



EUROPE

28 January 2011

On the value of privacy and data protection

European Privacy and Data Protection Day



LSTS
LAW, SCIENCE,
TECHNOLOGY &
SOCIETY STUDIES
VRIJE UNIVERSITEIT BRUSSEL
BRUSSEL



Vrije
Universiteit
Brussel

Microsoft

crosstalks

Many thanks to the contributors of this booklet for their collaboration!

Text editing: Rocco Bellanova, Rosamunde van Brakel and Sara Engelen

Concept & production: CROSSTALKS Vrije Universiteit Brussel

Layout & typesetting: Karel Van den Keybus – Gekko

Printing: Gekko

Cover picture: Watermael-Boitsfort by Dylan Belgrado, 2010

Pictures on pages 10, 18, 19 and 26 by © Marleen Wynants

Responsible publisher: Paul De Hert, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium

TABLE OF CONTENTS

Intro	p. 5
Prof. Paul De Hert, Law Science Technology & Society Research Group (LSTS), VUB	
Ambition is needed	p. 6
Peter Hustinx and Hielke Hijmans, EDPS	
Check in / Check out. The Public Space as an Internet of Things	p. 9
Christian van 't Hof, Rathenau Institute	
WikiLeaks: Welcome to the sousveillance society	p. 11
Gemma Galdon Clavell, Universitat Autònoma de Barcelona	
Big Brother: The glass citizen is a fact but we're far from a glass government and glass firms	p. 12
Raf Jespers, Progress Lawyers Network	
Big Brother Awards 2010	p. 15
Arne Vandenbogaerde, Liga voor Mensenrechten	
Moving dots: The need for proportionality in monitoring and screening travelers	p. 16
Sophie in 't Veld, MEP	
Developing Technology to Respect Privacy and Promote Freedom	p. 20
Ron Zink, EU Affairs Microsoft	
Strong Data Protection on both sides of the Atlantic	p. 23
Jan Philipp Albrecht, MEP	
Broadband Networks and Smart Grids	p. 24
Lillie Coney, Electronic Privacy Information Center (EPIC)	
Promoting the fundamental right to protection of personal data worldwide	p. 27
Kateryna Gayevska, Council of Europe	
Je m'en fish VZW	p. 29
Bart Dujardin, Je m'en fish	
Artistic Contributions	p. 30
Presentation of Events	p. 32

INTRO

Prof. Paul De Hert, Law Science Technology & Society Research Group (LSTS), VUB

Beste lezer,

Op vrijdag 28 januari 2011 wordt in Europa, maar ook in de rest van de wereld, de jaarlijkse European Privacy and Data Protection Day gevierd. Gedurende een hele dag organiseren overheids- en andere instellingen en het sociale middenveld activiteiten om de aandacht te vestigen op de waarde van privacy en de bescherming van persoonsgegevens in onze samenleving. 2010 was een jaar waarin er veel te doen was rond privacy: discussies over Facebook, Wikileaks, body scanners en uitspraken zoals 'privacy is dead' bevestigen de dringende nood aan een debat over deze kwesties.

Voorliggend programmaboekje wil de lezer laten kennismaken met enkele vooraanstaande privacy stemmen vanuit verschillende disciplinaire hoeken en een overzicht bieden van de activiteiten die in het kader van de European Privacy and Data Protection Day in Europa worden georganiseerd.

*Ik hoop u op die dag te mogen verwelkomen,
Professor Paul De Hert (Vrije Universiteit Brussel)*

Dear reader,

On Friday, 28 January 2011, Europe, but also the rest of the world celebrates as it is European Privacy and Data Protection Day. A whole day of events, organised by governmental and other institutions and civil society will draw the attention to the value privacy and data protection have in our societies. 2010 was a year in which there were a lot of discussions going on about privacy; discussions about Facebook, Wikileaks, body scanners and declarations such as 'privacy is dead' confirm the urgent need for debate about these issues.

This programme booklet introduces the reader to several prominent privacy voices and contains an overview of the activities that are organised in Europe on the occasion of European Privacy and Data Protection Day.

*I hope to welcome you on that day,
Professor Paul De Hert (Vrije Universiteit Brussel)*

Chère lectrice, cher lecteur,

Le vendredi 28 janvier 2011, l'Europe, mais aussi le reste du monde, célèbre la Journée Mondiale de la Vie Privée et de la Protection des Données. Une journée entière d'événements, organisés par des institutions étatiques et non, ainsi que par la société civile, sera l'occasion de porter l'attention sur la valeur de la vie privée et de la protection des données personnelles dans nos sociétés. 2010 a été une année riche en débats touchant à la vie privée. Toutes ces discussions concernant Facebook, Wikileaks, les « body scanners », ainsi que des déclarations telles que « la vie privée est morte ! » ne font que confirmer la nécessité et l'urgence d'un véritable débat sur ces questions.

Cette brochure-programme introduit les lectrices et les lecteurs à la perspective de certains des principaux experts de la vie privée, et offre une présentation des activités qui seront organisées en Europe à l'occasion de la Journée Mondiale de la Vie Privée et de la Protection des Données.

*En espérant de vous y voir nombreux,
Paul De Hert, Professeur de la Vrije Universiteit Brussel*

AMBITION IS NEEDED

PETER HUSTINX AND HIELKE HIJMANS, EDPS

■ Data Protection Day is the perfect occasion to outline the main priorities and challenges for data protection in a changing environment.

New technologies and globalisation allow the exchange and processing of personal data on an unprecedented scale. Modern phenomena like social networks, cloud computing and geo-location devices pose enormous challenges for data protection.

One can argue whether the general principles of data protection still remain valid today. We are convinced that they are and that also in a developed information society individuals need and expect to stay in control of their personal data. It is hard to imagine how a society could function without the protection of privacy and personal data.

However, we are also convinced that the current legislative arrangements will not provide for sufficient effective protection in the longer term. The Commissions' Communication on 'A comprehensive approach on personal data protection in the EU'¹ recognises the challenges and announces the review of Directive 95/46/EC and other legal instruments on data protection. This Communication is an important landmark on the way towards a new legal framework.

We fully support the main lines of this Communication, such as the need for better harmonisation of national data protection legislation, the need for a technologically neutral approach, the inclusion of the principles of privacy by design and accountability, and the introduction of a mandatory security breach notification covering all relevant sectors.

It is in our view imperative to include the areas of police and justice in the general framework. A separate framework for police and justice does not reflect a reality in which other actors are more and more involved in law enforcement activities, whether we like it or not. We do not only refer to the

involvement of private actors (PNR, data retention, money laundering), but also other public authorities like competition or tax authorities.

As a final remark on the review process, we recall that the EDPS constantly emphasised the need for ambition. An ambitious approach is needed to tackle the enormous challenges. This is not just another amendment of EU law.

The Review Process might be the most important development of EU policy making, relevant for data protection, but it is certainly not the only one. We highlight three actions which capture our big interest: the elaboration of the Stockholm Programme, Europe's Digital Agenda and the announced revision of the data retention directive.

The Stockholm Programme defines the framework for the area of freedom, security and justice until 2014. In this area, initiatives for a better cooperation between law enforcement authorities include on many occasions the collection and exchange of personal data. Many initiatives envisage the cross-border collection and sharing of personal data on a large scale, as essential parts of a Europe without internal borders. The Stockholm Programme announced an Information Management Strategy for EU internal security. Much can be said about this strategy which clearly includes privacy. On one specific aspect we would like to focus here, the need for evaluation of the existing framework before proposing new legal instruments. A method of 'ex ante' evaluation can be a good tool to ensure that only measures are proposed that are really necessary to protect the security of citizens.

The Digital Agenda is an EU strategy which aims to boost the European digital economy. It covers a wide range of policies having a direct impact on citizens' daily life.

¹ 4 November 2010, COM (2009) 609 final.

In our view, new information technologies should only be introduced if they are reliable, secure, under individuals' control and if the protection of their personal data and privacy is guaranteed. The trust of the citizens in these systems is crucial.

This is one of the reasons why we insist in the 'principle of privacy by design'. European legislation should ensure that only techniques are used which are privacy friendly and avoid unnecessary processing of personal data.

