



biometric TECHNOLOGY TODAY

ISSN 0969-4765 May 2010

www.biometrics-today.com

SURVEY

US citizens ready to sacrifice privacy for security

According to a Unisys survey, 93% of US citizens are prepared to sacrifice some measure of privacy if it means safer air travel.

The Unisys Security Index, carried out every two years, also found that two-thirds are happy with full-body scans at airports, and nearly three quarters (72%) would be prepared to submit personal data in advance of air travel.

However, while these respondents were prepared to give up personal data, that willingness dropped a little when the information in question involved biometrics. Some 57% said they would be willing to submit to identity checks using biometric data such as iris scans or fingerprints.

The concessions to security are not confined to Americans. For example, it appears from this study that body scans are acceptable to 90% of citizens in the UK (the highest level of any country) and 70% of Australians.

Mexicans were the least willing to give up privacy for security.

The survey ranged beyond air travel. Other findings showed that national security and identity theft rank as America's top concerns, with nearly two-thirds (65%) 'extremely' or 'very' concerned about US national security and 64% seriously concerned about ID theft. ID theft and fraudulent credit card use are the biggest concerns for UK citizens, with 87% putting these issues at the top of their list of security worries.

Nearly two-thirds of Americans (62%) are also seriously concerned about credit and debit card fraud. The percentage of Americans who are seriously concerned about the security of online transactions is at the highest level now (43%) since the Unisys Security Index began three years ago. The percentage of Americans who are 'extremely concerned' about the security of their online transactions rose to 20% (up from 16% in September 2009).

GOVERNMENT

L-1 links with World Bank

L-1 Identity Solutions has become the first biometrics company to join the World Bank's new eTransform Initiative (ETI). This programme aims to give developing countries access to the technologies and best practices of commercial organisations to help them better deliver social and economic services.

ETI will create a knowledge-sharing network that will help governments deploy electronic solutions in areas such as identity, procurement, health and education. It will also explore how technology can be used to help citizens take part in democratic processes such as voting, and ensure access to health and welfare programmes. The World Bank is already

involved in 14 e-ID and e-government schemes around the world.

"The speed and precision with which developing countries administer services is dependent upon many factors, not the least of which is the ability to verify the identities of those receiving services," said Mohsen Khalil, director of the World Bank's Global Information and Communication Technologies Department. "L-1 brings valuable expertise in identity management to the initiative's knowledge network. Together with L-1 and other vendors, we look forward to building systems that better administer critical government services and reduce the identity-related fraud that can dramatically

Continued on page 2...

Contents

News

US citizens ready to sacrifice privacy for security	1
L-1 links with World Bank	1
Clear back in business...	2
...but iQueue provides competition	2
Germany and US link trusted traveller programmes	2
Acuity forecasts big growth for e-passports	3
Rugged device for biometrics in the field	3
Voice Commerce opens UK trust centre	3
Apple goes to the heart of ID	4
Customer ID will drive biometrics market	4
IBG lands US Army contract	5
India defends use of iris scans	5
Pakistan and Afghanistan to use biometric border system	12

Features

Voice biometrics: real-world issues and solutions	6
Global mobility and security	8
Under lock and key – keeping sensitive data where it belongs	10

Regulars

News in Brief	3
Product News	4
Company News	5
Events Calendar	5
Comment	12

Photocopying

Global mobility and security

Silvia Venier, Centre for Science, Society and Citizenship

Globalisation and the development of the information society introduce new challenges but also new opportunities with respect to the mobility of people, goods, services and capital. Such mobility includes the movement of bodies (people), transactions (things that a person does either as physical actions or as captured in data), and artefacts (things associated with the individual). The importance of digital identity and identity management systems is increasing in the global and networked context. Technologies like biometrics are implemented to control the movement of people in order to prevent security threats, illegal immigration, and criminal and terror attacks.

The past decade has seen a dramatic evolution of biometric and security applications, and although the technological and performance aspects of these systems have significantly improved we still face challenges in understanding how to set the optimal policies to ensure that systems are not misused.

This is a particular issue as the breadth of the systems has grown: the next decade will see the launch of the largest systems to date, with India rolling out its Unique ID programme (now known as Aadhaar) to a population of more than one billion.¹

As the scale of these systems grows, it becomes even more imperative that policies around data protection, individual identity, and privacy keep pace.

