IEEE Standards Education e-Magazine

The IEEE Standards Education e-Magazine A publication for those who learn, teach, use, deploy, develop and enjoy Standards! Sponsored by the Standards Education Committee IEEE is committed to: promoting the importance of standards in meeting technical, economic, environmental, and societal challenges; disseminating learning materials on the application of standards in the design and development aspects of educational programs; actively promoting the integration of standards into academic programs; providing short courses about standards needed in the design and development phases of professional practice. Serving the community of students, educators, practitioners, developers and standards users, we are building a community of standards education for the benefit of humanity. Join us as we explore the three fundamental dynamics of standards--technology, economics and politics, and enjoy our feature articles about the use, deployment, implementation and creation of technical standards.

The IEEE Standards Education e-Magazine
Privacy, Freedom & Human Rights,
October 2018, Vol. 9, No. 3

Table of Contents

A publication for those who learn, teach, use, deploy, develop and enjoy Standards!

IEEE is committed to:

- promoting the importance of standards in meeting technical, economic, environmental, and societal challenges;
- disseminating learning materials on the application of standards in the design and development aspects of educational programs;
- actively promoting the integration of standards into academic programs;
- providing short courses about standards needed in the design and development phases of professional practice.

Serving the community of students, educators, practitioners, developers and standards users, we are building a community of standards education for the benefit of humanity. Learn more about the three fundamental dynamics of standards--technology, economics and politics, and enjoy our feature articles about the use, deployment, implementation and creation of technical standards.

What are Standards?
Technical standards are formal documents that establish uniform engineering or technical criteria, methods, processes and practices developed through an accredited consensus process.
Standards are:

- developed based on guiding principles of openness, balance, consensus, and due process;
- established in order to meet technical, safety, regulatory, societal and market needs;
- catalysts for technological innovation and global market competition.

Knowledge of standards can help facilitate the transition from classroom to professional practice by aligning educational concepts with real-world applications.
Join us as we explore the dynamic world of standards!

Return to Table of Contents

LETTER FROM THE EDITOR

16 October 2018

Privacy, Internet Freedom and Human Rights

Welcome to the Third Quarter issue of IEEE Standards Education E-magazine, an issue packed with perspectives on privacy, internet freedom and human rights!

It is my pleasure to bring you this issue of the SEC E-Magazine compiled and edited by Ms. Amelia Andersdotter, an expert in the domain of privacy and data protection. Her editorial itself is an educational piece which has made me realize how little I know about these topics, even unable to write a few intelligent words! I may be ignorant about this topic, but I am privileged to be surrounded by the globally renowned experts in the field. My sincere appreciation and thanks to Amelia and her panel of subject matter experts for compiling an exciting issue for us. Happy Reading!

Yatin Trivedi, Editor-in-Chief

Privacy, internet freedom, and human rights are topics which have gained increasing traction in recent years, as we will see in three articles by Prof. Ann Cavoukian, Niels ten Oever, and Lukasz Olejnik PhD. The roles of companies in the global ecosystem of rights protections have been accentuated in both standards development organizations (SDOs) and in intergovernmental settings such as the United Nations (UN).

We are no longer in the situation where privacy and the security of end-users are abstract and difficult problems for which no solution is in sight. Rather, we have advanced to where standard-setting can be a real help to engineers, deployers and implementers in realizing robust protections for private persons and consumers, boosting their confidence in the new technologies that increasingly surround them.

Similarly, technologies are increasingly being recognized for vehicles for the transformation of society. With the rise of global markets, the private sector has been recognized as a bearer for global community values, separate, but equally important, to the prior monopoly on bearing such values enjoyed by nation states.

With the rise of technologies that allow communications between people at great distances from one another, identity management has risen to the forefront of both commercial and human concerns. From Prof. Kim Keechang, we will learn about the particular concerns that arise when geographically delimited standards for identity management do not take into account global opportunities and what global standards exist to provide a remedy. Marcus Wong will also help us understand what happens when tried and tested methods for authentication turn out too onerous for the use-case.

We would be wrong to consider the emerging focus on corporate social responsibility as an abdication by nation states of moral power, however. An increased focus around the world on privacy laws—aimed at protecting individuals' autonomy, self-determination, and commercial security—and on security, has created real economic pressure on technology companies to consider their impacts on communities.

