

Protecting the digitized society—the challenge of balancing surveillance and privacy

Dr. Janne Hagen

Dr. Olav Lysne

ABSTRACT

Through technological development and the continuously expanding Internet, the challenges of physical distance, borders and time has diminished, enabling new and more efficient business models and concepts. With this technological development, however, follows an increase in global cybercrime, mass surveillance, internet censoring, and espionage. Terror attacks and cybercrime incidents are now forcing policy makers to balance surveillance and privacy through a paradox: While privacy regulations protect individuals' freedom of speech and safety from persecution, it may also restrain effective crime and terror investigation. In November 2015, the Norwegian Governmental Committee on Digital Vulnerability delivered an Official Norwegian Report (NOU) to the Minister of Justice and Public Security in which the problematic issue of balancing surveillance and privacy was emphasized. The intricate challenge is that in-between surveillance and the privacy lays the personal data—the new *gold* from a commercial perspective, a resource in the fight against terrorism from a security perspective, and a future threat of human rights from an individual perspective.

1. CYBER THREAT DEVELOPMENT IN RETROSPECT

Originally, the Internet was designed with the purpose of interconnecting a sparse network of selected trustees—it was not intended to be available to everyone. As time passed, protocols were developed and several networks of networks evolved, gradually merging into larger networks leading to an expansion that now serves everyone. Today, the Internet and the World Wide Web connects people and information around the world. However, with this expansion and dissemination of malware, security worries arose.



Dr. Janne Hagen holds a Master's degree in industrial economy and management. She received her PhD in information security in 2009. In 2008-2009 she was a visiting Fulbright Scholar at Naval Postgraduate School, Monterey, CA. From April 2015 she works at The Norwegian Water Resources and Energy Directorate (NVE) with SCADA and ICT security. She was until then working as principal scientist at the Norwegian Defence Research Establishment (FFI) and associate professor at the University of Stavanger. She has conducted research on societal security and protection of critical infrastructures since 1996. Since 2005, her work has been directed towards information security and societal security, the last years also covering information operations, strategic communication and the vulnerability of the digital society. Janne Hagen has been a member of several expert groups in Norway and also worked in EU funded projects. She was a member of the Norwegian Committee of Digital Vulnerabilities in Society. The Committee delivered an Official Norwegian Report (NOU) to the Ministry of Justice and Public Security in 2015.

This threat development was foreseen and well warned. Twelve years ago, the security expert Bruce Schneier predicted that fast automation attacks—hazardous actions at distance—and technique propagation would become a significant threat as it required only one skilled attacker; other attackers could simply copy and use their tools.^[1] Since 2004, the conditions pointed out by Schneier have been further aggravated, helped by unpatched vulnerabilities and incorrect configurations. Today, the market for malware and exploits has matured, as documented by a RAND Corporation study.^[2] State actors, organizations, and individuals participate and trade in this market. All that is required to purchase malware and cybercrime services are a web browser and a credit card. Many tools and services are furthermore available at affordable prices—some are even free of charge. The consequences are enormous, as pointed out by Rhoades and Twist (2015):^[3] the high profile data breaches during 2015 include, among others, the Snapchat 4.5 million names and phone numbers, the eBay database of 145 million users compromised, the UCLA Health 4.5 million records, the Army National Guard 850,000 records and more.

Pell and Soghoian in 2014, examined the historical perspective of security challenges in the mobile networks, showing how the US government disregarded the security challenges. In 1993, American policy makers took no actions in order to force the industry to improve the exposed technical security flaws in the analogous telephone technology. Instead, they prohibited eavesdropping equipment that could be used to exploit the weaknesses.^[4] This strategy did not pay off in the long run. When the mobile networks became digitized, they remained vulnerable, while the eavesdropping equipment was improved and became cheaper at the same time. Today, even



Dr. Olav Lysne is Director and founder of the Center for Resilient Networks and Applications (CRNA) at Simula Research Laboratory, and professor in computer science at Simula and the University of Oslo. He received the Master's degree in 1988 and the Doctor of Science in 1992, both at the University of Oslo. The early research contributions of Lysne were in the field of algebraic specification and term rewriting, with a particular emphasis on automated deduction. While working in this field he was a visiting researcher at Université de Paris-Sud. Later in his career he has been working on resilient computer architecture for supercomputing and cloud infrastructures, routing and switching techniques for IP-networks and measurement of national network infrastructures. Lysne was the leader of the Norwegian Government's Commission on digital vulnerability, which submitted its report to the Minister of Justice and Public Security in November 2015.

amateurs can gain wireless access to and use these tools and software to tap mobile phone calls.

