

Beyond the security vs. privacy debate

Report
October 2013



The views expressed in this report are personal opinions of the speakers and not necessarily those of the organisations they represent, nor of the Security & Defence Agenda or Transparency International, their members or partners.

Reproduction in whole or in part is permitted, providing that full attribution is made to the Security & Defence Agenda and to the source(s) in question, and provided that any such reproduction, whether in full or in part, is not sold unless incorporated in other works.

A ***Security & Defence Agenda*** Report

Rapporteur: **David Koczij**

Photos: **Jan Van de Vel**

Publisher: **Geert Cami**

Project Manager: **Andrea Ghianda**

Project Assistant: **Paul Cohen**

Date of publication: **October 2013**

Beyond the security vs. privacy debate

In light of the recent NSA scandal, the issue of citizen and consumer trust in government has taken centre stage participants heard at the Security and Defence Agenda debate 'Beyond the Security vs. Privacy Debate'. "Public authorities argue that they need to collect enormous data sets to be able to protect the well-being of their citizens," stressed **Jens-Henrik Jeppesen**, Director of European Affairs at the Centre for Democracy and Technology, but without legal oversight. "The issue has become muddled to the point where international and government agencies are breaking laws concerning citizen rights in order to defend those same laws," said **Joe McNamee**, Executive Director at European Digital Rights. "What are needed are necessity, proportionality, and a fresh look at digital privacy rights, based on international human rights." "This is no time for silence. People on the internet are almost entirely consumers and not citizens. The time is coming for us to change that" noted **Jane Lute**, former Deputy Secretary of Homeland Security at the US Department of Homeland Security.

Speakers			Moderator
			
Jens-Henrik Jeppesen <i>Director of European Affairs</i> Centre for Democracy and Technology	Jane Holl Lute <i>Former Deputy Secretary of Homeland Security</i> United States	Joe McNamee <i>Executive Director</i> European Digital Rights	Giles Merritt <i>Director</i> Security & Defence Agenda

The SDA would like to thank those who have supported the cyber initiative from its inception:

Finmeccanica | Huawei | IBM | McAfee | Microsoft | NATO | Raytheon | TNO
Europe's World

Beyond the security vs. privacy debate



In the wake of the recent revelations concerning the United States' National Security Agency (NSA) scandal, new questions are coming to light about cyber-security, participants heard at the Security and Defence Agenda's (SDA) debate '**Beyond the security vs. privacy debate**'.

"The cyber-security problem is symptomatic of a much wider change in human society," said moderator **Giles Merritt**, Director of the SDA. "Pre-internet national divisions were something that our laws and societies had adapted to quite well. We are now grappling with the big questions of how to deal with the ethics of the internet that transcends these boundaries, with the only certainty being that these questions will become more and more important as the world becomes more and more wired."

In reality, noted **Jens-Henrik Jeppesen**, Director of European Affairs at the Centre for Democracy and Technology, there is no debate between security and privacy. "The latest revelations concerning government interference in standards of encryption technology have quite clearly demonstrated that both security and privacy can be undermined by the same actions."



"There are 7 billion of us on this planet and there are only five things that claim the active affiliation of a billion or more people – being Chinese, Indian, Catholic, Muslim, and being a Facebook user"

Jane Lute

Furthermore, added **Joe McNamee**, Executive Director of European Digital Rights, "our societies are based on democracy, which requires freedom of speech, which in turn requires privacy. If we do not have privacy, we are missing a cornerstone on which our society is based. In other words, when we trade privacy for security, we are in fact seeking to trade security (of our individual rights) for (national) security."

The conversation about cyber-security has been held behind closed doors for far too long, indicated **Jane Lute**, former Deputy Secretary of Homeland Security, Department of Homeland Security. As the role of government in the lives of citizens changes in tandem with the spread of the internet and increases in data storage capacity and cloud computing, space must be made for a more open and inclusive debate.



The impact of global trends on the security vs. privacy debate

As the global penetration of the internet approaches 35%, many countries are witnessing a massive cyber-awakening. This massive growth in internet use – which has reached as high as 70% penetration in North America and Europe – is contributing to the changing role of governments in the lives of citizens, noted Lute.

“There are 7 billion of us on this planet and there are only five things that claim the active affiliation of a billion or more people – being Chinese, Indian, Catholic, Muslim, and being a Facebook user,” she stressed. “Of these groups, only Facebook knows its users to any degree; Facebook knows more about its users than national governments typically know about their citizens and our understanding of people online is almost entirely as consumers, not as citizens -- and that must change.