Finally, we would like to draw the attention to the foreseen revision of the Data Retention Directive 2006/24. As we all know, this directive requires the retention of traffic and location data of the communications of all persons residing within the EU. This directive has led to much criticism because of its intrusive nature. In this perspective, it is good to mention that on 2 March 2010 the Federal Constitutional Court of Germany (*Bundesverfassungsgericht*) ruled on the legality of the retention of telecommunications data². The Court allowed retention - in Germany - only for a short period and for a limited number of specified purposes.

We would even go one step further: the Directive is only based on the assumption that it constitutes a necessary and proportionate measure, but the necessity was not really demonstrated. An evaluation, based on concrete numbers and figures, should consider the necessity of the instrument. Such concrete evaluation has not yet taken place, but possibly the Commission will come up with facts and figures.

Peter Hustinx and Hielke Hijmans

BIO PETER HUSTINX

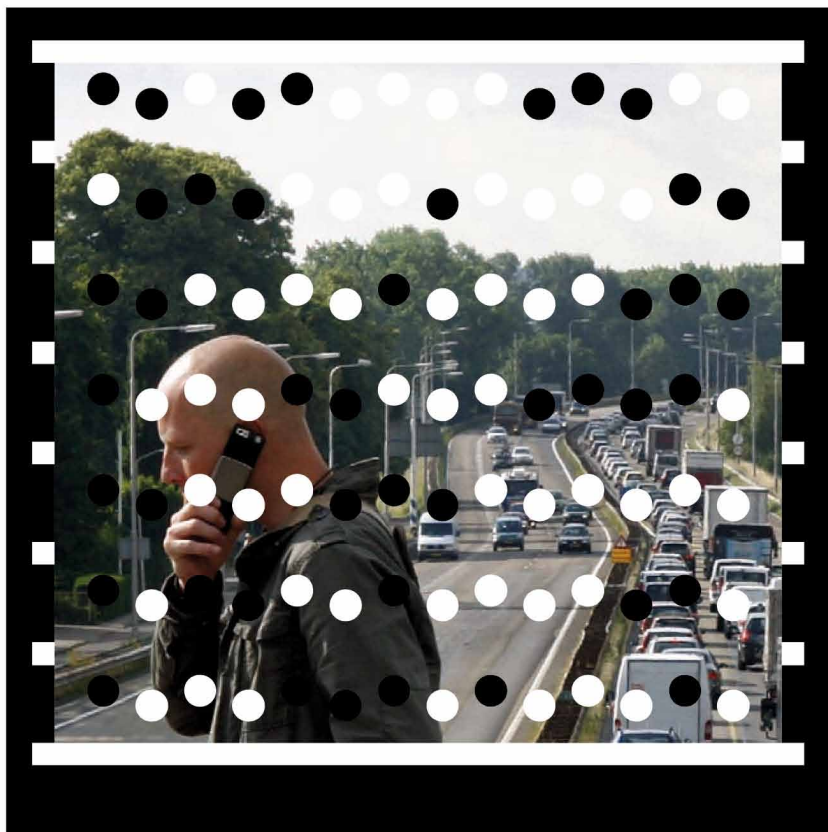
Peter J. Hustinx (1945) has been European Data Protection Supervisor since January 2004 and was re-appointed by the European Parliament and the Council for a second term of five years. He has been closely involved in the development of data protection legislation from the start, both at national and at international level. Before entering his office, Mr. Hustinx was President of the Dutch Data Protection Authority since 1991. From 1996 until 2000 he was Chairman of the Article 29 Working Party. He received law degrees in Nijmegen, the Netherlands, and in Ann Arbor, USA. Since 1986 he has been deputy judge in the Court of Appeal in Amsterdam.

BIO HIELKE HIJMANS

Hielke Hijmans works since 2004 for the EDPS, currently as Head of Policy and Consultations. He worked on dossiers like PNR, police and judicial cooperation, data retention and public access to documents and represented the EDPS before the Court of Justice. He specialised as EU lawyer working for the European Court of Justice (2000-2004) and for the Dutch Government (until 2000) and published several articles.

² Cases 1 BvR 256/08, 1 BvR 263/08, 1BvR 586/08.

01
.TAG



// International Edition

CHECK IN / CHECK OUT

Christian van 't Hof
Rinie van Est
Floortje Daemen

Rathenau Institute
NAi Publishers

The Public Space as an Internet of Things

CHECK IN / CHECK OUT. THE PUBLIC SPACE AS AN INTERNET OF THINGS - CHRISTIAN VAN 'T HOF, RATHENAU INSTITUTE

■ In public space we are increasingly surrounded by digital devices. Cameras guard over our safety, antennas and sensors keep track of our driving speed, and digital wicket gates determine whether or not we gain access to the train station. Provided with an ever growing arsenal of identification numbers in ID cards, mobile phones and vehicles, we prove who we are, that we have a right to be there, and that we paid for it.

This digitalisation of the public space marks a new phase in the Information Society: the rise of an internet of things. What will this new phase mean for us as users of the public space? Are these technologies liberating our lives or restricting our privacy? An example is real time information plotted on maps. Now we exactly know where our friends hang out. Does this extra dimension just provide you with more options or do you rather feel the need to be left alone? Who are actually behind the network of digital devices and why do they want to look at us and judge us?

The authors of *Check In / Check Out* tackle these questions and deliver a set of design principles for the future. They map digitalisation with case studies from Japan, China, US and Europe, with a focus on the Netherlands – a country which turns out to take up the digitalisation in its own particular way.

Christian van 't Hof, Rinie van Est and Floortje Daemen (eds.) (2011) 'Check in / Check out. The Public Space as an Internet of Things.' Rathenau Institute and NAI Publishers

www.naipublishers.nl

BIO CHRISTIAN VAN 'T HOF

Christian van 't Hof is a senior researcher at the Rathenau Institute, the Dutch office of Technology Assessment. With his background in sociology and electrical engineering, he analyses the relation between human and electronic networks. His research involves RFID, digital skills, network convergence, geodata, virtual communities and robotics, while he compares European and South East Asian perspectives on their developments. Aside from his research he also presents scientific talk shows.



2 tight
2 mention!

WIKILEAKS: WELCOME TO THE SOUSVEILLANCE SOCIETY

GEMMA GALDON CLAVELL, UNIVERSITAT AUTÒNOMA DE BARCELONA

■ Nobody questions the fact that we live in a surveillance society -the development of surveillance-oriented security technology, improved intelligence-gathering and data-mining, identification and tracking techniques embedded in our everyday lives and cities... The list of devices that monitor our moves, interactions with public bodies, online activities, consumption patterns, etc. is never-ending. And, for all the talk about privacy, we have not managed to hold most of the surveillants accountable to the surveilled. Even though the affordability of devices with surveillance capabilities, such as mobile phones, have made it possible for the odd example of surveillance being used against those in power (such as the police's role in the death of Ian Tomlison at the G20 protests in London in 2009), it is obvious that most surveillance is about those at the top (sur) being able to control and use data of those at the bottom (sous).

Until now.

Wikileaks is doing **exactly** what most corporations and governments do with our personal data on a regular basis: use it as they wish, even sell it, without our consent, while providing us with very few and very weak tools to protect what we care about or be able to monitor how our information is used and circulated.

Which, apparently, is fine when they do it. When the surveilled take control, however, all hell breaks loose. Personally, I would prefer stronger regulation and better protection of personal information -even that of those in power. I would rather prefer information to be recorded and stored only when necessary and with permission. But in the world of CCTV, biometrics, full-body scanners and the like, it does not look like that is going to happen anytime soon. Therefore, if I am asked to put up with the use and abuse of my personal data in the surveillance society, I might as well be given the possibility to turn the gaze on the surveillants.

So since I was never given the choice to opt out of the surveillance society, I choose to join the sousveillance society, and the ranks of those who refuse to be held accountable by the unaccountable.

I choose to support WikiLeaks.

BIO GEMMA GALDON CLAVELL

Gemma Galdon Clavell is a researcher based at the Universitat Autònoma de Barcelona, where she focuses on public policy, community safety, incivility, surveillance and public space. She has worked for the UN, the Transnational Institute and the Catalan Institute for Public Security and is a regular contributor to several Spanish and European periodicals.