And while these economic incentives provide a helpful framework for putting people back into the mix of technology design, they come with drawbacks. Or perhaps better-stated backdoors. The rise of global communications has contributed to what French philosopher Jacques Derrida derided as a breakdown of the grand narrative of 19th-century modernism. What was celebrated in the beginning of the 21st century as a breakdown of the geographic community (the natural unity we, people, feel with other people who are living close to us) in favor of the biographical community (the unity we can perceive with people from all over the world and who share our interests, be they the effective standardization of insulin pumps, the perfect instantiation of a fuzzy network or the ingenuity of signals processing), is now beginning to create alarm.

International concerns about fake news, propaganda and competing descriptions of what a community is, what its values may be, and how communities can co-exist on our pale blue dot, the Earth, is leading to calls for security features that restrict, in particular, free communications. It is the undoing of the biographical community and a regression back into the geographical communities established during modernism.

It leads to some interesting dilemmas for engineers to bear with them.

Few concepts are as burdened by values as the concept of security. Who are we protecting from what? The answer might be that we are protecting an incumbent from innovative start-ups, or a government from its people, or individuals from other individuals, or people from its government. In many situations, we can combine a couple of these objectives, but rarely all of them. They will boil down to choices, and it is up to us as designers and developers to make those choices.

Early designs of many communications standards in widespread use today avoided the penalties of difficult security considerations by overlooking security and favoring other forms of efficiency instead. For instance, the efficiency of being able to transmit larger amounts of data more quickly, or the efficiency of more rapid execution of commands in a processor.

These and other topics of digital rights are given increasing focus through biannual IEEE Security and Privacy symposia and the Workshops on Usable Security (with one of each event organized in North America and the other in Europe), the annual The Workshop on the Economics of Information Security (WEIS), USENIX Enigma and Privacy Enhancing Technologies Symposium (PETS) conferences, covering topics from the depths of technology, to the front-ends that help us use them, and the economics that governs their launch to market.

Technical standards, lacking control mechanisms implied by strong security mechanisms, have until now prioritized flexibility and ease of use in a wide range of situations fostering competitivity and rapid development. Now we are entering into a different time.

It is the success of global communication, and its catering to our basic need as a species to learn and develop, that now brings it into contact with the more serious moral dilemmas of how to uphold human rights, and at whose responsibility and under whose influence. In this issue, we explore some of the solutions – but it is the continued commitment of all engineers that will ensure trade-offs and challenges are made visible to the people who use technologies.

About this issue's guest Editor: Amelia Andersdotter is a former member of the European Parliament and an experienced public speaker and presenter. Her current focus is the understanding of data protection not only as a law, but as a tool for advancing the fundamental principles on which democracies are built. Amelia is consultant with ARTICLE 19, a human rights-focused non-governmental organization that defends and promotes freedom of expression and information.

Yatin Trivedi
Editor-in-Chief, IEEE Standards Education eZine
Member, IEEE-SA Board of Governors
ytrivedi@ieee.org

Yatin Trivedi, Editor-in-Chief, is a member of the IEEE Standards Association Board of Governors (BoG) and Standards Education Committee (SEC), and serves as vice-chair for Design Automation Standards Committee (DASC) under Computer Society. Yatin served as the Standards Board representative to IEEE Education Activities Board (EAB) from 2012 until 2017. He also serves as the Chairman on the Board of Directors of the IEEE-ISTO.

Yatin currently serves as Associate Vice President for semiconductor design services at Aricent Inc. Prior to his current assignment, Yatin served as Director of Strategic Marketing at Synopsys where he was responsible for corporate-wide technical standards strategy. In 1992, Yatin co-founded Seva Technologies as one of the early Design Services companies in Silicon Valley. He co-authored the first book on Verilog HDL in 1990 and was the Editor of IEEE Std 1364-1995™ and IEEE Std 1364-2001™. He also started, managed and taught courses in VLSI Design Engineering curriculum at UC Santa Cruz extension (1990-2001). Yatin started his career at AMD and also worked at Sun Microsystems.