It is excessively difficult to find out exactly what the oversight mechanisms are and how effective they are. This is not a state we can live with as global citizens.”

Jen-Henrik Jeppesen

In the digital age, the most powerful actors in cyber-space are high-tech companies. Google, Facebook, and Yahoo, among others, all control more data and connect more individuals than any single government. “Powerful cyber-actors prove that it is the power to connect, not the power to protect, that matters online,” she added. “This is meaningful because governments are what they are in part because they have legitimate consolidated control of the power to protect.”

For most of the history of the net, the U.S. government that had considerable political and administrative control over the Internet, noted McNamee. The fact that the internet has been able to grow into such an open, inclusive and global platform is owed greatly to the fact that the U.S. government was able to resist the temptation to exploit that control.

Unfortunately, he added, this benevolent stewardship has been lacking in recent years, as witnessed by the NSA scandal. “We are now faced with breaches of international law and the undermining of everyone’s information security,” he said. “This is not privacy vs. security. This is privacy, transparency, the rule of law, and security against a corrosive, out-of-control security

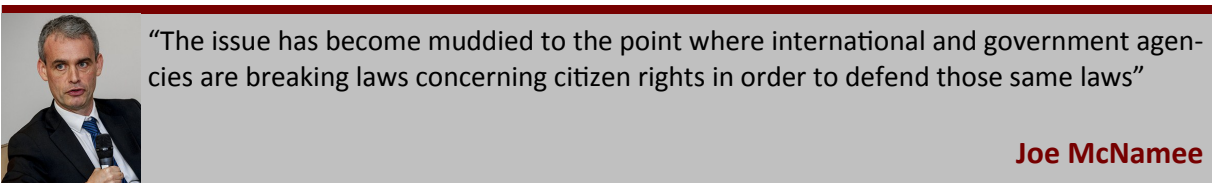
apparatus.”

There are four main trends underlying this paradigm shift and calling into question the status quo of privacy and cyber-security, Jeppesen indicated:

- 1) Revolutions in storage and data analysis, combined with fears about terrorism and more mundane demands of public-sector organisations. Public authorities argue that they need to collect increasingly massive amounts of data – held mostly by the private sector – in order to extract crucial pieces of information.
- 2) Transport implications of government demands for data pose unresolved challenges. Any transaction on the internet involving government entities from various countries expressing a legitimate interest in citizens from different geographical areas is likely to create problems for the companies that hold that data.
- 3) Fibre optic networks, web-based email and other cloud services. Data is increasingly stored and transmitted across borders and through transit countries, contributing to unclear definitions of jurisdiction as concerns data retrieval.
- 4) International laws and agreements have allowed governments much greater powers to collect data in the name of national security than in ordinary criminal cases.

“What we are seeing,” he concluded, “is a fundamental shift in the surveillance paradigm, away from particularised monitoring to a massive systematic surveillance regime which, within the U.S., violates the U.S. constitution and stretches constitutional frameworks beyond the imagination, making legal oversight impossible.” While U.S. capabilities in this area outstrip those of other countries, this is in fact a global concern, with similar examples to be found in France, Germany, and the United Kingdom.

The NSA scandal has laid bare the wholesale breaches of control of the U.S.’ constitutional safeguards, with global consequences, stressed McNamee. “There is too much tension in the



balance between individual security and a national security regime that has effectively declared independence from the people it was created to defend,” he concluded.

As the internet and data technology phenomena grow, there has been a global and near-comprehensive decline in the trust that people have in public-sector organisations, noted Lute. “The global moment of cyber-awakening coincides with a lack of trust in government. This is an issue that must be discussed and resolved sooner rather than later.”

Reconciling citizens and consumers: Trust in the digital age

With the advent of cloud computing and the diminishing importance of national boundaries as regards data storage, cloud providers have become increasingly concerned about losing consumer trust. “Corporations such as Intel flourish if the internet ecosystem flourishes,” Jeppesen said. “At the same time, ensuring that data pertaining to EU citizens remains in EU territory is anathema to the concept of cloud computing,” he added. There is a need to reconcile the benefits for consumers of a free and open internet with the privacy and security of citizens through functioning, legal, and trustworthy surveillance systems.

It is necessary to give up some freedoms for the benefits that surveillance based on massive amounts of data provides, noted Cdr. Kurt Engelen, Vice-President of the Euro-Atlantic Association of Belgium, in an intervention from the audience. “I am not scared about the government using my data,” he said. “When they access private data, they do so to prevent crimes. How can we make it clear to people that it is worth giving up a part of their privacy?”