<http://blogs.euobserver.com/galdon/2010/12/02/wikileaks-welcome-to-the-sousveillance-society/>

BIG BROTHER: THE GLASS CITIZEN IS A FACT BUT WE'RE FAR FROM A GLASS GOVERNMENT AND GLASS FIRMS

RAF JESPERS, PROGRESS LAWYERS NETWORK

■ Wikileaks has been the target of everyone's attention. By revealing documents on the Iraqi war and the (secret) diplomacy of the US, the doings of the most powerful state were put on show. On the other hand, the surveillance of citizens by the US but also by other states has become common practice.

In my book *Big Brother in Europe* (Epo 2010), I describe how in the first decade of the 21st century the evolution towards a surveillance society has taken a giant leap.

The surveillance society in 2010 is the result of three evolutions:

One: a technological and digital revolution which has made surveillance technologically possible;

Two: 9/11 which created an authoritarian climate which has made a surveillance society acceptable;

Three: the increased influence of the European Union, which has permitted exceptional legislation and uncontrolled institutions in the field of police, justice and secret services.

For the first time in the history of humankind, technology has become so advanced that every citizen can be constantly surveyed. Technology also makes it possible for businesses to transform everybody into an object of marketing. A spirit of the age is growing which accepts this is normal.

It's all high tech: RFID chips, surveillance cameras, scanners, DNA kits, spyware, databases, bugs, black boxes, track and trace. Our daily lives are full of it. The average Belgian is registered in about three hundred databases, UK citizens and Dutch citizens in about six hundred.

The dominant idea is that what is technologically possible may be put in practice without more ado.

It's a high speed evolution. Google goes back to 1999. Facebook dates from 2004. These sites spend billions on gathering information about who you are, what you read and think, who your friends are, what clubs and parties you're a member of. Internet has become a lucky bag where both government and private sectors greedily fish in your private affairs. When Facebook founder Mark Zuckerberg turned 26 he was the 36th wealthiest American. Facebook now has a market value of 41 billion dollars. The less privacy for the citizen the more money in the till for Facebook.

What is the cumulative effect of all this? It's not only that we have lost confidentiality but we have also lost our 'self'. The breadth and depth of this process are unprecedented. Glass governments and glass companies have a long way to go, the glass citizen on the other hand is a fact.

Privacy is no longer sacred and secure. Democracy cannot function because invading privacy means that exercising our fundamental rights (freedom of speech, freedom of association, freedom of press) is at risk. It's not that six billion people are constantly under surveillance, but the technology is there and is being used not only to keep an eye on criminals and terrorists but also young activists, suspect communities, critical journalists, professors or lawyers. Remember the database on 'political activists with a dissident opinion'. Big Brother is watching and isolating anyone who isn't mainstream.

9/11 was the second determining factor. The attacks geared up the surveillance society to its present speed. Terrorism was an alibi for invading privacy and other freedoms. The government sees all citizens as potential security risks. It is using the digital and technological revolution to its full capacity to record every word, every sigh and every shadow. Measures were taken which in normal times should have led to massive protest. Democratic rights and freedoms were oppressed. Exceptional measures became permanent. It's true that citizens have the right to live in safety and the battle against terrorism

should be relentless, but behind the war on terror and the security policy there is a hidden agenda. The specter of darker times (secret prisons, blacklists, torture) has reappeared.

'The 11th of September 2011 was nearly the end of the Europe of the Rights of Man' said J.F. Leclercq, public prosecutor for the Belgian Court of Cassation, in his opening speech in 2009.

There is also a third factor, which contributed to the expansion of universal control: the European Union. Nearly unnoticed, a very complex and unmonitored security architecture was built with Eurojust, Europol, the border patrolmen of Frontex, e-border concepts and expensive projects on security research.

In the Union, the executive branch – the Commission and the Council – took over the dominant power position at the expense of the parliament and the judiciary. The separation of powers has therefore been undermined. The warnings from lawyers and civil society were barely heard. The Union's rhetoric on human rights differs from its practice. These undemocratic ways in the EU have created a whole range of dangerous laws like the data retention directive or the PNR agreements with the US.

In the meantime the financial crisis has attacked the heart of the Union. All EU countries have made unprecedented budget cuts. The population has taken to the streets because it doesn't want to pay the bill for a crisis it didn't create. Will protest come up against the watchful eye of Big Brother?

There is however also resistance to Big Brother. EU commissioner Viviane Reding has stated that the defense of our privacy is 'the most important challenge for the next decade'. 'Individuals should be protected from intrusions into their private life. It is urgent that the principles of Rule of Law be reasserted in this area' declared Thomas Hammarberg, Human Rights Commissioner for the Council of Europe.

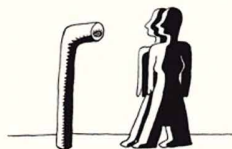
There has to be a democratic change. That's why I made a practical proposal in my book for a European Charter to protect fundamental rights and privacy. A legal and political perspective of resistance to these disastrous developments, in face of which civil society can no longer remain a bystander. It can use modern communication technology to the full because they need to be broadcast far and wide

BIO RAF JESPERS

Raf Jaspers has a Masters Degree in history and is a lawyer involved in the PROGRESS Lawyers Network Belgium. He is member of the International Association of Democratic Lawyers. He has published on migration, rights of activists, international law in relation to terrorism. In 2010 his book *Big Brother in Europa* was published by EPO (Antwerp-Belgium), a reference book about the control state Europe.



BIG
BROTHER
IN EUROPA



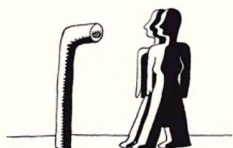
BIG
BROTHER
IN EUROPA



BIG
BROTHER
IN EUROPA



RAF JESPERS



BIG
BROTHER
IN EUROPA



RAF JESPERS



BIG
BROTHER
IN EUROPA



RAF JESPERS



BIG
BROTHER
IN EUROPA



RAF JESPERS



BIG
BROTHER
IN EUROPA

RAF JESPERS



BIG
BROTHER
IN EUROPA

RAF JESPERS



BIG
BROTHER
IN EUROPA

BIG BROTHER AWARDS 2010

ARNE VANDENBOGAERDE, LIGA VOOR MENSENRECHTEN

■ Following the example of many other human rights organisations across Europe the Liga voor Mensenrechten (Flemish League for Human Rights) organised the Big Brother Awards in November 2010. The Big Brother Awards marked the closure of a 6-month intensive campaign on the right to privacy in Belgium. The Liga is increasingly concerned about the measures taken by governments under the guise of the fight against terrorism and crime, which affects citizens' right to privacy. Social problems are more and more translated into security problems and subsequent solutions. Most concerning is the lack of knowledge and information citizens have about their right to privacy and the measures taking against it. During the last 6 months the Liga voor Mensenrechten therefore organised a series of events such as camp-spotting, privacy walks, lectures, and other actions aimed at informing the citizens about their right to privacy.

For the election of Belgium's very own Big Brother Awards, the Liga had selected 8 persons or institutions that were violating the right to privacy. However, it was up to the citizens to choose, which of the nominated was violating their privacy. The award, as a certificate for excellence in violating the right to privacy of the Belgian citizens, was eventually given to the EU data retention directive. Other candidates included amongst others the Passenger Name Records, camera surveillance, and the MOBIB public transportation card. Maybe not unsurprisingly the data-retention directive was elected from amongst the others as the directive has sparked a series of protests from other human rights groups, academics, legal experts, and even the EDPS. According to the directive all telecommunications data needs to be stored by the electronic communications providers (telephone companies, mobile telecoms, Internet service providers). The directive essentially thus stipulates that all location and traffic data from every EU citizen needs to be collected and stored. In a concrete sense this means that whenever you text, call, or use your email this data will be stored. Subsequently this is the most privacy intrusive directive the EU has ever adopted.