Through the Internet, the world has become globally interconnected. All nation states are increasingly exposed to cyber threats and cyber-crime from abroad. In the cyber domain, there are no physical borders, and *traveling* around the world is now possible, digitally speaking, in a microsecond. The world—with both good and bad actors—has entered our homes and businesses through cyberspace. It is not surprising then, that security authorities, and the military sector are concerned and aim to develop policies, plans, tools and modes of operations to defend the homeland. In this global cyber world, however, good security inventions, like for instance surveillance software, can later on be stolen and used against law abiding citizens. This brings us back to the challenge of evaluating and balancing surveillance versus privacy. On one hand, surveillance tools are in great demand, but on the other hand, they could become dangerous in the hands of an adversary, for instance a criminal organization, or a state in a potential conflict. Balancing surveillance and privacy is therefore very intricate, and hence of great importance, as raised by the Official Norwegian Report (NOU) to the Minister of Justice and Public Security.^{[5][6]}

The rest of this article is structured in the following way: In section 2, we introduce the Norwegian case of digitalization; the policy of modernization and digitalization, and a brief introduction to digital vulnerabilities. In section 3, we discuss the society's need for security and privacy to fight crime and terror. In section 4, we turn to the privacy issues and argue why privacy matters. Section 5 deals with the challenge of balancing surveillance and privacy, and section 6 presents the conclusion.

2. CASE: THE NORWEGIAN DIGITIZED SOCIETY

2.1 The Digital Agenda for Norway

The Norwegian government's white paper on the Digital Agenda for Norway^[7] presents the government's policy on how the Norwegian society should benefit from value creation and innovation opportunities offered by information technology and the Internet. The Digital Agenda adopts a long-term perspective, 2020.^[8] According to the policy document, widespread online participation represents a comparative advantage to the country and provides a variety of benefits for the citizens. The high political ambitions for digital participation are summarized here:^[9]

- ◆ Everyone in Norway who wishes to use digital tools and services should be able to do so.
- ◆ Provisions will be made to ensure relevant training opportunities for groups that need them.
- ◆ Within five years, the number of citizens not online will be halved, from 270,000 to 135,000 (Norway has about 5.2 million inhabitants).
- ◆ The education system will provide individuals with sufficient qualifications to continue developing their digital competence and keep pace with technology developments.
- ◆ Employees will be able to use digital tools and develop their digital skills at work.
- ◆ The population will have sufficient skills to use the Internet safely and securely.

Digitization has been driven by huge cost savings, new income opportunities, and future product innovations and business developments. According to Ark and Inklaar in 2005, as much as 50 percent of European productivity growth was attributed to the use of information and communication technology (ICT) and the Internet.^[10]

Today, Norway is a highly digitized society. The majority of Norwegians have access to the Internet at home, 98 percent have mobile phones, and 80 percent have smart phones (2014).^[11] Digitization has infiltrated all parts of modern society. Physical payment accounts for less than 5 percent of all transactions; the finance sector is digitized and it is difficult to get cash—even when visiting a bank. Smartphone applications now enable people to pay their bus and train tickets electronically from their mobile phones. Citizens also have access to their electronic patient journal from the Internet, and medical prescriptions can be provided electronically. The individual reporting to tax authorities is done electronically, with most of it by algorithms that automatically collect data from

a variety of registries. Internet voting has been on trial, and the preferred way for contact between the citizens and the authorities is through a web interface and Internet connection. Norwegian authorities aim furthermore to meet the population on social media, where the majority of the population is active. Within a few years, the electrical power grid rolls out smart digital meters, which enables the development of more digitized welfare and health services on the top of the meter infrastructure. These services will, among other things, help the elderly to stay longer in their homes. The country's welfare, income creation, and security depend increasingly on bits and bytes carried by the Internet Protocol (IP) wired or by air.

