# No Faustian Pact: Balancing Privacy and Security

**The rapid increase of Information and Communication Technologies (ICT) has thoroughly changed the debate on security and privacy concerns. Criminals, terrorists, corporations and foreign spies develop ever more sophisticated ways to get their hands on our personal data. At the same time, some see the recently exposed surveillance programs of national security agencies as proof that we are approximating George Orwell's 1984, where "[t]here was of course no way of knowing whether you were being watched at any given moment."[1] This Issue Brief disentangles these concerns, and suggests ways to find a more effective and acceptable balance between privacy and security in a digital world.**

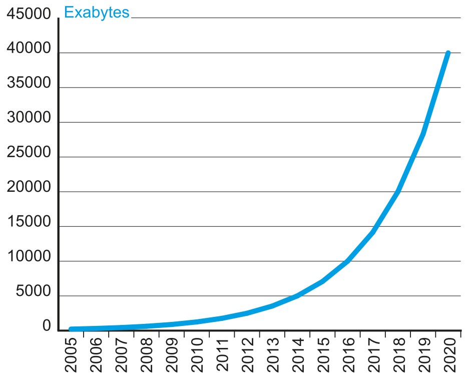


**Figure 1** The exponential growth of the data universe (Gantz & Reisel 2012)

## Changing security risks

Since the introduction of (digital) telephones, cameras, computers, and the internet, the amount of data created, replicated, and stored has expanded rapidly. It is predicted that in coming years, the "digital universe" will double every year. Data growth is expected to rise from 130 exabytes in 2005, to 40,000 exabytes, or 400 trillion gigabytes, by 2020. (see Figure 1).[2]

The digital world has changed the nature of certain security concerns. To be sure, the opportunities are tremendous. Digitally stored personal information is used to execute and coordinate political, economic, scientific and social operations and services, from the Arab Spring to the Obama election campaign. Large amounts of classified, confidential and personal data are stored on online bank accounts, loyalty cards, personal identification numbers, and Skype accounts. This data can all help in the direct support of and access to these operations. But there is a downside to these benefits too. Our data is a boon for criminals, terrorists, hacktivists, and intelligence agencies worldwide. Cyber attacks are on the rise. One indication is that, according to the United Nations Office of Drugs and Crime (UNODC), the number

The Hague Security Delta

The Hague Security Delta (HSD) is the largest security cluster in Europe. In this Dutch cluster, companies, governments, and research institutions work together on innovations and knowledge in the field of cyber security, national and urban security, protection of critical infrastructure, and forensics. They have a shared ambition: a secure world and economic development.

of mentions of cyber crimes in the main media in the six UN official languages has increased fivefold since 2005 (see Figure 2).[3] And the total number of reported internet security incidents in the US alone went up from little over 5,000 in 2006 to almost 50,000 in 2012 (see Figure 3).[4]

Figure 2 Cyber crime is increasingly mentioned in the media (UNODC 2013) of the six UN official languages

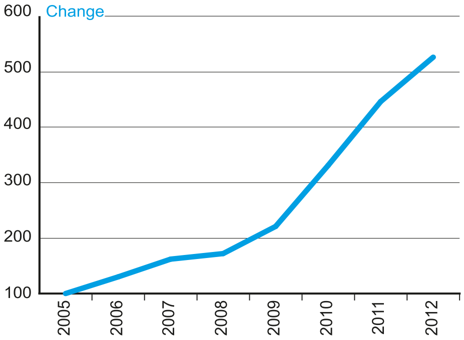
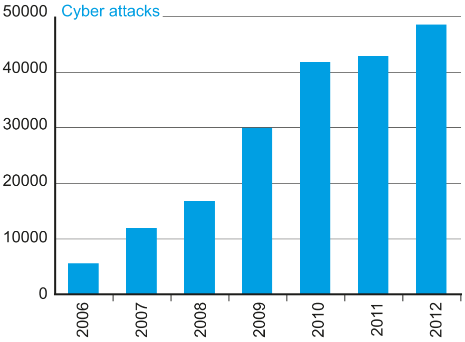