The Liga has argued that such an intrusion is neither proportionate nor necessary in relation to its aim, i.e. the detection and prosecution of serious crimes. Another concern is the cost of the directive. The data needs to be stored by the electronic communications providers and it is unsure who will carry these extra storage costs, a likely guess would be the clients of these providers. The Liga voor Mensenrechten finds these concerns strengthened with the election of the Big Brother Awards. The award itself was handed to Mr. Luc Beirens of the Federal Computer Crime Unit who lobbied intensively for the adoption of the data-retention directive in Belgium. After the presentation a debate followed where Mr. Luc Beirens could defend his position and where the directive was evaluated. Today the directive is being evaluated at a higher level. The European Commission is revising the directive and its impacts. The commission will have to demonstrate convincingly that this directive is necessary and proportionate in relation to its aim. Up till now it has failed to do so, which means the directive will need to be revised and safeguards for the protection of privacy will need to be installed.

BIO ARNE VANDENBOGAERDE

Arne Vandenbogaerde holds a MA degree in international politics and received an LL.M. in International Human Rights Law from the Irish Centre for Human Rights. He worked in numerous NGOs and intergovernmental organisations. Since 2010 he works as a campaign officer for the NGO Liga voor Mensenrechten and is the academic coordinator of the GLOTHRO research networking programme at the University of Antwerpen.

MOVING DOTS: THE NEED FOR PROPORTIONALITY IN MONITORING AND SCREENING TRAVELERS

SOPHIE IN 'T VELD, MEP

■ These days the latest Harry Potter movie is showing in cinemas around Europe. Throughout the series Harry and his friends are hunted down by monsters and evil creatures. Whenever things get really dangerous, Harry uses his "invisibility cloak", allowing them to move around unseen. He also has a map that shows him the movements of others in the building of Hogwarts, like little moving dots.

Travelers outside the world of Harry Potter do not have an invisibility cloak, but governments do have a map showing each individual traveler moving around. All our moves are detected and registered, and all travelers are subject to extensive tracking, tracing and screening. Camera's on the highways register and store our license plates, the itinerary of users of public transports is registered and stored in electronic systems, RFID chips in boarding passes reveal the movements of a passenger in the airport, our mobile phones betray our whereabouts any time anywhere, and people walking or cycling down the street may be captured by cameras. Even a hermit in the desert cannot hide from Google Earth. In today's society, Harry Potter's invisibility cloak would be a very useful tool!

In recent years, extensive government powers have been created for massive, indiscriminate and warrantless collection of personal data for law enforcement and security purposes. At the same time, the means for democratic scrutiny of those powers, as well as legal protection of citizens' rights have been seriously eroded. Checks and balances, core elements for a vital democracy, are dangerously weak.

Critical voices are silenced with the argument "if you have nothing to hide, you have nothing to fear", thus shifting to the individual citizen the burden of proof that government action is not warranted.

Whereas in a democracy we do accept that the police may search the home of a suspect, provided there is probable cause and a search warrant obtained from a judge. However, we would not accept random house searches by the police, without search warrant, without any suspicion, without explanation. So why do we so

meekly accept the equivalent of such random searches in an electronic environment?

Like the classic tale of the frog who does not escape if he is boiled slowly, citizens have accepted the ongoing reduction of their freedom and anonymity without protest. Governments told them these measures are necessary in the interest of (national) security.

And who would dare to challenge the need to fight terrorists who want to blow us up? But if we look closer, the justification for the massive use of personal data of travelers does not hold water.

European laws on privacy protection only allow the collection of personal data if it is for a legitimate purpose and proportional. The proportionality test means that the objective for which the data are collected cannot be achieved by another, less intrusive, measure.

So far no evidence has been produced of the usefulness of the mass collection of passenger data for the automatic prevention of terrorist attacks. Evil intentions cannot be detected by way of software and algorithms. The massive data collection seems to be the civilian equivalent of the 1% doctrine, or, as Amooore and De Goede call it: "screening of transactions data is the war on terror's banal face of the preemptive strike". PNR data are undoubtedly very useful in specific investigations, completing information on a known suspect. But that does not justify the collection and long term storage of all data of all passengers.

Secondly, it would seem that PNR data are used mainly for other law enforcement purposes, for example illegal immigration and drugs trafficking. Those are certainly very valid purposes, but not the same as preventing terrorism, and therefore the proportionality test should be applied to each of these purposes separately. Function creep is a problem that must be tackled urgently. Under the flag of counter terrorism, vast government powers have been created for a wide range of law enforcement and security purposes, unrelated to counter terrorism.

Thirdly, we must have an indepth and independent evaluation of the effectiveness of the counter terrorism policies. Have the new government powers indeed brought greater security, as promised? Despite the mass surveillance of citizens, terrorists still manage to slip through security checks.

The aim of terrorists is to destroy our free, democratic society. Therefore counter terrorism must focus on protecting civil liberties and democracy, and make them more robust. We may not be able to offer a full invisibility cloak to citizens, but we have to ensure civil liberties are respected at all times.

BIO SOPHIE IN 'T VELD

Dutch Liberal Sophie in 't Veld has been member of the European Parliament since 2004. She is Vice Chair of the committee on Civil Liberties, Justice and Home Affairs and rapporteur on Passenger Name Records. She has set up the EP Privacy Platform.

**WHAT K
ARE REQUIR
COM**



The Italian Pavilion at the 12th Architecture Exhibition, Venice 2010 – picture by Marleen Wynants

**IND OF SPACES
ED FOR DIFFERENT
MUNITIES?**



DEVELOPING TECHNOLOGY TO RESPECT PRIVACY AND PROMOTE FREEDOM

RON ZINK, CHIEF OPERATING OFFICER – EU AFFAIRS, MICROSOFT

■ The convergence of Internet-enabled devices, high-speed broadband networks and international data centers is providing millions of users with “anytime access” to a rich new world of cloud-based services and software. These new services and technologies have unquestionably improved the way we live by offering tremendous benefits, such as lower IT costs for businesses, and empowering individuals across the globe to more easily connect and share common interests.

Computing technology and the Internet are now interwoven with almost every aspect of our daily lives, informing and shaping our understanding of the world, our choices and decisions, and our interests and values. As an IT sector innovator, we are tremendously excited about the promise of these technologies. At the same time, we are also mindful of the challenges that the ability to aggregate and share data large quantities of data online creates in terms of how best to protect the privacy of data subjects. Likewise, we recognise the direct link between robust privacy protections and other fundamental human rights, such as freedom of expression.

But how do we continue fostering innovation in computing technology and Internet services while at the same time managing the social and ethical concerns these innovations may bring? As the EU deploys its Digital Agenda, aimed at delivering sustainable economic and social benefits by 2020, the IT industry, regulators users, citizens and consumers must work together to answer this critical question.

At Microsoft, we spend a great deal of time and resources thinking about and working on finding the balance between innovation and privacy. We are deeply committed to ensuring that our innovations respect the privacy and security of individuals who use our products and services. We believe that the success of our company increasingly depends on users having confidence in our ability to responsibly manage and

protect their data, and we invest heavily to build our products, operate our services, and train our people to maintain high standards of privacy. “Privacy by Design” is integral to our efforts in this regard.

A great deal has been said and written about privacy by design in policy circles and across industry. Ultimately, this concept is meaningless unless it is translated into effective practical protections for users. In order to effect this translation, we have firmly embedded the “privacy by design” concept into our culture: we integrate privacy best practices into software development to ensure that privacy is incorporated into our products and services at the design stage, and we continue to assess new products and services against privacy risks through implementation and testing, through to final release. Our standard -- the Microsoft Privacy Standard for Development (“MPSD”) -- includes detailed guidance on supplying controls when developing products and services, creating transparent customer notification and consent procedures, maintaining data integrity, and providing robust data security features.¹

Our recent announcement about the ground-breaking privacy protecting features of the forthcoming new version of our web browser, Internet Explorer 9, reflects our commitment to these principles. The “Tracking Protection” feature of IE9 builds on the “InPrivate” features of previous versions of Internet Explorer, and will enable consumers to limit the amount of data they wish to share with third parties that might otherwise be used to track their activities online. By engineering this sort of enhancement with privacy in mind at the design phase, we aim to provide consumers with additional levels of control over what they want to engage in and how they choose to do so.