The digitization project has brought Norway to the top ranking in Europe and number four globally according to the Cyber Security Index^[11] but digital vulnerabilities still remain. The complexity and the risk of failure are given by the long digitized value chains that stretch across national borders, by the traffic data and the signaling data that flows constantly. If you want to pay your bus ticket with the ticket app, the electronic money transfer depends on the functionality of a very long chain of various service providers, Internet and telecom providers, satellite services like accurate time and various technical systems; a chain from the mobile app and your bank server, and all the way to the bank account of the bus company. Your mobile phone is always connected, and the signaling data leaves traces of the location of the device.

The intricate challenge
is that in-between the
surveillance and the privacy
lays the personal data—
the new gold...

2.2 The threats towards the digitized society

Cyber threats grew out of the huge digitalization project with the opportunities and vulnerabilities that followed. According to the Norwegian Computer Crime Survey 2014, most cyberattacks misuse old and known vulnerabilities that are not supported or patched. Although Norway is a wealthy country, and in the frontline of digital technology adaption, the old unpatched systems show up as an important vulnerability that enables an attacker to gain unauthorized access to information and systems.

The results from the Norwegian Computer Crime Survey in 2014 documents that more than half of Norwegian enterprises have been hacked, not just 5 percent as the respondents in the survey reported. This conclusion was derived by a comparison of data of the Computer Crime Survey with data from Mnemonic, a Norwegian security company, and NSM NorCERT. Table 1 shows the number of hacking incidents detected in large Norwegian companies reported by the survey or detected by Mnemonic and NSM NorCERT. The results show that the ability to detect incidents is limited; of the reported hacking incidents in the survey, only 1 percent is reported to the police.^[13]

Table 1. Detected hacking incidents in large Norwegian companies, 2014.^[14]

Hacking Incidents in Large Companies	The Norwegian Computer Crime Survey 2014	Mnemonic	The Norwegian National Security Authority (NSM NorCERT)
Number of Hacking Incidents Reported	600	444	51
Percentage of Enterprises Experiencing Hacking	5	66	50

2.3 The use of cloud computing and the Snowden revelations

The use of cloud computing is on rise in Norway with two-thirds of Norwegian enterprises reported using cloud computing services in 2014. According to the Norwegian Computer Crime Survey 2014, the use of cloud services may be a favorable solution for the many small enterprises in Norway that otherwise lack sufficient IT security knowledge and enough resources to build and run secured IT systems.^[15] International cloud computing service providers represent increased technical security (better patching regime and remote backup), but at the same time, the use of cloud computing means reduced national control. The challenges with surveillance versus privacy exploded in 2013, when Edward Snowden, who worked for a contractor, Booz Allen Hamilton, leaked numerous classified documents about National Security Agency (NSA) intelligence programs.^[16] The Snowden leakages of the massive NSA surveillance program struck directly at privacy issues and the Safe Harbor regulation. The Safe Harbor regulation allowed companies operating in the European Union (EU) to send personal data to third countries outside the European Economic Area. In October 2015, the European Court of Justice responded to a referral from the High Court of Ireland concerning a complaint from an Austrian citizen, Maximillian Schrems, regarding transfer of his Facebook data to the US in the aftermath of the Snowden revelations. The European Court of Justice then held the Safe Harbor Principles to be invalid.^[17] The Maxmillian case illustrates the paradox between surveillance and privacy, and how it can hit back on commercial interests and trust.

There are two observations that can be made so far regarding the cyber environment. First, we are entering into a future where close to everything we do, will have a digital component. Most of our activities will be communicated over a network and can potentially leave a digital trace. This means that close surveillance of every individual in a society is becoming technically feasible, and thus constitutes a serious threat to privacy as a human right. The second observation is that criminal activity, ranging from amateur hacking to terrorist attacks, will also have a digital component. The same mass surveillance that is a threat to our human rights is also a powerful, and sometimes a necessary tool to ensure our security. We elaborate further regarding this dilemma in the upcoming sections.

3. THE SOCIETY'S NEED FOR SECURITY AND SAFETY

3.1 Incident detection and handling

As society becomes more digitized, vulnerable and complex, the need for continuous monitoring and surveillance of critical systems, security warnings, and incident handling services increase. Surveillance can have beneficial political impacts where it detects fraud.^[18] A system that monitors the banking industry and money transfers might support democracy by making corporate wrong-doing harder to hide.

The number of Computer Security Incident Response Teams (CSIRT) and Computer Emergency Response Teams (CERTs) in Norway is growing. Many of these institutions provide incident monitoring, warning, and incident handling services that will aid enterprises to detect and be aware of the attacks.