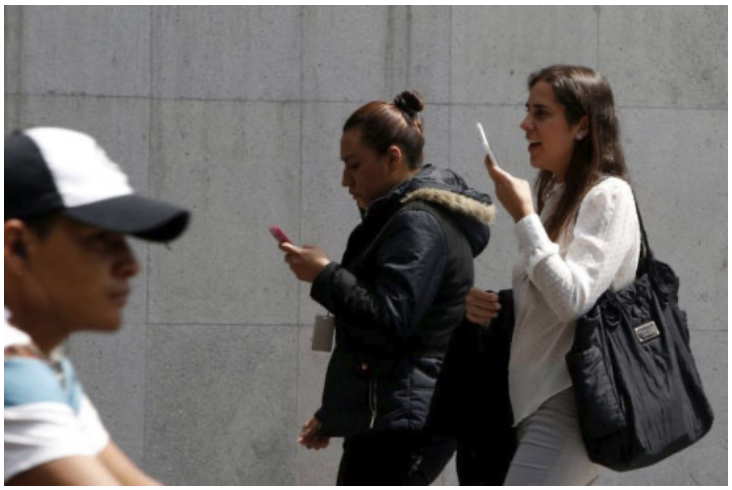
Yatin received his B.E. (Hons) EEE from BITS, Pilani and M.S. Computer Engineering from Case Western Reserve University. He is a Senior Member of the IEEE and a member of IEEE-HKN Honor Society.

Return to Table of Contents

PRIVACY BY DESIGN: THE GLOBAL PRIVACY STANDARD

16 October 2018
Ann Cavoukian

May 25, 2018 marked a significant milestone for Privacy by Design. This is the first time it has appeared in a regulatory framework, known as Europe's General Data Protection Regulation (GDPR). But we shouldn't let this overshadow earlier developments in this long road travelled. Allow me to start from the beginning.



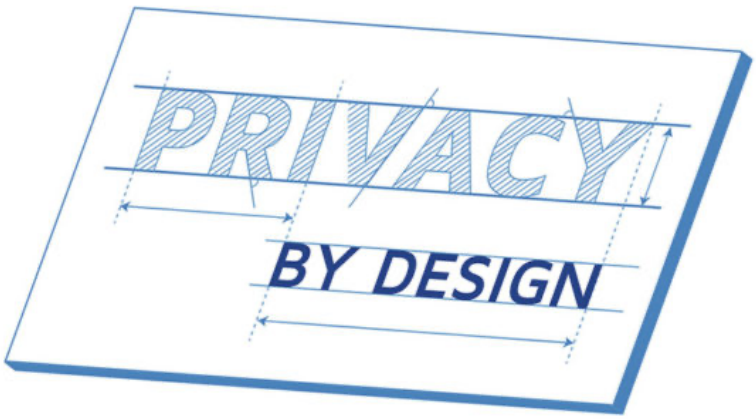
Over the last two decades, we have witnessed how the growth of technology has brought exceedingly new challenges to the protection of privacy. Individuals are now constantly subjected to new forms of intrusion and connectivity. Information technology is compact, mobile, and everywhere. You cannot walk down the street without seeing someone using some sort of mobile device that has more computing power than an office floor full of computers, just a generation ago. There is almost no aspect of our lives left that remains untouched by information and communications technology.

Continually evolving and increasingly complex privacy-invasive technologies such as biometrics and sensors have intensified the need to remain vigilant and continually evolve new methods to protect our privacy. Unlike some critics, however, who strictly see

technology as eroding privacy, I have always taken the view that technology is inherently neutral. I have always maintained, technology–which has resulted in many challenges–can also be tapped for innovative solutions, particularly for privacy and access. While technology has the ability to diminish privacy, its support can also be enlisted to protect privacy through Privacy by Design which emphasizes a positive-sum approach to privacy and technology innovation. I felt it was necessary to counter the prevailing zero-sum model, where privacy must be sacrificed for the sake of security, innovation or business interests; a view that is both false and misleading. If we change the paradigm to an inclusive positive-sum model, which allows the growth of both privacy and other functionalities, in tandem, then the future of privacy and freedom grows more certain.

It was in 2009, during my third term as Ontario's Information Commissioner, where I advanced Privacy by Design on the world stage by formally launching the 7 Foundational Principles of Privacy by Design. To ensure that Privacy by Design continued to gain strong global momentum, the principles have been translated into over 40 languages. A year later, in 2010, a landmark resolution was unanimously passed in Jerusalem by the International Assembly of Privacy Commissioners and Data Protection Regulators, recognizing Privacy by Design as an essential component of fundamental privacy protection–transforming it overnight into an international standard.