In addition to cultivating a culture that respects data protection and consumers’ privacy, Microsoft works with public and private sector partners worldwide to promote other human rights, including

freedom of expression -- after all, in addition to being a fundamental right in itself, privacy is also a fundamental enabler of free expression. Microsoft believes that while governments are principally responsible for promoting and protecting human rights and fostering the safety necessary for the information society to flourish, Microsoft and other online service providers also have a responsibility to promote respect for and advance human rights. We therefore helped form the Global Network Initiative (www.globalnetworkinitiative.org), an international consortium of technology companies, human rights organizations, academic representatives, and investors. Technology companies that join the consortium agree to incorporate basic principles and guidelines that respect fundamental human rights into their business practices, products, and services. Microsoft and other members have committed to notify users of online services about service-related policies and practices that affect their privacy; Microsoft also notifies users when we are ordered to remove content from a website or service, along with information about which laws or authorities required the removal.

As these practices and developments help illustrate, at Microsoft "Privacy by Design" is not just about auditing the privacy protections of our products and services, but instead involves creating a culture that embeds a respect for user privacy in the process of developing and deploying technology and services. Similarly, our commitment to fundamental rights involves living up to high standards that guide our operations on a daily basis. We recognise that as advances in devices and cloud computing deliver more powerful capabilities for interacting and sharing information on the web, technology providers, governments, law enforcement, community organizations, and Internet users have a shared responsibility to promote fundamental rights and a safer, more private and more secure online environment.

BIO RONALD ZINK

Ronald Zink, Chief Operating Officer EU Affairs and Associate General Counsel, Microsoft. Based in Paris, Mr. Zink is responsible for Microsoft's European policy and government affairs team. This team leads substantive and strategic positions on policy issues in Europe, the Middle East and Africa, including intellectual property. Prior to joining Microsoft in 1995, Mr. Zink worked in private practice advising companies of all sizes, ranging from start-ups to Fortune 500 corporations, on the protection, licensing and litigation of intellectual property rights relative to their businesses. Mr. Zink is a U.S. registered patent attorney and an inventor on several patent applications. He is active in numerous groups focused on technology policy, author of numerous papers on innovation and frequently speaks on technology-related topics.

¹ As part of our commitment to sharing best practices with the technology industry and privacy community, Microsoft has released a public version of the MPSD: Privacy Guidelines for Developing Software Products and Services.

PechaKucha Night

{ 20 * 20 }

IMAGES SECONDS

**Volume #16 on Jan. 25th 2011
in Brussels will take place at Les Halles de Schaerbeek!**

Pecha Kucha Brussels Vol. 16
Tempo, story, tension, show-and-tell.
Spread the word. Share the world.

Caroline Bergaud & Janice Richardson - eSafety, European Schoolnet
David Bond - Green Lions
Serena Borghero - Steelcase
Lillie Conney - EPIC
Nathalie De Bock - Charivari
Johan De Mey - UZ Brussel Radiology
Sang Hoon Degeimbre - Chef, L'Air du Temps
Andreea Druga - deco geometric
Dougald Hine - The Dark Mountain Project
Larry Moffett & Kumardev Chatterjee - European Young Innovators Forum
Deborah C. Peel - Founder and Chair, Patient Privacy Rights
Clemente Pestelli & Gionatan Quintini - Les liens invisibles
Liv Vaisberg - Ponyhof Gallery, Director
Peter Westenberg - Constant vzw & videomagazijn

**More info on speakers and registration on
<http://pechakucha.architempo.net/>**

Start at 20:20

We recommend that you arrive half an hour early.
Les Halles de Schaerbeek, Rue Royale Ste Marie 22a, 1030 Schaerbeek

STRONG DATA PROTECTION ON BOTH SIDES OF THE ATLANTIC - JAN PHILIPP ALBRECHT, MEP

■ Data protection rules are becoming very dynamic again.

- The EU Commission has published its first communication for the revision of the 1995 data protection directive;
- the same Commission is desperately searching for evidence that would legitimise the continuation of data retention;
- the US Federal Trade Commission has announced it will work on a "do not track" system for online customers;
- and on the transatlantic level, the shock in some corners (as can be read on Wikileaks) about the initial rejection of the SWIFT bank data agreement by the European Parliament has led to a new openness towards data protection in the field of security cooperation.

The EU Commission on 3rd December 2010 was given a mandate to negotiate with the United States a comprehensive data protection agreement for the area of police and justice cooperation. This is a good and really needed step, because it holds the potential to balance the strengthening of the security apparatuses that has happened at the cost of civil liberties in recent years. Transatlantic relations are not only important in the area of security cooperation, but also in assuring strong data protection and other civil liberties provisions. As the European Parliament's rapporteur for this, these are my key concerns:

Any agreement must strengthen data protection at both sides of the Atlantic, but it must also address the fragmentation of data protection rules here and there. It therefore has to harmonize existing and future agreements such as SWIFT, PNR and the many bilateral ones between EU member states and the US. Harmonized and easy to understand rules for their data is what the citizens need.

The agreement must create enforceable rights for EU citizens and others. They must have an effective possibility of access to the data and of juridical redress before a court. This is currently facing two problems: First, the United States still have the discriminating

definition of "individual" in the Privacy Act which excludes persons who are not US citizens or legal residents. Second, there is also a problem with the condition to prove actual "harm" following a breach of the fair information principles. This principle is unknown in EU data protection law and regulations. Access to a judicial revision of data protection infringements must be possible even if there is no obvious harm to the data subject.

Any transfer of data must be strictly prohibited if there is a risk that it leads to death penalties, illegal detention, torture, or other inhuman or degrading treatment or punishment in the US or third countries. We have a constitutional obligation to ensure that never under any circumstances data provided from the EU is being used to breach EU human rights standards.

Because of the real risk that data transfers to third states function as loopholes, these onward transfers should be generally prohibited. If third states want access to EU data, they instead have to enter into direct negotiations with the EU.

I look forward to working with my European and American colleagues on achieving a meaningful and strong transatlantic data protection agreement.

BIO JAN PHILIPP ALBRECHT

Jan Philipp Albrecht has been elected to European Parliament in 2009 for the German Greens. He is a member in the Committee on Civil Liberties, Justice and Home Affairs and a substitute member in the Committee on Legal Affairs, working on Data Protection, Internet Freedoms, and Civil Liberties. He became well-known as "Mister Anti-SWIFT", based on his successful efforts to have the first SWIFT bank data transfer agreement with the US rejected by the European Parliament. He studied law in Bremen, Berlin, and Brussels and IT-law in Hannover and Oslo. From 2006 to 2008, he was spokesman of the Green Youth in Germany.

BROADBAND NETWORKS AND SMART GRIDS

LILLIE CONEY, ASSOCIATE DIRECTOR EPIC

■ The United States does influence international privacy policy in a number of areas that impact consumer and human rights. While it may be assumed that the same or superior privacy protections exist in the United States—in fact they are often weaker in several respects.¹ There is no independent data protection authority or single law that protects personal identifiable information (PII) regardless of how it is collected or who might have it.

In the United States private sector entities often treat PII like a commodity that is owned by the entity that collected it. Further, there is no single law or regulation that establishes data privacy protection for PII that assures: transparency, right of correction, collection limitation, use restrictions, oversight, accountability, and legal recourse for consumers or data subjects. Further, the US Congress has more aggressively used its power to dramatically reduce the effectiveness of state laws that are intended to protect privacy and consumer rights.²

Privacy and Smart Grid

Privacy is not a matter of ownership, but rather of control over information: how information is collected, if it is retained, how it may be used, what rights belong to the data subject, data holder oversight, and accountability obligations. It is interesting that the word “ownership” is cropping up in the context of the Smart Grid. Many residential, and some commercial energy consumers will likely not realize the value of energy usage data until instances of data abuse or misuse make that value evident. It is likely that, as a result of abuses or misuses of energy consumption data, the model of customer control will dominate the collection, retention and use of Smart Grid data.

Unique Privacy Challenges Posed by the Smart Grid³

Disclosure of Private Facts or the Details of Activities within Homes or Businesses

Identity Theft

Personal Surveillance

Energy Use Surveillance

Physical Dangers

Misuse of Data

Cyber Security and Privacy

There are two kinds of harm that the Smart Grid might face: intentional and unintentional. Nature or the environment can cause harm, but it will never be based on an underlying intent. Utilities preparedness and response to hurricanes, tornadoes, ice storms, may in many ways resemble their response to man caused events that impact the reliability or availability of electricity.