Key role

Because of the key role played by biometric technologies in the globalised, networked society, the involvement of relevant stakeholders in the debate on ethics and policies of biometrics and security technologies is crucial.

On 25 and 26 March 2010, a high-level workshop addressing these issues took place in Brussels and attracted an audience of key European and international policymakers, industrial players, and experts from universities and research centres, coming from 21 different countries.

The agenda included the participation of speakers at senior political levels, such as: Siim Kallas, Vice President of the European Commission and Transport Commissioner; Peter Hustinx, the European Data Protection Supervisor; Jaak Aaviksoo, the Estonian Minister of Defence; and Margaritis Schinas, the Principal Advisor to the Bureau of European Policy Advisors.

There were also European Commission delegates, including: Jean-Michel Baer, Director of Directorate Science, Economy and Society from DG Research; and Jan Ostojka-Ostaszewski, a member of the cabinet of Vice President and

Commissioner for Justice, Fundamental Rights and Citizenship Viviane Reding.

The workshop was the product of the EC-funded project RISE – Rising Pan European and International Awareness on Biometrics and Security Ethics – and was the second of a series of three workshops addressing the emergence of the ethical, policy and social issues raised by security technologies. It also provided input for the forthcoming RISE Multi-stakeholder Conference, to be held on 9-10 December 2010.

As part of the RISE project's activities, these three workshops and the conference aim to encourage the involvement of European stakeholders such as regulators, responsible agencies, lawmaking bodies, industry, third-party privacy solutions providers and consumers' representatives, in setting technology security policy in Europe.

Opportunities and challenges

The workshop examined the opportunities and challenges that information and communication technologies (including biometrics) present for the mobility of people and information.

The opening presentations given by Prof Emilio Mordini, coordinator of the RISE project, and Prof Margit Sutrop, workshop chair, suggested that the main question to be addressed by relevant stakeholders is how to formulate new policy solutions for promoting mobility while minimising the risks to our privacy and security, rather than focusing only on technological issues.

Technology, they said, is hardly the ultimate solution to crucial policy problems: while setting security policies, the key question is not 'which technology represents the best option?' but 'in what kind of society do we want to live?'

The workshop was divided into three sessions around the themes of governance and policy-making processes regarding identity management systems; the multifaceted prism of fundamental

rights to privacy and security in relation to the implementation of biometrics, body scanners and other detection technologies; and the cyber-security of critical information infrastructures.

Special attention was paid to the issue of the biometric technologies in travel documents, border control and immigration management, as well as the deployment of body scanners at European airport security checkpoints.

Identity management: governance and policymaking

Identity management is the key enabler and critical component of securing the mobility of people and goods. Biometric systems are implemented to control the movement of people: in Europe, they are used for border and immigration control in e-passports or large-scale IT systems like EURODAC, SIS II and VIS.

However, there is no common policy at the European Union level regarding the concept of identity, identification and authentication, or on which types of information could be used to establish an identity or how the reliability of identity infrastructures could be determined. The first session of the workshop addressed the main governance and policy-making issues related to identity management.

A critical point of discussion was the use of biometric technologies as part of the e-services provided by European public administrations – and their interoperability. Electronic identities represent the pillars of a trustworthy information society and an enabler for the wider implementation within internal markets.

John Stienen from DG Informatics – European e-Governments Services (IDABC), talked about the Interoperability Solutions for European Public Administrations (ISA programme). These administrations are increasingly offering their services online to businesses and citizens. The ISA programme tries to support the interoperability of such systems, fighting against the e-barriers that might impede the proper functioning of the internal market, as well as supporting the cross-border use of national e-ID.² The STORK programme (Security idenTity for crOss boRders linKed) was announced in June 2008 to support the implementation of the EU-wide interoperability of electronic identities in cross-border activities, involving pilot projects in five Member States across Europe and a set of co-ordinated research initiatives.³

Another critical issue that needs to be addressed when setting security policies is information security, defined as “the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction”. As well as achieving this protection through technological solutions, there is a need for initiatives to raise awareness – the subject of a presentation by Alexander Nouak from the Fraunhofer Institute for Computer Graphic Research.

Awareness-raising initiatives are a critical tool in the management of power relationships – which encompasses the information management chain – in order to empower subjects who are less powerful. Above all, it is essential to take into account the widespread use of hidden detection technologies and the possibility of the combination of different data for the profiling of subjects who are often unaware of the dangers.