NSM NorCERT is the national CERT, which is coordinating incident handling in critical infrastructures and important societal services, in addition to operating a national warning system for critical infrastructures. There is a close cooperation between the intelligence services, the security police, and NSM NorCERT.^[19]

In addition to this national CERT, there are several sector or industry based CERTs and CSIRTs. The Norwegian defense sector's CSIRT serves the military forces. In civil society, the CERT of the national universities, UNINETT CERT, manages computer security incidents that target, originate from or misuse the networks or connected equipment belonging to UNINETT or its member institutions.^[20] Health CSIRT is the joint information security competence center for the Norwegian

health care sector. The center shares knowledge about ICT threats and protection mechanisms, and continuously monitors traffic within the health network. The goal is to prevent and remediate adverse ICT security incidents and malicious intrusion attempts.^[21] FinansCERT is dedicated for the Norwegian financial

sector, as represented by Finance Norway (FNO). FinansCERT serves banks, life insurance and pension companies that are members of Finance Norway.^[22] The Norwegian KraftCERT was established in October 2014. KraftCERT provides information sharing between companies and organizations both nationally and internationally and assist the energy sector in handling digital security incidents. KraftCERT participates in the national emergency response organization.^[23] In 2015, a CSIRT was established in the telecom sector, and a Municipality CSIRT is currently discussed.^[24] In addition to these CSIRTs and CERTs, private companies offer monitoring and incident handling services.

The digitization project has brought Norway to the top ranking in Europe and number four globally according to the Cyber Security Index ranking.

The involvement of the various CERTs and CSIRTs in Norway illustrates an important national effort for the monitoring of digital systems. This priority is driven by recognizing it is impossible to prevent all hacking incidents that Norwegian enterprises are exposed to, and that authorities and businesses should prepare to detect and handle the incidents when they occur.

3.2 Police internet patrolling and covert operations

Digitization itself has enabled more efficient systems, network surveillance, and more effective data analytics. By combining different sources of digitized data and using statistics and algorithms, new insight can be produced, giving better situational awareness, improved decisions, and more efficient operations.

Since criminal activities also have become digitized, law enforcement must visibly patrol the Internet. In addition, the police may need to operate covertly. To investigate serious crime and predict crime or terror attacks, predictive analysis, access to social media accounts and big data analytics could provide significant aid for law enforcement. With the latest Paris terror attacks in November 2015, it is not difficult to understand the importance of eavesdropping and the need to intercept mobile phone calls of suspects as described by Pell and Soghoian.^[25]

Signaling information is generated even when the phones are not used. The signaling data provides information about geo-localization, hence personal information. Law enforcement request three types of requests for information from telecommunication enterprises:^[26]

- ◆ Requests for subscription data that can be given.
- ◆ Requests for traffic and signaling data, where the Norwegian Communication Authority can by law accept the request and release the internet and telecom provider's non-disclosure commitment. It has been argued that release of traffic data is less interfering for privacy than release of signaling data. Traffic data are generated by an action by the mobile phone user, in contrast to signaling, where data are transferred all the time irrespective of any positive action from the mobile phone user and reveals the geographical position of the user.
- ◆ Requests for communication control, for instance interception of mobile phones that requires a court order.

The Committee on Digital Vulnerabilities recommended a strengthening of the police's ability to combat cybercrime by establishing a new Cyber Crime Center. The Committee observed that among businesses and individuals there are low expectations as regards the assistance provided by the police to the victims of cybercrime.^[27] This means that only a small percentage of cybercrime is reported, also documented by the Norwegian Computer

Crime Survey 2014. Therefore, the Committee supports the proposal to establish a new national center to prevent and investigate complex and cross-sectoral cybercrime. The center should be organized under the National Criminal Investigation Service (NCIS, Kripos), and it should have a national technical responsibility for the prevention and investigation of serious and complex cybercrime. It should also have a separate assistance function to support the 12 police districts both with respect to police tactics and prosecution.^[28]

4. CHALLENGES FOR HUMAN RIGHTS IN THE CYBER DOMAIN

The concept of human rights developed as a result of the World War II (WWII) and the Nazi regime's crime against humanity, and was further influenced by later conflicts and human rights violations. According to the Universal Declaration of Human Rights (UN, 1948), every individual has the right to life, liberty and security of person, and the right to privacy. Article 12 states for instance: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."^[29]

