

9th Symposium on Privacy and Security

Wednesday/Thursday, 15/16 September 2004
Swiss Federal Institute of Technology (ETH) Zurich

Everything under control?

- Total surveillance or blind trust? Conflict potential between employers and employees
- Is “whistleblowing” in the interest of corporate governance? Do the “traitors” need better protection, or do we need better protection against them?
- Security and freedom: transatlantic differences
- Firsthand reports from business and public administration on the subjects of control, surveillance, security and data protection

www.privacy-security.ch

The symposium is made possible by

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Swiss Re



PRICEWATERHOUSECOOPERS 



Computer Associates®

Media partner

d i g m a
Zeitschrift für Datenrecht und Informationssicherheit

in cooperation with the European Academy
for Freedom of Information and Data Protection, Berlin/Germany

“Privacy and security are key themes in the development of the information and communication society.”

Federal Councilor Samuel Schmid, Member of the Swiss Government, Head of the Swiss Federal Department of Defence, Civil Protection and Sports, Berne/Switzerland
Dr Markus Nötter, Member of the Government of the Canton of Zurich, Head of the Ministry of Justice and of the Interior of the Canton of Zurich, Zurich/Switzerland
Prof Olaf Kübler, President of the Swiss Federal Institute of Technology Zurich, Zurich/Switzerland
Prof Peter Forstmoser, University of Zurich, Chairman of the Board of Directors of Swiss Re, Zurich/Switzerland

SPS Partners

Premium partners



Superior partner

Media partner



in cooperation with the European Academy for Freedom of Information and Data Protection, Berlin/Germany

SPS Target audience

The need for control in business and government is increasing. This symposium offers answers and solutions for that challenge. It is directed at all decision-makers, project managers and specialists in the fields of technology, compliance, law, risk management, human resources, marketing and consultancy; at IT and data protection officers working in business, politics and public administration; and at all those wishing to become better informed with regard to data protection and information security.

SPS Programme overview

Everything under control?	
Wednesday, 15 September 2004	Thursday, 16 September 2004
Carte blanche: Challenges and controversy	Is everything under control?
Technological developments are radically impacting business and government. What will be the major challenges of the next decade? What will be the effect of the emerging (or re-emerging) conflict between the generations, and between Europe and the US?	Breaking the rules is sometimes necessary, but it poses a dilemma. Should there be protection for the “traitorous” whistleblowers in business and government? How much control is enough? How will data security be affected by regulations that require controls stringent enough to protect the interests of the stakeholders?
Is everything under control in the workplace?	Firsthand reports
Technology would allow the employee, as an inherent “risk factor”, to be monitored almost totally. But what is permissible? What is necessary? What is the right way between total surveillance and blind trust?	How are controls actually implemented in private business and public administration? How do such checks relate to other elements of corporate governance? What are the success factors for a Critical Incident Reporting System?
Practice forum: Controls in the workplace	Panel discussion: Everything is under control... Really?
You ask – experts answer: What controls are permitted in the workplace?	Protection for “traitors” or sharper controls to protect against “traitors”? Who keeps the keepers? How much control is enough?
SPS InfoPoints	
Leading providers present their solutions.	

Symposium language: German and English with simultaneous interpreting into the other language. Presentation materials in the symposium documentation are generally in the language of the presentation.