Fundamental rights, privacy and security

The assessment of the impact on fundamental rights of security technologies and the analysis of their effectiveness in protecting our security were the topics addressed during the second session of the workshop. This was opened by the special address delivered by Siim Kallas, who focused on the current and future challenges in aviation security.

A policy report – ‘Whole Body Imaging at airport checkpoints: the ethical and policy context’, prepared by the RISE project jointly with its sister project HIDE – was officially presented to the Transport Commissioner during the second session of the workshop.⁴ The report aims to clarify the European debate about the adoption of such a technology.

Kallas reported that the European Commission is analysing the results of a wide consultation process that addresses questions related to personal freedoms, fundamental human rights and the health and cost-effectiveness aspects of the so-called ‘security scanners’.

The report containing the results of this consultation and addressing the European Parliament Resolution of October 2008 is expected to be published in early 2010. This will serve as a basis to help formulate a uniform European approach regarding the installation of full body scanners at European airports by June 2010.⁵

According to Kallas, the traditional approach based on walk-through metal detectors and hand searches is reaching its limits and there is a need to provide law enforcement services and security screening staff with the means to act in a more targeted manner when implementing security controls.

The RISE project

RISE (Rising pan-European and International Awareness on Biometrics and Security Ethics) is a 36-month EU-funded project that aims to set up an international initiative to monitor ethical and policy issues raised by biometrics and security technologies. It builds on dialogue already instigated by two associated projects – BITE (www.biteproject.org) and HIDE (www.hideproject.eu) – and by two previous conferences on ethics and biometrics organised by the EC DG Research and the US DHS Privacy Office respectively in 2005 and 2006. The RISE project will involve key European and international actors in an ongoing, policy-related, non-official dialogue, and also aims to extend this dialogue to Asian and other international actors.

For further information, go to: www.rise-project.eu

Instead of treating every individual passenger as a potential high risk, said Kallas, “prior and timely identification of the passengers most likely to pose a high risk as well as unpredictable variations of control techniques need to be looked at.” Biometric technologies could help airport security services implement this task.

Challenges and powers

Jan Ostoia-Ostaszewski and Margaritis Schinas also spoke in this session. Ostoia-Ostaszewski talked about the new challenges to be faced in the review process of the European data protection legal framework. Schinas focused on the fact that, after the Lisbon Treaty came into force last December, we passed from the ‘European Community’ to a ‘Europe of values’, with those values having a legally binding power.

Schinas continued by saying that, in such a European Union, with its claims to be a world leader in technology, the ultimate ‘measure’ in taking political decisions must always be the human being. The multi-dimensional policy approach to security should always consider fundamental individual rights as well as the common good.

This challenging session also saw the participation of Peter Hustinx, who focused on the implementation of a privacy framework for the Stockholm programme, which was adopted last December, and the setting of the EU agenda in the area of justice, liberty and security for the 2010-2014 period.

Despite its emphasis on citizens’ freedoms and rights, the programme remains overtly oriented towards the reinforcement of technology usage within the context of EU security poli-

cies, particularly with computerised systems of information exchange and data processing.

Hustinx highlighted the need, when the EU data protection legal framework is reviewed, to ensure the effectiveness and proportionality of the use of personal data and to guarantee concrete individual control in order to strengthen the position of the citizen in the data management chain.

In the second part of this session another interesting presentation was given by Kamlesh Bajaj, Chief Executive Officer of the Data Security Council of India, one of the Asian partners of the RISE consortium. Bajaj covered the Indian national plan, UID, which aims to provide each citizen with a biometric-based national identification card. It is the biggest identification plan ever put in place and will eventually involve 1.2 billion citizens.

The biometric identity cards will provide a means of ID for the millions of people that currently do not possess any documentary proof of their existence, and it is hoped that it will help in fighting terrorism and crime.

Bajaj talked about the security and privacy challenges of this huge online centralised database that will retain Indian citizens’ personal information, and focused on the technological and policy solutions that have been put in place to support this project.

Critical infrastructure protection: the ethical and policy context

Because many services now rely on central ID management systems and infrastructures, we have become critically dependent on them. Protective measures need to be put in place to guarantee that these services and infrastructures are not vulnerable to failures, disruptions or attacks.

The third session of the RISE workshop, focusing on the policy implications of critical infrastructure protection, was opened by a keynote speech delivered by Jaak Aaviksoo. He first recalled the April 2007 cyber-attacks on Estonia, a country where the greater part of the population relies on electronic or Internet-based services. The issue of whether democratic states, built on a respect for fundamental human rights and liberties, are more vulnerable to cyber-terrorism was the central topic of Aaviksoo’s speech.