To further raise awareness, 2011 became the "Year of the Engineer," and this included reaching out to those who design and build the systems and technologies upon which we rely. This was to challenge every innovator and engineer to operationalize Privacy by Design and make it an everyday reality.



There are times when I still cannot believe the journey to make Privacy by Design the global standard for privacy. During my 16 years (three terms) as Commissioner, it was a unique historical period when the advent of the Internet would fundamentally change the very concepts of privacy and data protection. In a perfect world, we would not need privacy regulators. However, we do not live in a perfect world–far from it, and despite the advances we have made in privacy and data protection, our efforts are needed now, more than ever.

There was always a looming, yet common misconception–that privacy stifles innovation. The message is simple: Building privacy into the business ecosystem yields many benefits, ranging from cost-savings, to strengthening business/consumer relationships, to enhancing much-needed trust. This in turn creates a significant competitive advantage.

With the recognition as an international standard by international privacy and data protection commissioners in 2010, Privacy by Design Foundational Principles have since been embraced by public policy-makers, legislators, industry groups and associations as integral to their efforts to update 21st century information privacy governance systems. Alongside these gains in global recognition, these same market and technology leaders, academics, and regulators started looking at ways of translating the principles of Privacy by Design into technical and business requirements, specifications, standards, best practices, and operational performance criteria. This began as the next stage of Privacy by Design's evolution. The central challenge in producing this work over such a wide area of applications, is that there is no apparent "one-size-fits-all" response to specific privacy requirements.

For this task, there was an acknowledgement that specialized help was needed. The rise of the Chief Privacy Officer (CPO) role in organizations is a testament to the strategic importance of good information management and the demand for such skill sets. Privacy risk management as a distinct discipline is becoming more standardized and professionalized, and there is a new discipline of skilled privacy engineers and architects, if not an increased awareness of Privacy by Design amongst software developers and the like.

On the industry standards stage, such a goal was laudable and progress was made through the work of a Technical Committee of an industry standards body, the Organization for the Advancement of Structured Information Standards (OASIS), whose purpose was to develop and promote a standard for Privacy by Design in software engineering. As co-chairs, the author, in cooperation with Dr. Dawn Jutla, established the OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) Technical Committee in October 2012. The OASIS PbD-SE TC provides privacy governance and documentation standards for software engineers. It enables software organizations to embed privacy into the design and architecture of IT systems, without diminishing system functionality.

The PbD-SE TC work follows the 7 Foundational Principles of Privacy by Design:

1. Proactive not Reactive; Preventative Not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, Not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection

6. Visibility and Transparency – Keep It Open
7. Respect for User Privacy – Keep It User-Centric

PbD-SE offers a privacy extension and complement to the Object Management Group's (OMG) Unified Modeling Language (UML) and serves as a complement to OASIS' eXtensible Access Control Mark-up Language (XACML) and Privacy Management Reference Model (PMRM).

Privacy by Design principles are internationally recognized and aligned to Fair Information Principles (FIPs), Generally Accepted Privacy Principles (GAPP) and NIST 800-53 Appendix J controls. As a draft OASIS standard, it helps stakeholders to visualize privacy requirements and design from software conception to requirement. PbD-SE is a specification of a methodology, mappings, and guidance to help software engineers to : i) model and translate Privacy by Design (PbD) principles to conformance requirements within software engineering tasks, ii) produce privacy-aware software, and document artefacts as evidence of PbD-principle compliance; and iii) collaborate with management and auditors to simplify demonstration of compliance/audits.

With the advent of the Internet of Things, cyber-security professionals have long been lamenting the lack of standards in consumer goods accessing the Internet, bringing vulnerabilities that undermine data security and privacy. This year, a team of privacy experts was assembled by the International Standards Organisation (ISO) to develop the first set of preventative international guidelines that ensures consumer privacy is embedded into the design of a product or service, with protection throughout the whole life cycle. The new ISO project committee, ISO/PC 317, Consumer protection: privacy by design for consumer goods and services, will develop guidelines that are intended to both enforce compliance with regulations and generate greater consumer trust.

This recent standardization effort that complements the GDPR encapsulating all of the merits of Privacy by Design has been a long time coming. The majority of privacy breaches remain unchallenged, unregulated and unknown because there are far too many. Regulatory compliance alone is unsustainable as the sole model for ensuring the future of privacy. Prevention is needed.