Everyone has the right to protection under the law against such interference or attacks. Does the IT industry and the political decision makers take into account how human rights could be affected when they design and develop our digitized society? One example can illustrate the challenge: A misconfigured database leaking the personal information of over 191 million American voters was reported to DataBreaches.net by researcher Chris Vickery in December 2015.^[30] According to DataBreaches.net there were no social security numbers, driver's license numbers, or any financial information in this particular database—but it contained information about the voters' full name, date of birth, address and phone number, together with political party and other fields. A police officer expressed his concerns as it became apparent that criminals now could find his home address.^[31] In the long run, however, this kind of information can be used to obtain access to more private information about individuals. Even if it does not matter much today, it is just a question of time before it is possible to profile individuals, and then use this information to steal and misuse this person's digital identity, and to blackmail or threaten.

In fact, the vast amount of information stored on unsecured servers and in registries represents huge challenges for privacy and human rights. This challenge is illustrated with the current European refugee crisis: Norway, like other European countries, has in 2015 experienced a flow of refugees seeking a safe life in Europe. The refugees have escaped regimes that do not respect human rights, deny freedom of speech, and discriminate religion and political opinion. If the IT industry and government build data registries and IT systems that do not protect personal information, this might work well enough as long as the society remains safe, democratic and politically stable. In a potential future situation with a regime shift, new challenges and security issues might arise. For those who fled from the dangers in Syria and other countries, secure data registries containing personal information are a requirement to start a safe new life.

But there is another future security challenge. When society gets fully digitized, where can persecuted people, with digital identities shaped over time, escape? Is it possible to start a new life, to get a new digital identity? Is this possible if your digital biometric templates are stolen and disseminated?

A Swedish TV2 documentary, *You've Been Googled*,^[32] highlighted this issue. According to the documentary, digitized and searchable information did not fully disappear, and old traces of information, wrong or correct, remained on the Internet, accessible by search engines. In one case an identity theft, in which the innocent victim's identity was misused for criminal purposes, stopped the victim's future job career. The big question is: Will there be any opportunities for a new start? In May 2014, the European Court of Justice (ECJ) ruled that internet search engines must remove information deemed "inaccurate, inadequate, irrelevant or excessive" for the purposes of data processing, or face a fine.^[33] Will it be possible to enforce this regime, or have the policy makers made a similar mistake as they did in 1993 with cellular surveillance equipment?^[34] So far, even if removal requests are granted, those same articles are still available online

at the sites where they were originally published or at google.com where the US version of Google is hosted.

Close surveillance of every individual in society is becoming technically feasible, and thus constitutes a serious threat to privacy as a human right.

On one hand, social media and the Internet support human rights by providing a platform for free speech and information sharing, but on the other hand, the use of the same technology

might restrain for instance free speech and thus cause a chilling effect.^[35] What will be the long term impact of hate speech and harassment on the Internet? Will political discussions gradually diminish? It is well known that in several parts of the world, free speech is a risky business and bloggers 'just' disappear. So far, inhabitants of western democratic countries have the opportunity to speak out, but will this freedom last if everything we do and express are searchable on the Internet? According to Wright and Raab,^[36] surveillance technologies can have harmful psychological impact on individuals' sense of privacy. If people know that they are being surveilled, they are likely to be more cautious than they might otherwise be. This is the *chilling effect* seen from the standpoint of its psychological effect, not to mention its social consequence.

5. BALANCING PRIVACY AND SURVEILLANCE

Until recently, there have been strict legal, economical, technological and practical limits to how surveillance could be used. If someone wanted to wiretap a phone call, they

connected an extra wire to a physical phone line. The phone call needed to be recorded on tape, and the tape required a human listener in order to be interpreted. Furthermore, the fraction of human activity leaving a trace on a phone line was limited. Therefore, the regulation of surveillance only needed to address a very limited number of cases. As mass surveillance of almost all activity of every citizen is becoming technically and economically feasible, the balance between surveillance and privacy is no longer given to us through the limits of what is doable. Wright and Raab^[37] assess the political impacts of a surveillance system by asking a few questions: Who is being surveilled by whom and for what purpose? Who has authorized the surveillance? Will the project or technology enhance the power of some at the expense of others? Who will have access to the data gathered by a surveillance system and how will such data be used? Will it undermine the electorate's trust in their elected officials? Will the surveillance system support or undermine democracy?