Since the main aim of terrorists is not only to destroy or kill, but above all to create fear, national public authorities have to demonstrate zero tolerance against these attacks while implementing their security policies. The critical issue is the ability of democratic states to internally agree and define the levels of tolerable risk.

Aaviksoo briefly observed that the regulation of cyberspace is still an open issue to be

CSSC

The Centre for Science, Society and Citizenship (CSSC) is an independent, non-partisan, human impact research company specialising in the social, cultural and ethical implications of emerging technologies in various fields (eg, homeland security, biometrics and e-ID, smart ambient, ubiquitous computing, cloud computing, disaster preparedness, public health, eInclusion). CSSC's track record of research, partnering and networking has made it a leading European institution in the area of science and society.

CSSC serves as a member of the Fundamental Rights Platform of the Fundamental Rights Agency of the European Union (FRA). The Centre is also a member of the European Association of Centres of Medical Ethics (EACME) and of the International Association of Bioethics (IAB). CSSC is an associate member of the Italian Confederation of Education and Knowledge Companies (Assoknowledge), where it leads the sector group on biometrics.

CSSC carries out its work in several ways, including studies, publications, training and coordination of multicenter research projects.

For more information, go to: www.cssc.eu

addressed in the international arena, but also pointed out that, rather than the strict regulation of a virtual and ubiquitous environment, the bottom-up approach based on building private and public awareness on cyber-risks and cyber-opportunities still remains the best option.

Conclusions: a debate to be continued

Emerging technologies could act as strong empowering tools, but their deployment often raises critical ethical and policy issues that need to be constantly addressed. While setting and implementing security policies, such as the inclusion of biometric technologies in e-ID documents and the creation of centralised online databases, or the deployment of body scanners at airport security checkpoints, the rationale for political decisions must be strongly linked to fundamental human rights and freedoms. The real and critical question is: what kind of society do we wish to live in?

The RISE workshop addressed the need to create a new sense of responsibility for individuals and states, in order to find the balance between security, privacy and other fundamental human rights. In the European Union, a uniform approach to the definition of security priorities, as well as the man-

agement of e-identities, needs to be further developed. In these tasks, the involvement of relevant stakeholders in a constant, multi-disciplinary, international debate plays a crucial role: the dialogue initiated during the March workshop will continue during the next RISE workshops, to be held in September and December 2010.

About the author

Silvia Venier has a background in international political sciences (University of Trieste) and serves as a research assistant at the Centre for Science, Society and Citizenship, where she is in charge of the RISE and HIDE projects.

References

1. India's UID programme: <http://uidai.gov.in>
2. Decision N° 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on Interoperability Solutions for European Public Administrations (ISA)
3. Stork: www.eid-stork.eu
4. HIDE: www.hideproject.eu
5. European Parliament Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, RSP/2008/2651

Under lock and key – keeping sensitive data where it belongs

David Ting, founder and CTO, Imprivata

The growth in demand for biometrics as a factor of authentication stems from two main areas – hardened security for compliance and greater end-user convenience. As security threats grow and security regulations become more rigid, organisations are increasingly choosing to implement biometric authentication to protect data and comply with regulatory demands.

Authenticating each user before he or she is granted access to the corporate network is a challenge that faces CIOs across the globe on a daily basis. With the threat of data theft and hacking rife, organisations know they need to improve security at the point of access, whether this is from inside the organisation's building or from mobile devices that are playing an increasingly pivotal role in the modern business IT infrastructure. The trend towards

using externally hosted web applications will only further increase the password headache for end users and administrators alike.

Technologies such as Single Sign-On are being widely adopted in organisations where it is clear that the number of passwords the user has to deal with every day has spiralled out of control. However, this kind of technology is most effective when combined with strong authentication devices that include fingerprint



David Ting

biometrics as well as smartcards and password tokens. This results in two-factor authentication that can increase security and improve workflow if the right method of authentication is selected in the right environmental setting.

Huge flexibility

The biometric scanners we see today offer huge flexibility and come mounted on keyboards, notebooks, electronic door locks and safes. They are often direct imaging silicon sensors capable of producing high-quality images with a very small footprint, differing hugely from the earlier generations of fingerprint scanners that were only commonly adopted on civil biometrics programmes.