Figure 3 Cyber attacks in the US are on the rise (USGAO 2012)



Illegal activities are increasingly coordinated and conducted in the digital world, where communication is more anonymous and less location bound. According to the Dutch Intelligence and Security Service AIVD, in 2013 the Netherlands suffered cyber attacks emanating from Russia, Syria, China and Iran, among other countries.[5] Criminals develop websites that resemble trusted online banking services and try to lure visitors to leave valuable personal details behind. Companies are under attack by hacktivists, such as a when a Dutch 16 year old attacked the websites of Visa and MasterCard because they refused to transfer donations to WikiLeaks.[6] And states are subject to cyber attacks trying to cripple infrastructure, such as the Stuxnet virus attack on the Iranian nuclear power installation.

## Surveillance encroaching on privacy

Spurred by the ever increasing possibilities that information technology offers, and in light of the proliferation of cyber threats to national, societal, and individual security, governments have ramped up their surveillance programs. In the wake of the 9/11 terrorists attacks, intelligence gathering capabilities were further increased in an effort to protect national security. As a consequence, the question of how much intrusion into people's lives is warranted to increase security has become more pertinent than ever.

Given the amount of data that is available, and because of the difficulty of tracing perpetrators, governments feel compelled to process large amounts of data in order to detect, prevent, and respond to threats. Such surveillance activities generally focus on metadata, or "data about data" – for example, the length of a phone call, rather than the conversation itself. The amount of data that is tapped by governments worldwide is on the rise. And intelligence agencies are increasingly requesting tech companies like Google and Facebook to share such metadata – and not just by the US government (see Figure 4).[7]

States use surveillance for different purposes. In countries with larger political and social freedoms, the predominant focus is national security threats. But in more autocratic regimes, surveillance is used to repress domestic dissent and keep the government in power (see Figure 5). The Bahraini government for example resorted to online repression to quell Shi'a-led protests in 2011 and 2012.[8] It censored websites used by protestors and recorded online behavior to incriminate those criticizing the regime.

## The main challenges

There are four key challenges that impact how to balance privacy and security concerns. ICT innovations lead to new privacy/security trade-offs; debate on how to balance privacy with security concerns has been lacking; national and international legal frameworks are inadequate; and people, companies and governments possess insufficient knowledge about of the threats they face, or about the purpose and utility of surveillance programs.

### *The impact of ICT innovations*

Privacy-security problems are constantly changing due to ICT innovations. The relation between technology and privacy is constantly "pushed" by new technologies. This relationship can be seen as an "arms race" between technologies that increase and diminish privacy.[10] Better virus-scanners and improved encryption techniques lead to more privacy. But conversely, portable mobile technology that records people's whereabouts, or using UAV's for intelligence gathering, can present new security and privacy concerns. Personal data may be hacked, while surveillance programs may violate privacy rights. The expectation is that the amount of data that needs to be secured will only further increase. As one report indicates, the amount of data that needs to be secured is indeed increasing, from about a third of all data in 2010, to over 40% in 2020. And more worryingly, only half of all data that needs protection is adequately secured.[11]

One key development is centralizing information storage in "the cloud", which some reports suggest will store or process around 40% of all data in 2020.[12] The paradox here is that, although the

Figure 4 Government User Data Requests to Google (GUDR) per million inhabitants (Google 2013)