However, the next greatest threat will be manmade intended or unintended consequences to the Smart Grid. New applications or devices added to a complex system of Smart Grid architecture may offer threats to reliability that might challenge service providers. Further, weaknesses in the underlying architecture; grid software and firmware development could also introduce vulnerabilities to information privacy and security. Further threats are posed by updates, or intentional exploitations of vulnerabilities or weaknesses inherent in the complexity of Smart Grid systems. Additionally, the applications introduced by third party service providers may also pose risk to consumers.

¹ <http://epic.org/privacy/>, http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0052_0053.pdf, http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf

² <http://epic.org/privacy/preemption/>

³ <http://epic.org/privacy/fusion/>

Recommendations

The Smart Grid should be structured to avoid the retention of PII. Moreover, the prospect of remote access to Smart Grid data may lead to unauthorized access and misuse of the data. Many companies and government agencies provide employees and contractors with remote access to their networks through organization-issued computing devices. Remote access to Smart Grid customer information or utility usage data should be prohibited. However, even if permitted, appropriate security measures should be implemented. Computing device remote access should limit access to Smart Grid critical infrastructure and PII of customers. Access should include protocols to rapidly terminate access from devices that are lost or stolen, and personal use of the devices should be prohibited in order to help avoid viruses, worms, or malicious applications.

A global approach to solving the important privacy challenges of the Smart Grid may offer opportunities for better cooperation and collaboration on technologies that can benefit society, while at the same time protecting the consumer and privacy rights of users.

<http://epic.org>

BIO LILLIE CONEY

Lillie Coney is Associate Director of EPIC a public policy think tank based in Washington DC. EPIC began in 1994 and works to raise public awareness and focus debate on issues that impact privacy rights. Ms. Coney joined EPIC in 2004 to lead the organization's voting privacy project. In 2005, she took on EPIC's coalition development and civic participation portfolio. Ms. Coney identifies emerging privacy challenges presented by new technology, personal information use, and changes in personal data policy. Ms. Coney's work identified whole body imaging technology's use at airports, CCTV, biometrics, fusion centers, cloud computing, cyber security, and smart grid technologies as important areas for the organization. She is routinely consulted by Hill staff and has testified before U.S. House Committees as well as the Department of Homeland Security Data Privacy and Integrity Advisory Committee.



Aluminum & copper wire stitching Installation by El Anatsui at the 52nd International Art Exhibition, Venice, 2007 – picture by Marleen Wynants

JOINT HIGH LEVEL MEETING ORGANISED BY THE COUNCIL OF EUROPE & THE EUROPEAN COMMISSION

KATERYNA GAYEVSKA, COUNCIL OF EUROPE

■ On 28 January 2011, the Council of Europe and its Member States will celebrate Data Protection Day for the fifth time.

Data protection issues, including their cross-border dimension, are for ever present in citizens' lives – at work, in their relations with public authorities, in the health field, when they buy goods or services, when they travel or surf the Internet. Nevertheless, many citizens are unfamiliar with data protection issues and unaware of their rights in this respect. Moreover, data protection does not usually feature in the curricula of schools and universities.

On the occasion of Data Protection Day 2011, events will be organised not only in Europe, but all over the world to raise awareness on data protection and inform citizens of their rights and good practices, thereby enabling them to exercise these rights more effectively. It presents an opportunity for citizen to become more aware of personal data protection and what their rights and responsibilities are in that regard.

The event will mark the 30th anniversary of the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, known as "Convention 108", which was opened for signature on 28 January 1981. This Convention is a cornerstone of privacy and personal data protection in Europe. It has been ratified by 43 member states of the Council of Europe and is open for signature by any country in the world.

The process of modernisation of Convention 108 has just been launched. What are our immediate common challenges? Data protection principles must be upheld in light of the impetuous technological development in our globalised world and their effective implementation reconsidered. Convention 108 constitutes an excellent basis with a possibility to further develop the existing requirements in line with current realities. The event on 28 January 2011 will mark the beginning of a public consultation organised in this context.

Effective data protection is at the heart of Council of Europe action. Ensuring effective data protection is a precondition for the free flow of information. It will help the Internet economy to flourish, transforming traditional business models and will contribute to the modernisation of countries and their economic and social well-being.

Internationally agreed minimum standards must find the right balance between security and privacy, ensure the necessary protection of individuals' personal data and support the free flow of information which is essential in today's globalised world.

Worldwide recognition of the fundamental right to the protection of personal data becomes crucial for the development and sustainability of any democratic society and serves as an additional guarantee for the effective exercise of other fundamental rights and freedoms.

BIO KATERYNA GAYEVSKA

Kateryna Gayevska is currently working at the Directorate General of Human Rights and Legal Affairs of the Council of Europe. She accompanies activities related to the functioning of the Convention for protection of individuals with regard to automatic processing of personal data (STE. No 108); in particular, she acts as Secretary of the Consultative Committee of the Convention. Prior to that, she worked as a lawyer at the Registry of the European Court of Human Rights.

www.coe.int/dataprotection



[PRIVACY]
PARTY
FRIDAY 28.01.2011
@recyclart

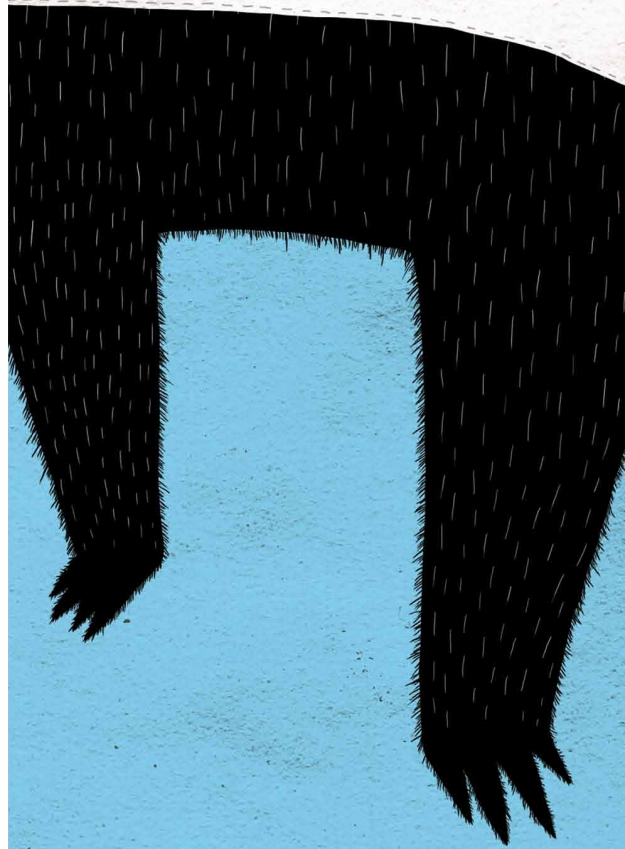
LEGOWELT NL live
ALDEN TYRELL NL
TLR NL
BAT *that's a fact
the acid mercenaries*
STEL-R

presale 8€
door 10€

recyclart: wvslimmerstraat 25 - 1000 Brussels. ♥



**PRIVACY
IS DEAD
LONG LIVE
PRIVACY**



AFTER LAST YEAR'S AMAZING SOLD OUT PRIVACY PARTY, COME AND JOIN US THIS YEAR @ RECYCLART FOR THE ULTIMATE EVENT TO CLOSE WORLD PRIVACY DAY! COME AND DANCE TO SHOW EVERYONE THAT PRIVACY IS NOT DEAD BUT STILL VERY MUCH ALIVE.

APART FROM GREAT MUSIC THERE WILL BE SEVERAL ARTISTIC INSTALLATIONS THAT WILL CONFRONT GUESTS WITH THE PRIVACY IMPLICATIONS AND SHOW THE IMPACT OF NEW SURVEILLANCE TECHNOLOGIES IN SOCIETY.

ORGANISED BY LIGUE DES DROITS DE L'HOMME / LIGA VOOR MENSENRECHTEN, VRIJE UNIVERSITEIT BRUSSEL (LSTS) AND JE M'EN FISH / CRÈME ORGANISATION.

JE M'EN FISH VZW

BART DUJARDIN

Privacy is dead long live privacy!

■ After last year's amazing sold out privacy party, come and join us this year @ Recyclart for the ultimate event to close World Privacy Day!