I frame privacy as being essential to freedom, revolving around personal control and freedom of choice – the need to maintain user control over the collection, use and disclosure of one's personal information. This view of privacy is perhaps best reflected in the right of "informational self-determination," enshrined in the German Constitution in 1983–that the individual should be the one to determine the fate of his or her personal information. Recognizing privacy as an exercise in personal control has always been important, but it is especially critical today in an age characterized by far-reaching, ubiquitous computing, and invasive surveillance by the state.

We are experiencing an era of near-exponential growth in the creation, dissemination, use and retention of personal information. Whether applied at the level of information technology, business practices, or systems, it is more critical now than ever to embrace

Privacy by Design if privacy, as we know it, is to survive well into the 21st century. With increasingly savvy and interconnected users, an organization's approach to privacy may offer precisely the competitive advantage needed to succeed. Privacy is essential to creating an environment that fosters trusting, long-term relationships with existing customers, while attracting opportunity and facilitating the development of new ones. In an ever-changing world of emerging technologies, the right to privacy is more important than ever. We must remain vigilant in the protection of privacy, the bedrock of our freedom and liberty.

Ann Cavoukian Executive Director | Privacy and Big Data Institute, Ryerson University Dr. Ann Cavoukian is recognized as one of the world's leading privacy experts. She is presently the Executive Director of the Privacy and Big Data Institute at Ryerson University. Appointed as the Information and Privacy Commissioner of Ontario, Canada in 1997, Dr. Cavoukian served an unprecedented three terms as Commissioner. In that time, she elevated the Office of the Information and Privacy Commissioner from a novice regulatory body to a first-class agency, known around the world for its cutting edge innovation and leadership. There she created Privacy by Design, a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible.

Return to Table of Contents

MAKING WEB ECOSYSTEM SAFER – CERTIFICATES, BROWSERS, WEB

16 October 2018 | Lukasz Olejnik

Unsecured ways of web browsing are fading away at an accelerating pace. At a technical level, this is thanks to the increased deployment of Transport Layer Security (TLS)-enhanced HTTP on the web (visible in the URL bar of your web browser as HTTPS). Recent data as reported by LetsEncrypt, citing Firefox metrics, indicates that over 70% of websites are now accessed via this secured protocol, and those numbers are quickly increasing. We have reached an important milestone in information security.

This has not happened over night. Getting here involved years of security research, engineering, awareness and incentive building. Public pressure played a significant part as well. Higher standards of information security means improved user trust in the services offered on websites, and stronger opportunities for users to understand who they are trusting to, and with, what information. But to fully appreciate the road from there to here, I will focus on the technical foundations of web browsers. Three game-changing factors are particularly worth mentioning:

1. The rise in availability of affordable HTTPS certificates thanks to providers such as LetsEncrypt;
2. flagging of connections to websites as "Not Secure" by major web browsers (Chrome 68 made it the default as of July 2018);
3. the evolution of the web, driven by standardisation of browser mechanisms.

In simple terms, TLS-enhanced HTTP guarantees three important things:

1. The web user trusts the identity of a website;
2. ata integrity, namely that the transmitted data continues to be that same data, is protected from being altered, tampering during the user-server connection;
3. data confidentiality, meaning any transmitted data is accessible only to the parties of the user-server connection, is guaranteed.

Certificates

LetsEncrypt (LetsEncrypt.org) is a service launched by Internet Security Research Group (ISRG), a consortium "sponsored by a diverse group of organizations, from non-profits to Fortune 100 companies."LetsEncrypt offers cryptographic certificates for HTTPS free of charge. At the time of its launch, it was a game changer. Not only did LetsEncrypt remedy an earlier problem of the expensive cryptographic certificates necessary for HTTPS, but it also provided a simple, technical way for managing certificate renewals. Additionally, any cryptographic certificate worth its name is only valid for a limited period of time, after which the certificate holder needs to reassert continued interest.Certificate renewals ensure that the certificate is up to date even considering new security threats, that the holder still exists.

One historical obstacle facing a broad adoption of encrypted traffic was the relative computation overhead introduced by cryptographic operations needed in the use of TLS. Fortunately, modern equipment such as servers are powerful enough and this concern is no longer valid.