From 08.30	Check-in, coffee, opportunity to visit the "SPS InfoPoints"
09.15	Opening
SPS Carte blanche: Keynote reports	
	<p>Information and communications technologies (ICT) have significant growth-generating potential. Their further development will impact business and government to an extent we can hardly imagine. This means that the importance of information security and integrity will increase. ICT will also confront society and government with new challenges.</p> <p>The emergence of new conflicts will make it more difficult to find viable, long-term solutions. One of the most important of these conflicts is the generation gap. To one generation, "Big Brother" means George Orwell; to another, it's a TV programme. Similarly, the risks of the information society are perceived in completely different ways by the cell-phone generation and the older age set. Does data protection have a future?</p> <p>Another opening split – or one that is reasserting itself in the public consciousness – relates to the different meaning of "freedom" and "security" on the two sides of the Atlantic. What will these new (or newly perceived) splits mean as we try to master the challenges of the information society?</p>
09.30	<p>Security and integrity of information: a rising value</p> <p>André Kudelski, Chairman of the Board and CEO of Kudelski Group, Cheseaux-sur-Lausanne/Switzerland</p> <p><i>In your country or in your town you know for example which information you may trust, or which document is real. This is possible when you consider one country or one culture. However in a global environment of six billion people you cannot apply the same rules. To differentiate the true from the false information you need to get this information from a reliable source and in a secure form based on encryption. More than just reliability and trust, you need to have secure channels to communicate with your home and your trusty partners to avoid losing your ground. This is a growing need in a globalized environment.</i></p>
10.10	<p>Does data protection have a future?</p> <p>Prof Spiros Simitis, Johann Wolfgang Goethe University, Chairman of the National Ethics Council, Frankfurt</p> <p>One generation has read Orwell; has experienced firsthand the ravenous information appetite of security agencies and public administration; has seen the explosion of marketing and advertising strategies. The younger generation has grown up with SMS, e-mail and camera-equipped cell phones. Will generational differences in the perception of risk pose future challenges to the protection of privacy?</p>
10.50	Networking: coffee break, opportunity to visit the "SPS InfoPoints"
11.20	<p>Freedom and security in the US and in Europe</p> <p>Dr Gret Haller, publicist, author of <i>Die Grenzen der Solidarität, Europa und die USA im Umgang mit Staat, Nation und Religion</i>, (The Limits of Solidarity: State, Nation and Religion in Europe and the US), Berne/Switzerland</p> <p>The two sides of the Atlantic have different approaches to the privacy/security problem. Now – most notably since 11 September 2001 – similar differences are emerging with regard to freedom/security, although these were perceived in essentially the same way during the Cold War. Yet, when we look at the way the religious dimension is approached, for example, or compare the "Federalist Papers" with the achievements of the French Revolution, isn't the difference much older?</p>
SPS Overview	
	Everything under control?
12.00	<p>Is everything under control? A corporate surveillance survey</p> <p>Prof Edgar Fluri, titular professor in public accounting at the University of Basel; Chairman of the Board, PricewaterhouseCoopers AG, Zurich/Switzerland</p> <p>The day when larger organisational units were "black boxes" is long over. Under the rubric "corporate governance", a concern's management (and public administration managers as well) must implement the necessary controls to ensure that they can fulfill their responsibility to their stakeholders – whether shareholders, investors or taxpayers. What role do various elements play – elements such as internal control, audit compliance, risk management, corporate reporting or management monitoring? Where are their limits?</p>
12.30	Networking: buffet lunch, opportunity to visit the "SPS InfoPoints"

SPS Update: Technical, legal and psychological issues

Is everything under control in the workplace?

Any successful manager of a company or an administrative department must have access to the necessary information. Protecting the shareholder interests goes beyond having an efficient organisational structure and carefully selected, trained personnel. The members of executive boards and boards of directors must also have sufficient control over the risks they run, and ensure the quality of all activities in their remit. This is the reason for auditing the way resources are committed: IT, finances, information, etc. Inevitably, employee behaviour is scrutinised as well, because it is employees who use these resources carefully or less carefully; who run risks deliberately or recklessly; who themselves become risk factors.

Yet nowhere is there more uncertainty than in the area of employee monitoring in the workplace. With today's technology, virtually everything can be kept under surveillance – but what is permissible? Is there no longer any privacy on the job? And in the final analysis, is workplace monitoring efficient and effective – or does it create a climate of mistrust that will ultimately kill employee motivation and initiative?