To address that question and provide perspective, one must compare and contrast the online and offline worlds, Jeppesen said, likening the massive collection of data by government agencies to the notion that every letter one receives or sends could be registered at the post office. “It is likely that there is nothing to worry about, but the NSA scandal suggests otherwise,” he stressed. “You have to put a lot of trust in the people who collect and store your data.”

A fair representation of the argument for data surveillance is that governments are searching for the terrorist needle in the citizen haystack. While this argument may be valid, the critical element of the issue is what happens to all the other data that is collected in the process. “If the national security officials in charge of this data come across another piece of data that looks suspicious, they may launch an inquest into non-terror-related activities,” he concluded.

“The existence of a database is a greater security threat than having no database at all,” stressed McNamee. “Yes, one might find fifteen strands of straw that look like needles but are not, and fifteen lives can be ruined.” As an argument in support of this, he cited examples of police and tax authorities in Ireland abusing database privileges to stalk and harass innocent citizens.

Underlying the trust issue are the divergent social views on questions of privacy and the relationship between citizen and state, Lute indicated. For example, EU countries issue national identity cards, whereas in the U.S. this would be unthinkable, and companies in the EU are required by law to hand over data to a greater degree than their counterparts in North America.

“We have to determine what our comfort levels are as regards government intrusion in our lives as citizens,” she concluded. “It is a false choice between privacy and security. We must reconcile the practical aspects of the discussion.”

Moving forward in the security vs. privacy discussion

The first step towards finding workable global solutions to these questions is to reconcile



fundamentally different views of privacy between governments, citizens, and both public- and private-sector organisations. Furthermore, noted Lute, citizens must seek to define what expectations they hold for governments in cyberspace, and how to narrate the value proposition of governments in their own lives.

“We as the public need to become better informed,” she concluded. “Normally governments are charged with security – managing police forces and the military. While this is true for most ‘spaces’, it has not thus far been true for cyberspace. We must begin by asking ourselves how do we assign responsibility for our cyber-security?”

In the case of the NSA, there is supposed to be oversight but, Jeppesen stressed, but by their own admission, these overseeing bodies have not been able to perform their function. “There is a tremendous amount of work that needs to be done in terms of reining in these surveillance programs,” he said. “It is excessively difficult to find out exactly what the oversight mechanisms are and how effective they are. This is not a state we can live with as global citizens.”

He urges an international debate on how to handle the issue, beginning with the EU and the U.S., as the foremost proponents of the rule of law and global human rights. “The best way forward can be found in the context of international human rights law,” he said. “International human rights treaties recognise the right to privacy and they also say that this right is not absolute.”

The European Court of Human Rights says that public authorities can interfere with the right to privacy for national security purposes in accordance with the law, when necessary. “What this



This is no time for silence. People on the internet are almost entirely consumers and not citizens. The time is coming for us to change that.”

Jane Lute

means is not clear at the moment,” he concluded. “We need more transparency in order to have an informed debate.”

“The truth is that the NSA has admitted that, in the twelve months prior to May 2012, there were 2.776 breaches of data as a result of their activities,” McNamee underlined. “I think the EU and the US are well-placed to take a lead in solving the cyber-security problem. However, the current practices have done too much damage to their credibility worldwide.”

“The issue has become muddied to the point where international and government agencies are breaking laws concerning citizen rights in order to defend those same laws,” he concluded. “What are needed are necessity, proportionality, and a fresh look at digital privacy rights, based on international human rights principles.”

“What is doing severe damage to the openness of the internet are not the revelations,” concluded Lute. “What is doing damage to you and me every day are the criminals who are online. This is no time for silence. People on the internet are almost entirely consumers and not citizens. The time is coming for us to change that.”