Aside from making it easy for any system owner to act on the altruistic desire of making web browsing safer for users, the rising numbers of secure web connections are motivated by other factors, too.

'Not Secure' flags
Web browser vendors started marking websites accessed via HTTP that is not TLS-enhanced with a "Not Secure" flag next to the URL bar. This may negatively impact user trust towards a website. In particular, it serves as a motivation for decision makers (owners, managers, etc.), and developers. Sticking to HTTP is increasingly looking unsustainable from a trust perspective.

But while browser flags are among the crucial strategic motivators for better information security on the web that are relatively well known, there are other important components of the web ecosystem that contribute to the increased interest in secure connections. Namely, standardisation.

Modern Web features require HTTPS

Modern web features make browsers powerful. Some examples are:

- Mechanisms such as the ability of using low-level hardware (e.g. sensors).
- Ability to make connections outside of the Internet, even with Bluetooth or USB.

The web browser can make these features accessible from the level of the website the user is visiting. These browsersare powerful and sensitive; and they are made—by design—available only via secured channels. From a technical perspective, this is achieved by permitting browser features to function only when accessed within "Secure Contexts" (https://www.w3.org/TR/secure-contexts/). Among the elements required to be classified as a secure context is having an HTTPS connection.

Consequently, to make a modern web application, HTTPS is becoming the norm. HTTPS is now additionally an initial element of the setup, rather than the last element. The adoption of HTTPS will be further accelerated by modern web design patterns, because information

security can no longer be an afterthought. Developers themselves will help in making this happen.

With a broad adoption of secure connections via HTTPS, many security issues of the past will be resolved. This process will take some time, but not too long. This aspect of security and privacy will be in good shape soon; and we will all benefit from it.

Lukasz Olejnik is a security and privacy researcher and advisor. He specializes in web security and privacy, privacy engineering, privacy reviews, privacy impact assessments. He has industry, research and technology policy experience, including cybersecurity and privacy policy. He contributes to privacy reviews of web standards as a W3C Invited Expert. He has completed his Ph.D. at INRIA (Grenoble, France), where he was a member of the Privatics Team. He was a Research Associate at the University College London. Lukasz is an affiliate at the Princeton's Center for Information Technology Policy. He is also currently a scientific advisor at an international organisation.

Return to Table of Contents

WOES OF GOVERNMENT DRIVEN 'STANDARD' – KOREAN PKI IMPLEMENTATION 1999-2018

16 October 2018

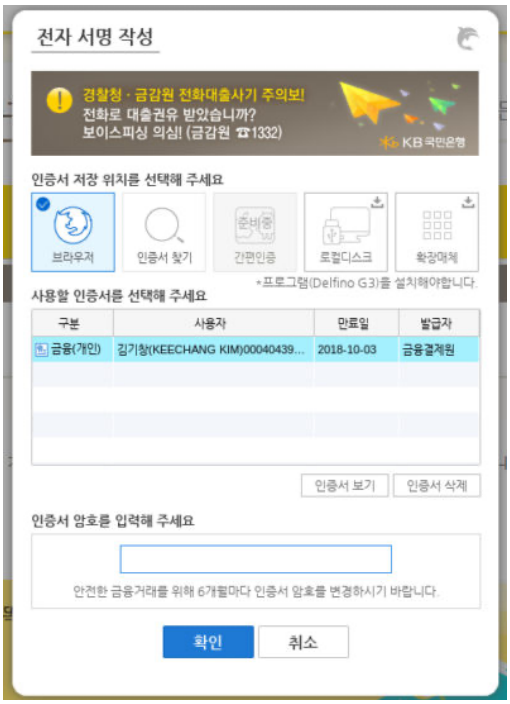
Keechang Kim, Professor at Korea University Law School

South Korea used to take great pride in its Public Key Infrastructure (PKI) implementation. Government officials could no doubt parade impressive 'numbers' and 'achievements.' As of 2016, for example, more than 35 million user certificates were issued by the Certification Authority (CA) accredited by the government under the Korean National PKI regime ("NPKI"). Korean NPKI has been in existence since 1999 in isolation from the rest of the world. Almost all internet banking, e-commerce providers and e-government agencies in Korea require users to present user certificates (issued by an NPKI accredited CA) for authentication purpose and to ensure integrity of transaction records (transaction confirmation). No other countries that I know of have achieved this level of adoption of PKI technology at the client side.