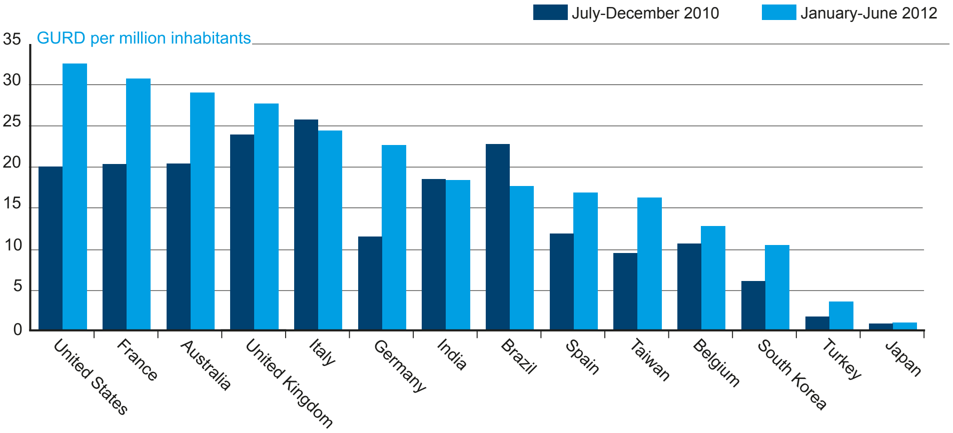
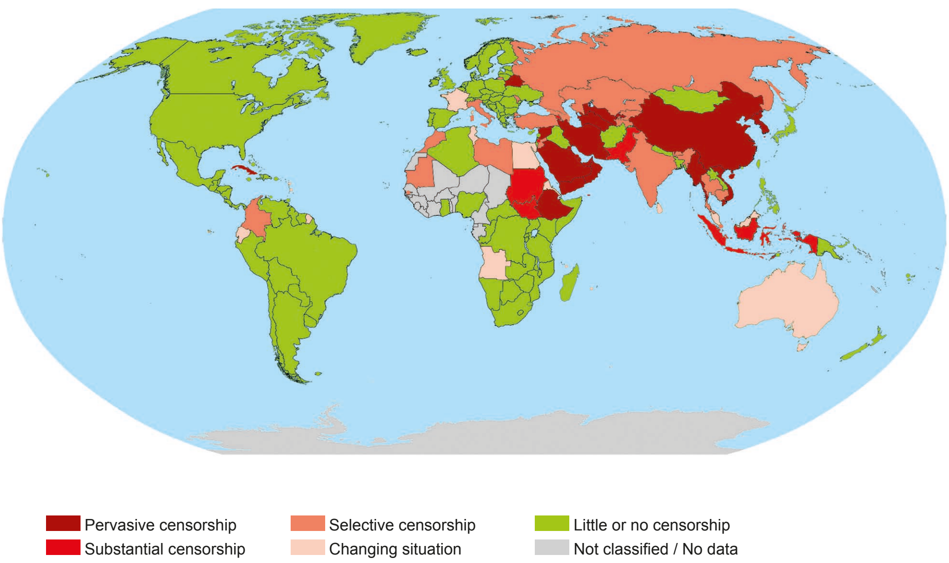


Figure 5 Internet censorship by country (OpenNet 2012; Reporters Without Borders 2012)[9]



chances of security breaches diminish, the consequences of a breach may increase. For example, with the advent of the “internet of things”, which links machines to the internet and stores information in a cloud, new security threats emerge. Recently, over 100,000 consumer appliances were hacked, such as TVs and refrigerators.[13]

### *Limited debate*

The Wikileaks and Snowden revelations have exposed surveillance programs that were hitherto unknown to many. Under pressure of the ever expanding cyber threat and new technological opportunities, and in contrast with for example the use of camera’s for surveillance purposes, programs like PRISM were not subjected to extensive public debate. The exposure of large-scale surveillance programs may make people less trustful of their governments. In the Netherlands, for example, parliamentarians have called for an inquiry into the role of the Dutch intelligence services following the supposed collection of personal data on internet forums in possible violation of the law.[14]

Governments worldwide are now addressing criticism from civil society groups, other states, and foreign nationals over how personal data is handled in surveillance programs.[15] The Obama administration has pledged to better respect privacy rights of US citizens by no longer storing bulk data on government servers, and subjecting all wiretap requests to the approval of Foreign Intelligence Surveillance Act (FISA) courts.[16]