Technical monitoring raises questions about surveillance and privacy. One such dilemma was raised in an article by Sveinbjørnsson in 2012.^[38] In order to protect informants, the Norwegian national broadcasting company NRK decided to exit the monitoring and sensor services provided by NSM NorCERT. NSM NorCERT's response to this decision was that the sensors could be regarded as a kind of intrusion alarms, and if they were removed, intrusions would not be detected. Thus, any successful undetected hacking could disclose the informants' personal information anyway. The NRK later decided to join the NSM NorCERT's monitoring and sensing services.^[39]

Also, covert operations conducted by law enforcement raises important questions about the value and balance between human rights, the right to free speech, privacy, and the rule of law. The Norwegian official report (NOU 2015:13) points to the challenges of using signaling data from telecommunication providers for other purposes than originally applied for. This challenge should be studied in more detail. Law enforcements extensive use of signaling data indicates it might be necessary to regulate the access to such data.^[40]

Almost everywhere, you can travel virtually along the public roads by using Google Street View. People and vehicle identities are anonymized, but you can zoom to a high degree and study the houses and gardens. Norwegians have a high level of trust in government, enterprises and their fellow citizens. In Germany, in contrast to Norway, Google Street View is not offered. The reason is Germany's WWII history and the raised awareness of the value of privacy after the Snowden leakages. In Germany, 70 percent of the population do not accept that the government surveils data traffic and phones.^[41] It is now 75 years since WWII and the occupation of Norway. In retrospect, if Norway was digitized during WWII, what digitized information would be accessible for the occupants about the enlisted youth in the military and about those who sympathized with the opponents of the Nazi regime? What intelligence advantages could be gained about the enlisted in the army by the use of predictive analysis based on social media utterings? How could meanings and

utterings by opponents be analyzed and interpreted as coming actions?

When the Islamic extremists went underground and used encryption, the need for new intelligence methods arose. According to the Norwegian newspaper *Aftenposten*, the Norwegian Police Security Service wanted to install key loggers on suspects' devices.^[42] It is a well understood demand from a counter terrorism perspective, but it raises some challenges from a privacy and human rights perspective: One is the potential strength of electronic data in court compared with for instance voice tapping, another is the risk for surveilling innocent persons. A third challenge is to ensure that the intent of the written text is correctly understood.

A comment in *Journal of Criminal Law, Criminology and Police Science* (1970) states that "The courts should not be willing to permit the state to employ techniques of stealth and deception to obtain information which it is prohibited from obtaining by means of unrestricted wiretapping, legislative inquiry, or search and seizure. The state's license to secretly survey and eavesdrop should be subject to more than only the unfettered discretion of police officials".^[43] Today, this challenge has moved into the cyber domain. In the NOU 2015:13 the governmental committee notes that the interests of public safety lead to proposals to introduce new and intrusive surveillance methods.^{[44][44]} Examples are proposals to introduce digital border surveillance and the Norwegian Police Security Service's desire to register utterances on social media, and to analyze information from open channels. The committee further acknowledges the police and intelligence agencies' needs behind such proposals, but argue that the proposals are of such an intrusive nature that they should not be introduced without prior public debate. Such a debate should be prepared through a public report that discusses these types of measures in full. Intelligence needs, technological expertise and protection of privacy must be safeguarded, and a thorough report must be made on the technological, legal and social issues the cases raise.

If people know that they are being surveilled, they are likely to be more cautious. This is the chilling effect seen from the standpoint of its psychological effect, not to mention its social consequence.

The committee has also pointed to the international debate on whether the use of strong cryptography should be regulated. It is extremely difficult—perhaps impossible—to develop systems that safeguard legitimate needs for protection and monitoring at the same time. It is therefore reasonable to believe that any limitations in the lawful use of cryptography will


affect Norwegian citizens, businesses and authorities. Any limitations on cryptography will at the same time not deter dishonest players from using cryptography and therefore not solve the police and the intelligence services' problem either. That is why the committee believes that use of cryptography should not be regulated or banned in Norway, moreover the Norwegian authorities should work actively against regulation or prohibition internationally, and that new investigation methods must be developed to ensure efficient law enforcement and intelligence work.^[45]

6. CONCLUSION

Digitization has opened up borders and made it possible to exchange ideas and thoughts worldwide. It has enabled new business concepts and increased information flow and effectiveness. Many voices not previously heard can now get attention through social media and blogs. An increase in global cybercrime, mass surveillance, Internet censoring and espionage has however followed this technological development, and with this development a subsequent need for surveillance of crime and terror investigation. In retrospect, the mobile phone surveillance case in 1993 illustrated the risk that adversaries will utilize the technological opportunities and developed tools. The 1993 case also demonstrated that legal measures alone are not enough when the technological development provides cheap opportunities for surveillance and eavesdropping for anyone.