All this started in the late 1990's. Government funded researchers succeeded in developing a high-grade encryption algorithm (128 bit encryption, which was state-of-the-art in 1990s). A handful of companies came up with prototype PKI implementations for client authentication and transaction confirmation using web-browser plugins incorporating the Korean-developed high-grade encryption algorithm. Government officials were impressed with the achievements. They thought the technology would have great potential for e-commerce (which was at its nascent stage then) and e-government services as well as nationwide online identity infrastructure. Scholars were commissioned to produce consultation papers recommending legislation, 1) to introduce governmental scrutiny to ensure the security of the NPKI certification service; and 2) to grant the privileged status on government-accredited CAs.

As a result, the 1999 Digital Signature Act was introduced in Korea. It stipulates that where signature is required by law, in order to satisfy such a legal requirement electronically, one has to use the certificate issued by an NPKI accredited CA. No other electronic signatures, no matter how secure, reliable or appropriate, can meet the legal requirement for a signature under the Korean law. This outright 'legal' and systematic institutional discrimination of foreign or non-accredited Korean CAs and the preferential treatment of government accredited Korean CAs are in many ways against the UNCITRAL Model Law on Electronic Signatures. Art 3 of the Model Law stipulates that signatures must be treated equally provided that they are equally reliable (Art. 3). Art 12 of the Model Law requires global recognition of a certificate or an electronic signature regardless of the geographical location of the issuer of the certificate or the user (the signatory). The "national" regime of Korean NPKI which confers the legal effect only on the electronic signatures created using a certificate issued by an NPKI accredited CA located in Korea is against these clauses of the Model Law and resulted in a self-imposed isolation of the Korean NPKI.

Moreover, the Korean legal approach which confers a privileged status on its "national" PKI implementation and denies legal effect to all other implementations of electronic signatures is an anomaly compared to the European Union (EU) E-Signature Directive 1999 and Electronic Identification, Authentication and Trust Services (eIDAS) Regulation 2014. The EU legal approaches to electronic signatures are "inclusive" in the sense that they do not purport to deprive legal effect of any electronic signatures merely on the ground that they do not meet the requirements of qualified electronic signatures. The US state laws, which are mostly based on the Uniform Electronic Transactions Act 1999, are also inclusive in the sense that electronic signatures, regardless of their reliability, are not denied legal effect merely on the ground that they are in electronic form. But the Korean Electronic Signature Act confers legal effect only on electronic signatures created using a certificate issued by an NPKI CA located in Korea. No other electronic signatures may have a comparable legal status in Korea.



Boosted and protected by this peculiar legal regime, five or six NPKI accredited CAs have been in operation in Korea for the past two decades in isolation from the rest of the world. All these NPKI accredited CAs use more or less the same technology. They claim that they have standardized the client side PKI implementation and achieved interoperability. Which means that as long as you have your user certificate issued by one of the NPKI accredited CAs, it will not be difficult to use it for e-commerce or e-government transactions–provided that you use the supported web-browser or you installed an appropriate mobile app. All this, however, started from the government initiative to supervise the NPKI certification service and to grant special privileges to the NPKI accredited CAs.

Inside Korea, the Korean NPKI certification service has become ubiquitous and it certainly feels like a “standard” technology. But once you leave Korea, the technology and the services are hardly known. They are, for all practical purposes, un-workable for non-Koreans and even for Koreans outside Korea. Indeed, this piece of technology (as it is used for user authentication and transaction confirmation) is the one which isolates Korean e-commerce from the rest of the world as it prevents Korean e-commerce providers from reaching out to customers in the rest of the world.

But most of all, there are serious security vulnerabilities of the Korean NPKI implementation of user authentication and transaction confirmation. As the accredited CAs routinely “re-issue” user certificates online without face-to-face verification of the applicant’s identity, phishing attacks to obtain user credentials needed to obtain user certificates through online application/issuance became rampant. Every year, thousands of successful phishing attacks are reported but the banks are allowed to put the blame squarely on the so-called “gross negligence” of the users, who were merely victims of carefully orchestrated attacks. As far as negligence or gross negligence is concerned, I believe that the banks are far more negligent or even grossly negligent because they have knowingly persisted in using the method whose

weakness to phishing attacks is fully documented already. Unfortunately, Korean judges do not agree and they side with the banks rather than with the victims of the phishing attacks.

