: Harvard University Press, 2008.

Szreter, Simon. "The Right of Registration: Development, Identity Registration, and Social Security – a Historical Perspective." World Development 35, no. 1 (2007): 67-86. Stutzman, Woodrow; Hartzog, Frederic. "The Case for Online Obscurity." California Law Review 101, no. 1 (February 2013).

Warren, S. D., Brandeis, L. Brandeis. The Right to Privacy, Harvard Law Review, Vol. IV, December 15, 1890, No. 5.

Wright, David. De Hert, Paul (Eds.) Privacy impact assessment. Dordrecht: Springer, 2012.

Yee, George O.M. Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards. IGI Global, 2012 doi:10.4018/978-1-61350-501-4.

Zelazny, Frances. "The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries." In CGD Policy Paper. Washington, DC: Center for Global Development, 2012. Zureik, Elia; Karen Hindle. "Governance, Security and Technology: The Case of Biometrics." Studies in Political Economy 73, no. Spring/Summer (2004).

PUBLISHING INFORMATION

Contact
Giesecke & Devrient GmbH

Fabian Bahr, Head of Berlin Office
Phone: +49 (0)30 2009 5480
fabian.bahr@gi-de.com

Mareike Ahrens, Project Manager
Phone: +49 (0)30 2009 54812
mareike.ahrens@gi-de.com

Design: Havas Worldwide Munich

Desk research: TNS Infratest GmbH

ISBN: 978-3-00-044224-7

November 2013
Printed on FSC®-certified paper using a carbon-neutral process