It is well documented that digital systems are vulnerable to espionage as well as physical and electronic sabotage. It is reasonable to believe that the complexity and lack of transparency of the digital value chains together with old versions and unpatched systems will remain a security headache in the future. An even bigger nightmare might be loss of privacy and misuse of personal information. With access to data registries and the ability to merge and analyze personal information, including personal utterances and movements over time, an adversary can steal identities, blackmail and pose huge pressure towards single individuals and groups of people. At the very end it will become easier to select single individuals, key players in society as well as children. From a counter terrorism perspective increased surveillance would be a good idea, but the flip side of the coin would be that the surveillance capacity could be used against citizens sometime in the future. This could next threaten the population's trust in government, national security, and societal stability.

The intricate challenge is that in-between the surveillance and the privacy lays the personal data—the new *gold* from a commercial perspective, a resource in the fight against terrorism from a security perspective, and a future threat of human rights from an individual perspective. There is no simple solution to the paradox. The Norwegian report (NOU 2015:13) recommends not regulating encryption, and that any eavesdropping and surveillance for the purpose of fighting crime or enhancing national security should have a foundation in national law and sanctioned through public debate. Finally, an

enormous responsibility is laid on industry to design products and software that protect privacy, i.e., privacy by design. 

ACKNOWLEDGEMENTS

We would like to thank Ms. Eva Jarbekk, Lawyer and partner of Føyen Torkildsen Advokatfirma AS and member of the Norwegian committee of privacy (Personvernemda) for contributions to the article. We would furthermore thank Mr. Bjørn Olav Knutsen (Principal Scientist at FFI and Associate Professor at the University of Nordland), Mr. Torgeir Broen and Torkjel Søndrål, Senior Scientists at FFI, the Research Managers Ms. Hilde Hafnor and Mr. Ronny Windvik at FFI for comments, and finally, Ms. Ålov Runde Language Advisor at FFI, for spell check and language vetting.

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

NOTES

1. Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World, with New Information about Post-9/11 Security*, 2nd ed., (Indianapolis: Wiley Publishing, 2004), 14-22.
2. Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime. Tools and Stolen Data. Hackers' Bazaar* (Santa Monica: RAND Corporation, 2014) http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (accessed December 29, 2015).
3. Blake Rhoades and Jim Twist, "Our Data is Not Secure", *The Cyber Defense Review Blog*, published October 2015 <http://www.cyberdefensereview.org/2015/10/28/our-data-is-not-secure/> (accessed January 5, 2016).
4. Stephanie K. Pell and Christopher Soghoian, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy", (*Harvard Journal of Law and Technology*, 28 Number 1 Fall, 2014), 1-35. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678 (accessed December 29, 2015).
5. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden*. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
6. *Committee of Digital Vulnerabilities in Society – Summary, Official Norwegian Report (NOU 2015: 13) to the Ministry of Justice and Public Security 30. November 2015* <https://www.regjeringen.no/contentassets/fe88e9ea8a354bdlb63bc0022469f644/nosved/9.pdf> (accessed January 5, 2015).
7. *Digital Agenda for Norway — Meld. St. 23 (2012–2013) Report to the Storting (white paper)*, <https://www.regjeringen.no/en/dokumenter/meld.-st.-23-2012-2013/id718084/?ch=1&q=> (accessed December 29, 2015).
8. *Ibid.*, chapter 1.
9. *Ibid.*, chapter 2.
10. Bart van Ark and Robert Inklaar, *Catching up or Getting Stuck? Europe's Troubles to Exploit ICT's Productivity Potential*, Groningen Growth and Development Centre, Research Memorandum GD-79 (University of Groningen, 2005) <http://www.rug.nl/research/portal/files/2856698/gd79online.pdf> (accessed December 29, 2015).
11. Statistikkbanken, SSB, Statistics Norway, <https://www.ssb.no/statistikkbanken/SelectVarVal/saveselections.asp> (accessed January 7, 2015).
12. *Global Cyber Security Index*, (New York: ABI Research, 2014) <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf> (accessed December 30, 2015).
13. Mørketallsundersøkelsen, Informasjonssikkerhet, personvern og datakriminalitet 2014 (the Norwegian Computer Crime Survey), Næringslivets sikkerhetsråd (NSR), http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014_WEB.pdf (accessed January 8, 2015).
14. *Ibid.*
15. *Ibid.*
16. Laura Poitras and Glenn Greenwald, *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'* – video, (Hong Kong: The Guardian, 2013) <http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video> (accessed January 8, 2015).
17. "International Safe Harbor Privacy Principles", article, Wikipedia, https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles (accessed January 8, 2015).
18. David A. Wright and Charles D. Raab, "Constructing a surveillance impact assessment", (*Computer law & security review* 28, 2012), 619.
19. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden*. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014. Avgitt til Justis- og beredskapsdepartementet November 30, 2015. (In Norwegian)
20. UNINETT CERT – Policy and service level statement, published 6th June 2015, <https://www.uninett.no/cert/policy.html> (accessed January 7, 2015).
21. Health CSIRT, Helsenett, home page <https://www.nhn.no/english/Pages/HealthCSIRT.aspx> (accessed January 5, 2015).
22. FinansCERT, Norwegian Financial CyberCrime Unit, home page, <http://www.finanscert.no/engelsk.html> (accessed January 5, 2015).