13.50 **“There is no privacy in the workplace” – or is there?**

Dr Johann Bizer, Schleswig-Holstein Independent Centre for Data Protection, Kiel/Germany

Employees are becoming ever more entangled in a net of workplace controls: through monitoring of Internet use and e-mail traffic; through the use of spyware; through biometric identification systems and electronic access systems; through video monitoring and drug screening. Faced with these systems, can we still speak of privacy in the workplace? How is legislation in Germany and the European Union reacting to these risks?

14.20 **Surveillance in the workplace: The legal framework – labour law, data protection law**

Prof Thomas Geiser, Research Group for Labour and Labour Law, University of St. Gallen, St. Gallen/Switzerland

Whoever monitors employees should be aware of the laws that govern this area. Indeed, some laws even require employers to exercise supervision over their employees. But where are the limits of the admissible in monitoring the workplace? What is the legal framework as defined in labour law, in data protection law, and in the recommendations of the International Labour Organisation?

14.50 Networking: coffee break, opportunity to visit the “SPS InfoPoints”

15.20 **Between total surveillance and blind trust: technical monitoring in the workplace and the underlying concept of the individual**

Prof Gudela Grote, Institute of Labour Psychology, ETH Zurich, Zurich/Switzerland

Diverse employer cultures have developed as business and government try to come to grips with a very complex risk factor: their employees. Should employees be trusted blindly, or watched at every turn? What does the use of workplace surveillance say about our concept of the individual? And is the use of monitoring technology efficient or counterproductive? Where are the limits of surveillance from the perspective of (labour) psychology?

SPS Practice forum: Q&A

15.50 **Is “everything under control” in the workplace? You ask – experts answer**

Experts:

Dr Johann Bizer, Schleswig-Holstein Independent Centre for Data Protection, Kiel/Germany

Prof Thomas Geiser, Research Group for Labour and Labour Law, University of St. Gallen, St. Gallen/Switzerland

Peter Helbling, Head of Legal Services, Federal Office of Personnel, Berne/Switzerland

N.N., (Corporate human resources manager)

Moderator:

Dr Beat Rudin, lecturer at the University of Basel; Managing Director of the Symposium on Privacy and Security, Basel/Schweiz

How can the diverse, often conflicting interests of employers and employees be optimally harmonised? Concrete examples will be used. How is employee monitoring carried out in business and government?

You may send your questions to the experts before the conference: visit symposium@privacy-security.ch

16.45 End

Networking: drinks, opportunity to visit the “SPS InfoPoints”