List of participants

Emil Akander

Project Manager
The Swedish Trade and Invest Council

Farnaz Alimehri

Student
Vesalius College

Charlotte Allen

Official
European External Action Service (EEAS)

Andrius Avizius

*Director, Committee on the
Civil Dimension of Security*
NATO Parliamentary Assembly

Eda Aygen

Communication Manager
European Organisation for Security

Oana Badan

Assistant
Council of the European Union

Oxana Bartels

Policy Officer
European Commission
Directorate General for Fisheries
& Maritime Affairs

Alexandra Beaulieu

Researcher
Hobart and William Smith Colleges

Joanna Beczala

Administrator, International Relations Officer
European Commission

John Bird

*Department of Homeland Security
Attaché to the EU & NATO*
Mission of the United States of
America to the EU

Henrik Bliddal

Director, Science and Technology Committee
NATO Parliamentary Assembly

Giorgio Bombassei

Independent Researcher and Writer

Elena Bossi

Project Assistant
Friends of Europe

Jake Braun

Executive Vice President
Resolute Consulting

Margaret Brusasco-Mackenzie

Senior Advisor
Institute for Environmental Security

Richard Caine

Policy Officer
European Commission
Directorate General for Home Affairs

Geert Cami

Co-Founder & Director
Security & Defence Agenda (SDA)

Joannie Caron

Assistant, Political section
Mission of Canada to the EU

Lt. Fabio Casula

Human Factor Analysis, Psy. Operations
Ministry of Defence, Belgium

Pavel Chervonobab

First Secretary
Mission of the Russian Federation to NATO

Cdr. Jeffrey Cima

Executive Officer
United States Mission to NATO

Paul Cohen

Project Assistant
Security & Defence Agenda (SDA)

Maruša Conič

Assistant
Ludwig von Mises Institute Europe

Robert Cox

Trustee
Friends of Europe

Atu Darko

Director EU Affairs
Flying Bridges

Amb. Jean De Ruyt

Senior European Policy Adviser
Covington & Burling

List of participants

Elizabeth Dengal

Researcher

Hobart and William Smith Colleges

Utku Dogan

Intern

Turkish Industry and Business Association

Eliot Edwards

Senior Associate

Interel European Affairs

Maria Elena Efthymiou

Administrator

European Parliament

Elina Eloranta

Researcher

University of Tampere

Cdr. Kurt Engelen

Vice-President

Euro-Atlantic Association of Belgium

David Fouquet

Senior Associate

European Institute for Asian Studies (EIAS)

Maximilian Freudenthaler

Seminar Assistant

Friedrich-Ebert-Stiftung

Daniel Furby

Senior Account Executive

Fipra International

Andrea Ghianda

Project Manager

Security & Defence Agenda (SDA)

Laurent Giquello

*Programme Manager, Crisis Management
and Planning Directorate (CMPD)*

European External Action Service (EEAS)

Adam Gono

Assistant to the Secretary General

European Liberal Youth

Virginie Goupy

Journalist

Europolitics

David Grivet

Research Analyst

Mission of South Korea to the EU

Victorine Hage

Assistant

Atlantic Treaty Association

Ben Hale

First Secretary, Security

Permanent Representation of
the United Kingdom to the EU

Monica Hargis

Programme Manager

Strategy Analytics

Tuija Hirvonen

Consultant

Cognizant

Justin Hustwitt

Counsellor

Permanent Representation of
the United Kingdom to the EU

Jens-Henrik Jeppesen

Representative and Director for European Affairs
Center for Democracy and Technology

Péter Király

Assistant, Public Affairs

Permanent Representation of Hungary to the EU

Daria Kovarikova

Political Officer

Embassy of the United States
of America to Belgium

Yves Lagoude

European Affairs Director

Thales Group

Vesna Ljungquist

Administrative Coordination

Assistant, Children's rights

European Commission

Jane Holl Lute

Former Deputy Secretary

United States Department of
Homeland Security (DHS)

List of participants

Amb. Douglas Lute

Permanent Representative
United States Mission to NATO

Shaoxuan Ma

First Secretary
Mission of the People's Republic
of China to the EU

Natalia Marczevska

Consultant
North Atlantic Treaty Organization (NATO)

Pauline Massart

Deputy Director
Security & Defence Agenda (SDA)

Joe McNamee

Executive Director
European Digital Rights (EDRI)

Giles Merritt

Director
Security & Defence Agenda (SDA)

Gabriel Moldoveanu

Counsellor
Delegation of Romania to NATO

Valérie Moutal

Business Continuity Coordinator
European Commission
Directorate General Human
Resources and Security

Molly Nadolski

Policy Analyst
Global Governance Institute

Nikolaj Nielsen

Journalist
EUobserver.com

Mihai Costin Nitoi

*Counsellor, Cyber Security,
EU Internal Security*
Permanent Representation of
Romania to the EU

Andrey Ognev

First Secretary
Mission of the Russian Federation to NATO

Pavel Palencar

Diplomat
Permanent Representation of the
Slovak Republic to the EU

Areva Paronjana

Project Assistant
Security & Defence Agenda (SDA)