Another issue relates to the extent that governments are allowed to demand tech companies to hand over metadata. In a letter to the US Government, Apple, Google, Microsoft, Facebook, Yahoo, LinkedIn, Twitter and AOL have suggested and international ban on bulk data collection.[17]

Mistrust between governments is also limiting cooperation on national security issues.[18] The EU Parliament heavily criticized snooping by US and UK intelligence agencies, and called upon the American authorities to adopt legislation that “recognise[s] the privacy and other rights of EU citizens”.[19] The surveillance scandals have led to a re-evaluation of what information governments can and want to share with international counterparts. Countries such as Brazil and Germany started to push for routing regional online traffic via their own local servers, instead of via the US.[20] The Dutch government is exploring the possibility of creating separated networks so as to “better ensure the continuity of vital processes.”[21] If this trend continues, the outcome may be a less open world wide web, and less cooperation between intelligence services.

### *The law leaping behind*

Cyber space today resembles the high seas when the first explorers set sail with no clear boundaries marking ownership and responsibility. In theory, privacy is a universal right, laid down in the Universal Declaration of Human Rights. Yet in practice, data protection laws are rarely well developed. According to the Human Rights Council of the UN, most countries lack adequate laws to secure privacy rights in the face of ever more sophisticated surveillance programs.[22] Surveillance agencies often invoke arguments of national security concerns to override privacy rights that are difficult to evaluate, and judicial oversight to warrant such actions is limited.

One specific problem is “function creep”: technologies may later be used for surveillance purposes that were not originally intended.[23] In the Netherlands, for example, it was suggested that biometric data in passports would also be used for surveillance purposes. Challenged by increasing public discontent over the prospect of a slippery slope towards ever more intrusive surveillance practices, the Dutch Parliament eventually shelved the idea.

### *Knowledge deficit*

Most people are unaware of the details of surveillance programs and the national security threats they target. Citizens have limited knowledge of the risks that their online behavior entails, and what they need to do to protect their personal data. As the Snowden revelations indicate, not many people knew of the extensive surveillance programs, nor the threats they were aimed at. However, to evaluate the balance between privacy and security that government surveillance agencies make, the public and businesses alike need to be well informed. For governments and companies to protect themselves against growing digital threats, awareness, expertise, and cyber resilience policies are essential. Yet such knowledge and awareness is often lacking.[24]

## Solutions

This concluding section suggests how to find a more effective and legitimate balance between privacy and security concern by stimulating informed debate; improving legal frameworks; strengthening global governance; and integrating privacy in technology development.

### Stimulate informed debate

What is the rightful balance between privacy and security? How do privacy and security concerns relate, and how is their character changing in an ever more digital world? A new and invigorated debate is needed on these questions between governments, parliaments, businesses, experts, and the general public. Such a debate needs to go beyond viewing privacy and security as a zero-sum game. Privacy may actually be increased by better surveillance, for example through more effective personal data protection against hackers. Conversely, a poor privacy track record may hamper international security efforts. If western governments have the reputation of spying on their own people, they run the risk of being accused of applying double standards when criticizing other regimes on respect for privacy – something the Chinese government has repeatedly done.[25] In addition, public knowledge about the purpose and needs of surveillance should be increased, and governments will have to be more transparent about their intelligence programs.

### *Improve legal framework*

Finding a legitimate balance between privacy and security will require reevaluation of the legal framework within which surveillance takes place. Reviews in several countries have already led to strengthened oversight and control by courts and parliaments. For example, a special expert commission installed by the Dutch Parliament to review the 2002 surveillance law, suggested simultaneously increasing oversight and expand the mandate of surveillance agencies.[26] One suggestion to improve privacy guarantees in light of a structural and growing gap between digital threats and the need for surveillance, would be to create a legal framework that would focus more on the information needed, instead of the technologies that can be used.

### *Strengthen global governance*

Global data governance needs to be strengthened. Although there are large differences in how governments value privacy vis-à-vis security, stepping up dialogue at the international level can help  to work towards an international legal framework on the protection of data communication. For example, an international body with judicial power could assess if governments have illegally tapped citizens – and if found guilty, penalize these states.