Come and dance to show everyone that privacy is not dead but still very much alive. Apart from great music, both live from some of the world's most renown artists in live electronic music such as Legowelt and Alden Tyrell, there will be several artistic installations that will confront guests with the privacy implications and show the impact of new surveillance technologies in society.

Recyclart, Rue des ursulines
Ursulinenstraat 25, 1000 Brussels
<http://www.recyclart.be>

Organised by Ligue des Droits de l'Homme/Liga voor Mensenrechten, Vrije Universiteit Brussel (LSTS) and Je M'en Fish/Crème Organisation

www.jemensfish.be

For those not familiar with it, Recyclart is located at Brussels Brussel Kappellekerk, by day a modern train station that transforms during the weekends and on selected weeknights into an artistical breeding pit, home to some of Brussels' most popular concerts, but also accommodating workshops, info-sessions, a restaurant and bar, and more. Dive literally into Brussels' underground by being able to party in a literally underground location, if you're early enough (or stay late enough) you might hear a train passing by over your head!

ARTISTIC CONTRIBUTIONS @CPDP2011 & PRIVACY PARTY - CURATED BY BART DE MELKER & JEROEN DE MEYER

Dusk (by Peter Beyls)

Project "Dusk" is an internet-based project developed over the last three years at the Interaction Lab of University College Ghent, Belgium. Its subject is the capture, analysis and sonification of *changes* in the harbour of Amsterdam.

"Dusk" is entirely created using live images taken from the Internet. The project is being realised as a series of photographs, a film and audiovisual installations.

PanoptiCONS (by Bas van Oerle and Thomas voor 't Hekke aka Helden)

panoptiCONS addresses the fact that we are constantly being watched by surveillance cameras in city centres. Because people don't really notice this constant breach of their privacy, the cameras don't make them feel safer. The reaction to this feeling of unsafety is often to put up more cameras. In this way the surveillance camera spreads through the city like a pest, a pest that feeds on our privacy.

To represent this, camera birds – city birds with cameras instead of heads – are placed around the conference facility, to feed on the presence of people. In addition, a camera bird in captivity is displayed to show this feeding process and to make the everyday breach of our privacy more personal and tangible.

The Surveillance Hundred Ltd. Edition (by Humans Since 1982 & Victor)

The Surveillance Light: Blending the typical appearance of a surveillance camera with a standing lamp is the basic idea behind Per Emanuelsson and Bastian Bischoff's ironic work.

In hindsight they are very proud about the fact that they have not only reached the design scene but also touched the political sphere by contributing a design piece to a social issue. In the future the lamp could be considered as a contemporary witness.

(No title) (by Peter Westenberg)

Constant VZW and the League of Human Rights organised walks through a city during which they intercept signals coming from security cameras that use a wireless network to transmit their data.

The central question during the walks was what the legal status of the cameras they came across was, and the 'video capture' action itself: do you make a violation of the privacy act when you're in a public place viewing unprotected data / received (wireless) data that you didn't ask for? And although the responsibility for securing the frequency / images / data lies with the owner of such information, as receiver you continuously have the impression that you are crossing a privacy border.

A documentary about the walks will be represented during the conference.

iTea (by Don Blaauw – Mediamatic)

It appears you are visiting your old aunt at her home. She will get to know everything there is to gossip about and she will get to know every little juicy detail. Using RFID technology, this Dutch team shows us how easy it is to read your data. If it says so about you on the internet, who is going to tell the others otherwise?

Free wireless, free refill (by Inmodis and coworkers)

Visitors are invited to come on in and drink a nice cup of coffee at this coffee house. As good old tradition goes, you get free refills, and since we're up with the modern age there's a free wireless network for all clients. We even have our own java application so you can pay for your drinks safely by creditcard online, stay up to date with our monthly promotions and enhance your lifestyle, be cool & tune in!

Transitions (by Max Pinckers)

Many photographers and painters have explored the limits and possibilities of the two dimensional portrait. All contributing to what it has become today. The question still remains; Are we able to capture a persons character. Thoughts or emotions in a single image? With the series Transitions, the artist explores this idea by making an attempt to 'catch' people as they are dissociated from the encompassing world. Deeply entranced in their own thoughts and absorbed in whatever is going through their mind.

Submerged into an 'absorptive mode', people's expressions depict themselves in an honest way unposed, unconcerned and unaware of either the photographer or the camera. The relation between the photographer and the subject has therefore been obscured. Something which provokes us to ask ourselves if these really are portraits.

Briko2K

It is in a context where machines are increasingly present in our every day lives, from clock radios to the coffee machine, from the lift to the computer ... that this project was born. To illustrate this situation, to power machines that, realistically, we surpassed in many areas, we are releasing a "punk-bots band", an attempt to machine stardom ... code, volts and rock'n'roll.

Manu Luksch

Manu Luksch, founder of Ambient Information Systems, is filmmaker who works outside the frame. The moving image, and in particular the evolution of film in the digital or networked age, has been a core theme of her works. Characteristic is the blurring of boundaries between linear and hypertextual narrative, directed work and multiple authorship, and post-produced and self-generative pieces. Through her films, telematic performances and interdisciplinary

works, Manu Luksch explores her preoccupation with the effects of emerging technologies on: daily life, social relations, and urban and political structures. Films to be shown include amongst others the Order, Spectral Children and Mapping CCTV.

Stop shouting so loud! (by Anonymous)

In all forms of communication, be aware that someone or something might hear it, spread it and use it for other purposes. Its actions might go by unnoticed at first glance, but you're never safe, be critical and stay alert at all times!

Nocturnal Animals (by Joost Jansen)

A Brussels based illustrator who loves the cosiness of his new suits. With simple markers Joost Jansen creates realistic characters who are hiding in monstrous suits. Through the proper use of these markers a colorful palette appears, fusing the pictorial whole into a dark dualistic image.

ReglSt-L01-06 (by Anna Scholiers)

The negatives were made with a pinhole camera or camera obscura (read: camera without lens) wherein light sensitive paper is lit during one minute. The camera recorded the interior and exterior of a school (classrooms, hallways, staircases, open spaces etc.) during school hours. It's an atypical view (tin box with millimeter hole) and long period of lighting ensured the spaces and people present to be photographed unwitnessed.

These contributions are on display at the CPDP2011 (25-27/01/2011) in Les Halles de Schaerbeek, Rue Royale Ste Marie 22a, 1030 Schaerbeek and at the Privacy Party (28/01/2011) in Recyclart, Rue des Ursulines 25, 1000 Brussel.

PRESENTATION OF EVENTS

Wednesday, January 19 2011, 18:00 - 20:00

Be Tech event

@Resto Bar Club L'Axess Tour & Taxis – Avenue du Port 86C 1000 Brussels

Organised by: Initiative by: Fabienne Brison • Steven De Schrijver • Thierry Léonard • Benoît Michaux Alain Strowel • Jean-Paul Triaille • Erik Valgaeren • Gerrit Vandendriessche

Contact: info@betech.be

Invitation Only

BeTech is a reference ICT network in Belgium where technology professionals can meet, exchange views and share experiences regarding new ICT trends. This is its second meeting with keynote speeches on some challenges of cloud computing. Keynote speeches by Ron Zink (Microsoft) and Achim Klabunde (European Commission) "Cloud Computing: Navigating the Privacy and Contractual Challenges."

Friday, January 21, 2011 - 18:00 - Friday, February 4, 2011 - 18:00

BROAD EXHIBITION

@TOLDI CINEMA, BUDAPEST

Organised by: Ivan Szekely, Eotvos Karoly Policy Institute
<http://www.pet-portal.eu>

Contact: szekelyi@ceu.hu

Open Event

A selection from the creative works submitted to the amateur contest announced in the framework of the Broadening the Range Of Awareness in Data protection (BROAD) project. Drawings, illustrated stories, photos, digital montages, linocuts, silk screen prints, collages exhibited in the cinema hall.

Monday January 24 2011, 09:00 - 18:00

ENISA workshop on data breach notifications

@Stanhope Hotel, Rue du Commerce 9, 1000, Brussels
Organised by: European Network and Information Security Agency

<http://www.enisa.europa.eu/act/it/data-breach-notification/>

Contact: sta@enisa.europa.eu

Workshop on the future of notifications about data breaches. On the one hand it will provide an opportunity to present the results of ENISA work in this area, while on the other it will serve as a forum for the exchange of ideas on the way forward. Please register before the 20th January 2011.