Amy Pipher

Student
Vesalius College

Detlef Puhl

Senior Advisor, Strategic Communications
North Atlantic Treaty Organization (NATO)

Col.Yi Qiu

Counsellor
Mission of the People's
Republic of China to the EU

Eberhard Rhein

Honorary Trustee
Friends of Europe

William Roelants de Stappers

Deputy Permanent Representative
Delegation of Belgium to NATO

Anna Rozenich

Independant Researcher and Writer

Lailuma Sadid

Freelance Journalist
For Afghanistan Newspaper

Elena Safronova

Second Secretary
Mission of the Russian Federation to the EU

Jonathan Sage

Government Programmes Executive
IBM UK

Donald Scargill

Director
Information2Intelligence

Charles Schmidt

Student
Vesalius College

List of participants

Teri Schultz

Freelance Reporter
National Public Radio (NPR)

Catherine Sheahan

Junior Analyst
European Union Institute for Security Studies

Michael Sieber

Deputy Director, R&T
European Defence Agency (EDA)

René Steiner

Administrator
European Commission
Directorate General Human
Resources and Security

Nagayo Taniguchi

Journalist
SEKAI

Meryem Uyar

Assistant
Turkish Industry and Business Association
(TÜSIAD)

Ulrich van Essen

Head of Unit, Protection of EUSI
Council of the European Union

Willem van Sluijs

Counsellor, Interior Affairs
Permanent Representation of
the Netherlands to the EU

Wout Van Wijk

EU Public Affairs Manager
Huawei Technologies

Nicolas Vandaele

Commissioner-Auditor
Standing Intelligence Agencies Review Com-
mittee, Belgium

Bart Vande Ghinste

Enterprise Architect - Evangelism Manager
Microsoft

Cecilia Verkleij

Head of Sector
European Commission

Luc Véron

Advisor
European External Action Service (EEAS)

Kostyantyn Voytovsky

Counsellor
Mission of Ukraine to NATO





SECURITY & DEFENCE AGENDA

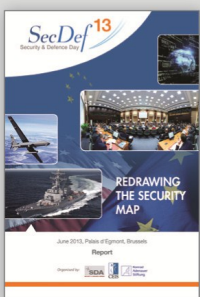
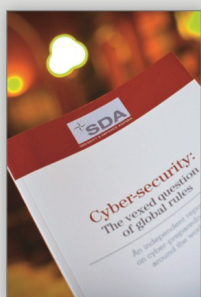
FEEL THE PULSE OF EUROPE'S DEFENCE DEBATE!

The **Security & Defence Agenda** (SDA) is Brussels' only specialist defence and security think tank. Its activities since its founding in 2002 have ranged widely across the international agenda, and focus on the issues of concern of NATO and the EU as well as those of national governments, NGOs, industries, academia and defence analysts around the world.

REPORTS OF OUR LIVELY DEBATES AND IN-DEPTH STUDIES OF PRESSING SECURITY ISSUES

can be found at: www.securitydefenceagenda.org

Cyber-security: The vexed question of global rules | Next steps in missile defence | France in Mali: Now or never for European foreign and security policy | Safeguarding defence technologies | SecDef' 13: Redrawing the security map | Turkey's growing security role: Where does NATO fit in?



The SDA recently welcomed



General Philip M. Breedlove
NATO Supreme Allied Commander Europe



General Jean-Paul Paloméros
NATO Supreme Allied Commander Transformation

They are the latest in the long line of distinguished leaders who have spoken at our debates



www.facebook.com/s.d.agenda

Twitter: [@secdefagenda](https://twitter.com/secdefagenda)



The Security & Defence Agenda (SDA) would like to thank its members and partners for their support



The SDA gratefully acknowledges the generous support of the following governments:
Belgium | Czech Republic | Finland | France | Georgia | Italy | Netherlands
Poland | Qatar | Romania | Russia | Sweden | Turkey | United States | United Kingdom

For further information on SDA membership, contact us at:
Tel: +32 (0)2 300 29 91 | E-mail: info@securitydefenceagenda.org

SECURITY & DEFENCE AGENDA (SDA)

4 Rue de la Science
1000 Brussels, Belgium
Tel: +32 (0)2 300 29 92 **Fax:** +32 (0)2 300 29 90
E-mail: info@securitydefenceagenda.org

www.securitydefenceagenda.org
twitter [@secdefagenda](https://twitter.com/secdefagenda)