From 08.30	Check-in, coffee, opportunity to visit the "SPS InfoPoints"
09.15	Welcome address
SPS Update: Challenges and solutions	
	<p>Everything under control?</p> <p>No scandal like Enron was necessary to show how important controls are. However, such scandals have recently triggered regulatory activity aimed at providing controls capable of protecting stakeholders and shareholders, whether this takes the form of the Sarbanes-Oxley Act in the US, or European or Swiss legislation. Indeed, this issue gives rise to many questions: How will such regulations affect information security? What would a controlled way of handling information risks look like? How can we ensure that internal warnings of malfeasance and error are taken seriously? Should we protect "traitors"?</p> <p>A view of current practice will show how controls are implemented in business and government environments. What relationship do controls have to other elements of corporate governance? What are the success factors for a Critical Incident Reporting System?</p>
09.20	<p>Everything under control? Rule-breaking is a necessity</p> <p><i>Prof Günther Ortman, Helmut Schmidt University – Universität der Bundeswehr Hamburg, Hamburg/Germany</i></p> <p>Organisations have always been concerned about control. Earlier, it may have been driven by a misanthropic picture of the individual, or the fear of employee indolence; today, the focus is increasingly on the upper levels of the hierarchy. Yet at the same time, we are finding that controls are powerless. We are confronted with a paradox: employees in organisations, whether business or governmental, must break rules in order to maintain the functional viability of the organisations themselves. Yet this only reformulates the age-old question: Who will keep the keepers?</p>
09.50	<p>Who are the "traitors" – whistleblowers, or those they expose?</p> <p><i>David Nussbaum, CEO Transparency International, Berlin/Germany</i></p> <p>Corporate leaders have often regarded whistleblowers as disloyal troublemakers, yet they can provide a powerful impetus towards corporate integrity and vital information in the fight against corruption and unethical practices. Protection for whistleblowing has been lacking, in both private and public sectors, and is notoriously difficult to implement. How can those who take the risks inherent in whistleblowing be protected, as a rarely known element of the Sarbanes Oxley Act now requires? How do we protect companies and administration from unjustified accusations? Where does the balance lie?</p>
10.20	Networking: coffee break, opportunity to visit the "SPS InfoPoints"
10.50	<p>Controlling information security in highly sensitive areas</p> <p><i>Adrian Turtschi, Head of Strategic Information Management, Swisscom AG, Berne/Switzerland</i></p> <p>The significance of information security is intimately connected with the significance of information. Telecommunication service companies and institutions are an increasingly sensitive area, due to their explosive growth if for no other reason. They require – beyond the usual legal requirements and audits – a number of concepts, instruments and mechanisms. May this be the reason why information security is the very core interest of information companies, whether in the hardware or software area, whether manufacturer or service provider? Is a global enterprise a special case as regards information security? Do they have unlimited resources for security at their disposal? How can information security be integrated organically into processes and services – beyond the lifetime of those services, beyond the company's own contribution to the value chain? How can this be coordinated?</p>
11.20	<p>Information risk control: Controlled handling for critical business information</p> <p><i>Dr. Pierre Brun, Partner, PricewaterhouseCoopers AG, Zurich/Switzerland</i></p> <p>Information is one of the most important intangible assets that business or government possesses. The controlled handling of threats and risks is of decisive importance, both with regard to distinguishing an organisation from its competitors, as with regard to potential litigation. Yet catalogues of these information assets, with classification and evaluation, are frequently incomplete and out of date. What risks confront the operational side of a business? What effect do they have? And with what approaches and methods can they be controlled?</p>
11.50	Networking: buffet lunch, opportunity to visit the "SPS InfoPoints"

SPS Solutions: A look at business and government

13.20 Firsthand report: Controlling data traffic – and who controls the controllers?

Dr Hannes P. Lubich, Private Lecturer, ETH Zurich, Computer Associates AG, Kloten/Switzerland

Networks monitor their data traffic, of course... but how do they do it? What types of analysis are used? What is technically feasible? And because this touches on the employees' communication habits, as well as privacy protection issues, we must ask, "How can these controls be brought under control?" – in other words, "Who keeps the keepers?"

13.45 Firsthand report: Tracking down white-collar crime in government

Michel Huissoud, Vice Director, Swiss Federal Audit Office, Berne/Switzerland

Government, too – at the federal level as well as in the cantons and localities – is not immune to white-collar crime. What measures, what resources does the Swiss government use to ensure that shady wheeling and dealing is found out and prevented or prosecuted?

14.10 Firsthand report: Good corporate citizenship in a global corporation

Nico Sieben, Group Compliance Officer, Novartis International AG, Basel/Switzerland

The "corporate citizenship" concept is today an important element in implementing Novartis' "global compact". Ideally, it would only be necessary for everyone in the company to keep to its policies and the law. What mix of preventive measures, organisation and control does a global corporation use to ensure that the incentives for its employees to do just that are greater than the temptations to infringe upon them? What are the critical factors in such a system?

14.35 Networking: coffee break, opportunity to visit the "SPS InfoPoints"

15.05 Firsthand report: Handling mishaps and near-misses – Critical Incident Reporting Systems (CIRS)

Dr Georg von Below, MD, Area Head, Quality Management, Swiss Medical Association (FMH), Berne/Switzerland

Devastating mishaps can often be traced back to "insignificant" events that are actually fairly common. Couldn't a "Critical Incident Reporting System" recognise error patterns early enough to prevent the occurrence of a catastrophe?