NOTES

23. KraftCERT, home page <https://www.kraftcert.no/english/index.html> (accessed January 5, 2015).
24. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
25. Stephanie K. Pell and Christopher Soghoian, “Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy”, (*Harvard Journal of Law and Technology*, 28 Number 1 Fall, 2014), 1-35, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678 (accessed December 29, 2015).
26. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet November 30, 2015. (In Norwegian)
27. Ibid.
28. Ibid.
29. Universal Declaration of Human Rights, United Nations, 1948, <http://www.un.org/en/universal-declaration-human-rights/index.html> (accessed December 30, 2015).
30. 191 million voters’ personal info exposed by misconfigured database (UPDATE2), Databreaches.net, published December 28, 2015 <http://www.databreaches.net/191-million-voters-personal-info-exposed-by-misconfigured-database/> (accessed January 8, 2015).
31. Ibid.
32. “Du är Googlad” (You are googled), Documentary (in Swedish), Swedish TV, with Nikke Lindqvist, Brit Stakston, Johan Ripås, Tina Ax och Bengt Gangemi. (Published April 11, 2012) <https://www.youtube.com/watch?v=6JFlfvZV2VM> (accessed March 5, 2015).
33. Curtis, Sophie, “EU ‘right to be forgotten’: one year on”, published May 13, 2015 <http://www.telegraph.co.uk/technology/google/11599909/EU-right-to-be-forgotten-one-year-on.html> (accessed December 30, 2015).
34. Stephanie K. Pell and Christopher Soghoian, “Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy”, (*Harvard Journal of Law and Technology*, 28, Number 1 Fall, 2014), 1-35 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678 (accessed December 29, 2015).
35. David A. Wright and Charles D. Raab, “Constructing a surveillance impact assessment” (*Computer law & security review* 28, 2012), 619.
36. Ibid.
37. Ibid.
38. Sveinbjørnsson, Sigvald, “NRK kastet ut statens «spionboks», (Publisert November 5, 2012) <http://www.digi.no/sikkerhet/2012/11/05/nrk-kastet-ut-statens-spionboks> (accessed December 29, 2015).
39. Kabakk, Per Arne, “Elektronisk kildevern i NRK”, comment, NRK, published 19th September 2014 <http://www.nrk.no/ytring/elektronisk-kildevern-i-nrk-1.11941196> (accessed January 7, 2015).
40. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
41. Jørgensen, Sten Inge, *Tyskland stiger frem*, Oslo: Aschehoug, 2014.
42. Olav Døvik, Camilla Wernesén, and Mon, Su Tiet, “PST vil overvåke datatastaturer”, NRK, published 04. March 2014 <http://www.nrk.no/norge/pst-vil-overvake-datatastaturer-1.11583286> (accessed January, 5, 2015).
43. Police Infiltration and dissident groups, comment (*The Journal of Criminal Law and Police Science* 61 2, 1970), 194.
44. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
45. Ibid.