### *Integrate privacy in technology development*

Include privacy concerns in ICT design process. Making "privacy by design" the norm in the development of information technologies will require increased cooperation with the private sector. How does Google Glass affect our privacy? What personal information will driverless cars have access to, and how do we make sure such data is kept private? Posing such questions at an early stage of technology developments will diminish the need for the continuous adjustment of privacy legislation later – and ideally limit the need for ad-hoc technological changes needed to accommodate privacy concerns.[27] At the same time, such a step would have to take account of additional costs, and reduced consumer friendliness.

[1] Orwell, George. 1984. New York: Signet Classic, 1950.
[2] Gantz, John, and David Reinsel. *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East.* IDC, 2012.
[3] UNODC. *Comprehensive Study on Cybercrime*. Vienna: UNODC, February, 2013.
[4] United States Government Accountability Office, *Cybersecurity. Threats Impacting the Nation*. April, 2012.
[5] National Cybersecurity Centrum. *Cybersecuritybeeld* Nederland. The Hague: National Cybersecurity Centrum, 2013.
[6] Essers, Loek. "16-jarige MasterCard DDoS'er vrijgelaten." *Webwereld*, December 16, 2010.
[7] *Google Transparency Report 2012. Available at http://www.google.com/transparencyreport/.*
[8] *Surveillance Briefing: Bahrain*. London: Privacy International, 2012.
[9] Based on the ranking from the OpenNet Initiative "Summarized global Internet filtering data spreadsheet", from October 2012, and the "Internet Enemies" report by Reporters Without Borders of March 2012.
[10] Etzoni, Amitai. "Are New Technology the Enemy of Privacy?" *Knowledge, Technology & Policy 20* (2007).
[11] Gantz and Reinsel, 2012.
[12] Ibid.
[13] Rodriguez, Salvador. "Refrigerator among Devices Hacked in Internet of Things Cyber Attack." *LA Times*, January 16, 2014
[14] "Pechtold Wil Parlementaire Enquête Afluisteren AIVD." *VK*, November 30, 2013.
[15] Clarke et al. *The NSA Report: Liberty and Security in a Changing World.* Princeton: Princeton University Press, 2013.
[16] *Obama's Limited Response on NSA Surveillance.* IISS, January 22, 2014.
[17] Roberts, Dan. "Twitter, Facebook and More Demand Sweeping Changes to US Surveillance." *The Guardian,* December 9, 2013.
[18] "EU Says Distrust of US on Spying May Harm Terror Fight." *BBC*, October 25, 2013.
[19] Hopkins, Nick, and Ian Traynor. "NSA and GCHQ Activities Appear Illegal, Says EU Parliamentary Inquiry." *The Guardian*, January 9, 2014.
[20] Matthew Taylor et al. "NSA Surveillance May Cause Breakup of Internet, Warn Experts." *The Guardian*, November 1, 2013.
[21] *National Cybersecurity Strategy* 2: *From Awareness to Capability*. The Hague: National Coordinator for Security and Counterterrorism, 2013.
[22] La Rue, Frank. Report of *the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Human Rights Council, 2013.
[23] WODC. *Function Creep and Privacy*. The Hague: Boom Legal Publishers, 2011.
[24] David Chinn et al. *Risk and Responsibility in a Hypeconnected World: Implication for Enterprises.* Cologny/Geneva: World Economic Forum, 2014.
[25] Branigan, Tania. "China Accuses US of Human Rights Double Standards." *The Guardian*, April 11, 2011.
[26] Commissie Dessens. *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*. 2013.
[27] CPB. *Richtsnoeren beveiliging van persoongegevens*. 2013.

**HSD Issue Brief 1/2014**
*The Hague* Centre for Strategic Studies:
Maarten Gehem and Willem Oosterveld
www.hcss.nl

**The Hague Security Delta**
HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN The Hague
The Netherlands
T +31 (0)70-3028180
info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

The Hague **Security Delta**