What are the success factors for improved error handling? And how can we get around a dilemma: that a CIRS is supposed to collect just the information that prosecuting attorneys and liability lawyers want to get their hands on?

SPS Arena

15.30 Panel discussion: Everything is under control... Really?

Moderator:

Medard Meier, publicist, former Editor-in-Chief, BILANZ, Küssnacht/Switzerland

Panelists:

Prof Gudela Grote, Institute for Labour Psychology, ETH Zurich, Zurich/Switzerland

National Councillor Hans Kaufmann, Consultant, Kaufmann Research AG, Wettswil/Switzerland

National Councillor Susanne Leutenegger Oberholzer, Judge, Muttenz/Switzerland

National Councillor Ruedi Noser, Noser Group, Hombrechtikon/Switzerland

Prof Günther Ortman, Helmut Schmidt University – Universität der Bundeswehr Hamburg, Hamburg/Germany

Thomas Pletscher, Head of Legal Issues, economiesuisse, Swiss Business Federation, Zurich/Switzerland

Dr Bruno Porro, Chief Risk Officer Swiss Re, Zurich/Switzerland

Protection for "traitors" or sharper controls to protect against "traitors"? Who keeps the keepers? How much control is enough?

16.35 Wrap-up

Dr Johann Bizer, Schleswig-Holstein Independent Centre for Data Protection, Kiel/Germany

16.45 End

Networking: drinks, opportunity to visit the "SPS InfoPoints"

The symposium is made possible by



Additional information: www.privacy-security.ch
 German language version: www.privacy-security.ch



"The Symposium on Privacy and Security is intended to offer the fields of science, business, administration and politics an international platform for the discussion of the key themes of privacy and security."

Dr Bruno Baeriswyl

President of the foundation council, privacy commissioner for the Canton of Zurich, editor of the magazine *digma*, Zurich/Switzerland

Prof Dr Ueli Maurer

Member of the foundation council, professor of computer science and head of the Information Security and Cryptography Research Group, Swiss Federal Institute of Technology (ETH) Zurich, Zurich/Switzerland

Dr Beat Rudin

Member of the Foundation Council, Managing Director of the Symposium on Privacy and Security, lecturer at the University of Basle, editor of the magazine *digma*, Basle/Switzerland

3DS Advisory Board

"We support the foundation so that in future the most contemporary and relevant topics for society and the economy can be taken up and addressed in depth by first-class speakers."

Dr Pierre Brun, PricewaterhouseCoopers AG, Partner, Zurich/Switzerland

Prof Alfred Büllsbach, DaimlerChrysler AG, Chief Officer Corporate Data Protection, Stuttgart/Germany

Martin Fricker, Swiss Re, Group IT Security Officer, Zurich/Switzerland

Prof Hansjürgen Garstka, Commissioner for Data Protection and Freedom of Information of the State of Berlin, Berlin/Germany

Dr Hannes P. Lubich, Private lecturer ETH Zurich, IT Security Strategist, Computer Associates AG, Kloten/Switzerland

Dr Armgard von Reden, IBM Germany, Director Public Affairs, Berlin/Germany

Walter Widmer, UBS AG, IT Security Risk Management WM&BB, Zurich/Switzerland

3DS Organisation

Date

Wednesday, 15 September 2004 – Thursday, 16 September 2004

Venue

Auditorium Maximum, Swiss Federal Institute of Technology (ETH), Main Building, Rämistrasse 101, 8006 Zurich

Fees

- Symposium on Privacy and Security:
15–16 September 2004
CHF 1'080.00 (plus 7.6% VAT on CHF 160.00)
CHF 980.00 (plus 7.6% VAT on CHF 160.00) for previous subscribers of the journal *digma*
- Individual days:
either 15 September 2004 or 16 September 2004
CHF 690.00 (plus 7.6% VAT on CHF 80.00)
CHF 590.00 (plus 7.6% VAT on CHF 80.00) for previous subscribers of the journal *digma*

All fees include admission to the relevant event, symposium documentation, refreshments, buffet lunch and a 2005 subscription to *digma**, the journal for data law and information security.