Tuesday 25 January-Thursday 27 January 2011

Computers, Privacy & Data Protection 2011

Data Protection: in Good Health?

@Les Halles de Schaerbeek Rue Royale Ste Marie 22a 1030 Schaerbeek

Information and registration at info@cpdpconferences.org, www.cpdpconferences.org, tel. +32 2 629 20 93.

Computers, Privacy and Data Protection – CPDP 2011 – is a three-day conference organized by academics from all over Europe, with the ambition of becoming Europe's most important forum for academics, practitioners, policy-makers and advocates. Discussions will range from technology to philosophy.

Tuesday 25 January 2011, 18h15

Book Launch: Check in / Check out. The Public Space as an Internet of Things

@Les Halles de Schaerbeek, Rue Royale Ste Marie 22a 1030 Schaerbeek

18.15 opening prof. Frans Brom, Head of Technology Assessment at the Rathenau Institute

18.20 Presentation "Check in / check out" Christian van 't Hof, senior Researcher Rathenau Institute and author of the book

18.35 First copy will be received by Gerald Santucci,
Head of Unit Enterprise Networking and RFID,
European Commission
18.50 Responses from expert panel
19.15 close

Tuesday 25 January 2011, 20h00

Public Debate on Surveillance in Flanders and The Netherlands

@Beursschouwburg (in Dutch), A. Ortsstraat 20 – 28,
1000 Brussel
registration via info@deburen.eu

Are we living in a control society in which Big Brother watches us continuously? Should we resist the upcoming surveillance society before it's too late or is it a necessary evil to protect our security? Is it necessary to give up more and more freedoms (such as privacy and non-discrimination) to protect us from criminals and terrorist or are there alternative ways, which protect both our freedoms and our security? During the debate these and other questions and several current surveillance issues will be discussed. There will be enough time for questions and reactions from the audience.

Moderated by Paul De Hert (Vrije Universiteit Brussel/
Universiteit Tilburg)

Confirmed speakers:

Raf Jespers (author Big Brother in Europa and lawyer
Progress Lawyers Network)
Bart Jacobs (Radbout Universiteit Nijmegen)
Gerrit-Jan Zwenne (lawyer, Bird & Bird),
Bart de Koning (freelance journalist),
Christian van 't Hof (Rathenau Instituut),
Quirine Eijkman (NJCM)

Tuesday 25 January 2011, 20h20

Pecha Kucha Night Brussels

@Les Halles de Schaerbeek, Rue Royale Ste Marie
22a 1030 Schaerbeek
registration via <http://pechakucha.architempo.net>

Pecha Kucha is Japanese for the background murmurings that you hear during conversation. The concept was devised in 2003 by architects Astrid Klein and Marc Dytham who wanted to offer a platform for young architects in their night club, Superdeluxe. Since then the phenomenon has been taken up in more than 380 cities around the world. The Pecha Kucha Nights Brussels were launched in 2007 by multimedia-engineer Alok Nandi and CROSSTALKS.

26-27-28 January 2011, 11:00-15:00

EDPS Information Stand in EU Institutions

@Council (26/01): Justus Lipsius Building, Atrium;
European Commission (27/01): Berlaymont Building,
Piazza, close to the restaurant; European Parliament
(28/01): ASP Building, main street.

Organised by: EDPS/DPO

Admission: entry badge needed to access EU
institutions buildings.

The European Data Protection Supervisor (EDPS) and the Data Protection Officer (DPO) of the concerned institution will hold an information stand on three consecutive days in the Council of the European Union (26 January), the European Commission (27 January) and the European Parliament (28 January).

The aim is to raise awareness among the EU staff about their rights and obligations regarding data protection. It is also an opportunity to meet and discuss with the legal advisors from the EDPS and with the institution's Data Protection Officer.

Thursday 27 January 2011, 18h00

Round-table on Body Scanners

@CEPS (Centre for European Policy Studies), Place du Congrès 1, 1000 Brussels
registration via miriam.mir@ceps.eu

Organised by VUB-LSTS, CEPS and PRIO, within the framework of INEX activities Hosted by Elspeth GUILD and moderated by Valentina POP

Panel Elspeth GUILD, Radboud University Nijmegen and CEPS (NL and BE), Marc ROTENBERG, EPIC (USA), Mark SALTER, University of Ottawa (CA), Martin SCHEININ, European University Institute (IT), Claudia FUSCO, European Commission DG MOVE (EU), Jim GAUDOIN, L-3 Security & Detection Systems (UK)

Friday 28 January 2011, 22h00

Privacy Party

@Recyclart, Rue des Ursulines 25, 1000 Brussels (8 EUR before midnight, afterwards 10 EUR),
tickets via www.recyclart.be

Privacy is dead long live privacy!

After last year's amazing sold out privacy party, come and join us this year @ Recyclart for the ultimate event to close World Privacy Day!

Come and dance to show everyone that privacy is not dead but still very much alive. Apart from great music, both live from some of the world's most renown artists in live electronic music such as Legowelt and Alden Tyrell, there will be several artistic installations that will confront guests with the privacy implications and show the impact of new surveillance technologies in society.

Organised by Ligue des Droits de l'Homme/Liga voor Mensenrechten, Vrije Universiteit Brussel (LSTS) and Je M'en Fish/Crème Organisation

Friday January 28 2011, 09:00 - 13:30

Joint High Level Meeting on Data Protection Day

@European Commission – Charlemagne Building meeting room Alcide de Gasperi – 2nd floor 170, Rue de la loi, 1049 Brussels

Organised by: European Commission & Council of Europe

<http://www.data-protection-day.net/home.jsp>

Contact: just-dp-conference@ec.europa.eu

Invitation Only

Mr Thorbjørn Jagland, Secretary General of the Council of Europe, and Ms Viviane Reding, Vice-President of the European Commission, have decided to seize the opportunity of the Data Protection Day to organise a high-level joint event to allow to both institutions joint forces and to promote the fundamental right to data protection.

Friday, January 28, 2011 - 14:00

VON HACKING BIS TRACKING - DATENSCHUTZ UND SICHERHEIT BEIM BETRIEB VON INTERNET-ANGEBOTEN

@LANDTAG RHEINLAND-PFALZ, DEUTSCHHAUS-PLATZ, 55116 MAINZ

Organised by: Landesbeauftragter für den Datenschutz Rheinland-Pfalz

<http://www.datenschutz.rlp.de>

Contact: poststelle@datenschutz.rlp.de

Open Event

Eine Informationsveranstaltung für Web-Designer und Datenschutzbeauftragte

Friday, January 28, 2011 - 17:30 - 19:00

DON'T LET THEM KNOW ALL ABOUT YOU!

@TOLDI CINEMA, BUDAPEST

Organised by: Ivan Szekely, Eotvos Karoly Policy Institute

<http://www.pet-portal.eu>

Contact: szekelyi@ceu.hu

Open Event

Screening and discussion with creative artists. Privacy videos, experimental films and other works created in the framework of the Broadening the Range Of Awareness in Data protection (BROAD) project will be shown with an open discussion with the creators.

Tuesday, February 1, 2011 - 10:00 - 16:00

DATA PROTECTION ACT (DPA) 1998: AN A-Z GUIDE

@THISTLE HOTEL, MARBLE ARCH, LONDON

Organised by: Act Now Training Ltd

<http://www.actnow.org.uk/courses/505>

Contact: info@actnow.org.uk

This workshop takes a thorough look at the Data Protection Act 1998 (DPA) and its codes of practice. We will also examine the link with other legislation such as Freedom of Information and Human Rights. The latest issues and guidance from the Commissioner will also be discussed. This workshop is suitable for those with little or no knowledge of the DPA. Accredited by SRA and ILEX with 4.5 hours CPD



LSTS

LAW, SCIENCE,
TECHNOLOGY &
SOCIETY STUDIES
VRIJE UNIVERSITEIT BRUSSEL
BELGIUM

Booklet distributed by the Law
Science Technology & Society
Research Group (LSTS)