* not applicable to *digma* subscribers receiving the "digma discount" on the symposium fees.

Discounts (can be combined)

- CHF 100.00 "digma discount" for previous subscribers of the journal *digma*
- 10% early booking (registrations received no later than 31 July 2004)

Registration

Deadline for registration: 27 August 2004

Register online at: www.privacy-security.ch

or use the attached registration form.

An invoice will be sent upon receipt of registration. The number of participants is limited: registrations will be accepted on a first-come, first-served basis.

Cancellations

50% refund for cancellations reaching us from 16–31 August 2004. No refunds for cancellations after this date. Participation is transferable.

How to get there

Few parking spaces are available near the ETH Zurich. You can easily reach the symposium venue by public transport (http://www.ethz.ch/about/location/ethzentrum/index_EN):

- From Zurich Main Station's Bahnhofplatz tram stop, by Tram No 10 (towards Seebach); or from Zurich Main Station's Bahnhofstrasse tram stop, by Tram No 6 (towards Zoo): get off at ETH/Universitätsspital. From Central, take the Polybahn (funicular) to the Polyterrasse
- Arrival by plane: Take the train from Zurich Airport to Zurich Main Station (about 8 minutes)

Hotels

Hotels can be reserved through Zurich Tourism www.zuerich.com, E-Mail: hotel@zuerich.com
Tel. +41 (1) 215 4040
Fax +41 (1) 215 4044

The Symposium on Privacy and Security offers leading companies the opportunity to present their solutions at InfoPoints in the foyer.

The full list of exhibiting companies will be posted at

www.privacy-security.ch

“SPS InfoPoints” organisation, information and registration

Huber & Partner PR AG, Forchstrasse 239, 8032 Zurich/Switzerland
 Tel. +41 (1) 385 9999, Fax +41 (1) 385 9995
 info@huber-partner.com



The symposium is made possible by



Additional information: **www.privacy-security.ch**
 German language version: **www.privacy-security.ch**

Registration

I would like to attend the Symposium on Privacy and Security on 15/16 September 2004 in the Auditorium Maximum at the ETH Zurich.

Mrs Mr

Surname _____ First name _____ Academic title _____

Company, organisation _____

Position _____ Address _____

City, post code _____ E-mail _____

Business tel. _____ Business fax _____

Date _____ Signature _____

Symposium on Privacy and Security

- Whole symposium, 15-16 September 2004
CHF 1,080.00 (plus 7.6% VAT on CHF 160.00)
- Whole symposium, 15-16 September 2004
CHF 980.00 (plus 7.6% VAT on CHF 160.00) for previous subscribers of the journal digma

Individual days

- First day only: 15 September 2004
CHF 690.00 (plus 7.6% VAT on CHF 80.00)
- First day only: 15 September 2004
CHF 590.00 (plus 7.6% VAT on CHF 80.00) for previous subscribers of the journal digma
- Second day only: 16 September 2004
CHF 690.00 (plus 7.6% VAT on CHF 80.00)
- Second day only: 16 September 2004
CHF 590.00 (plus 7.6% VAT on CHF 80.00) for previous subscribers of the journal digma

Online registration: www.privacy-security.ch

or send the registration form to:

Symposium on Privacy and Security
 c/o Stiftung für Datenschutz und Informationssicherheit
 Kirschgartenstrasse 7, Postfach
 CH-4010 Basel
 Switzerland

or by fax to +41 (61) 270 1771



Symposium on Privacy and Security

Premium partners

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Swiss Re



PRICEWATERHOUSECOOPERS 

Superior partner



Computer Associates®

Media partner

Zeitschrift für Datenrecht und Informationssicherheit
d i g m a

in cooperation with the European Academy
for Freedom of Information and Data Protection, Berlin/Germany

Date for your diary:

10th Symposium on Privacy and Security: 31 August–1 September 2005