Compared to "FIDO" (Fast Identity Online), the industry standard for online authentication which started in 2013 and is currently in active development and adoption worldwide, the Korean NPKI's implementation backwardness and vulnerabilities are all the more striking. The creative breakthrough underpinning FIDO standard is to distinguish and insulate "user interaction scenario" from "authentication process." The former occurs on a given device and stays within the device. The latter occurs online between the device and the service provider. This can ensure interoperability of FIDO standard across a wide range of devices and the user interaction scenario can accommodate a variety of user-friendly authentication methods without compromising the "authentication process" which is insulated from the "user interaction scenario." Moreover, the authentication process under FIDO standard requires that a key issued to a particular website can only be exercised by that website. So phishing attempts to acquire the authentication key become useless. In stark contrast, the NPKI authentication process relies on a user certificate which can open all the doors to the websites the user is registered with. According to a recent Korean Supreme Court ruling, an attacker who has fraudulently obtained a user certificate issued by an NPKI accredited CA can even open up new accounts with any financial companies and start borrowing money in the name of the victim. This is indeed an attackers' heaven! But when a particular authentication technology is described in the statute book as "secure" or "reliable," judges are bound to show deference to the power of "words" and "provisions" rather than understanding the vulnerable realities of a complicated technology. The Korean NPKI regime is grounded on a technology which is inherently and conceptually more vulnerable compared to FIDO standard. But it enjoys a statutory backing dating back from 1999.

An old technology of the late 1990s proving to be less secure than the cutting-edge security standards of the 2010s should not surprise anyone because the technology progresses and improves. But the problem with a government driven 'standard' is that once such a government driven regime is put in place, it becomes authoritative and remarkably difficult to get rid of. After nearly two decades, the Korean government, as well as its citizens, are still stuck with the outdated authentication concept and process of NPKI client authentication. Some of those who have vested interests in the continuation of the old PKI regime are busying themselves with unconvincing proposals purportedly to "combine" FIDO and PKI. In my view, it is inherently impossible to combine these two concepts without losing or cancelling out the essential features of each of these two fundamentally incompatible design concepts. The so-called proposal for combining FIDO and PKI is merely an effort to artificially prolong the shelf life of client authentication technology which relies on "globally identifiable" client certificate. Authentication with a key (such as NPKI client certificate) which can work across all websites

is now a shockingly vulnerable concept. Had NPKI not been supported by the government, the industry in Korea would have been much more swift in learning about and realizing its vulnerabilities, and would have much sooner adopted better and newer alternatives including the industry standard such as FIDO.

South Korean government at long last accepted that they made a wrong decision in 1999. In 2018, the government prepared a bill to completely abolish the government accredited NPKI regime. The bill is now in the National Assembly. One hopes that it passes before the twentieth anniversary of NPKI regime in Korea. Governments in other countries should take the Korean NPKI episode as a cautionary tale about the importance of governmental non-interference with industry standard in the authentication and online identity technologies.

---

1. "FIDO UAF and PKI in Asia – Case Study and Recommendations", pp. 4-5. https://fidoalliance.org/wp-content/uploads/FIDO-UAF-and-PKI-in-Asia-White-Paper.pdf
2. For a detailed discussion, see Keechang Kim, "Reform Proposals for the Korean Electronic Signature Act", Journal of Comparative Private Law, vol 24, no. 4 (2017) pp. 1883-1930 (in Korean).
3. Article 5(2) of E-Signature Directive 1999; Article 25(1) of eIDAS Regulation 2014.
4. UETA, Section 7(d). Also see US Federal E-Sign Act (15 USC 7001) Section 101(a)(1), 101(a)(2).
5. For a brief overview of the Korean NPKI certification service, see Keechang Kim, "Recent Changes in the Regulatory Landscape for e-commerce in South Korea", 16 Asian Business Lawyer 78 (2015).
6. The FIDO Alliance Whitepaper on Privacy Principles, (Feb 2014), p. 5. http://fidoalliance.org/wp-content/uploads/2014/12/FIDO_Alliance_Whitepaper_Privacy_Principles.pdf
7. Supreme Court Judgment 2017Da257395, dated 29 March 2018.
8. See, for example, https://fidoalliance.org/wp-content/uploads/FIDO-UAF-and-PKI-in-Asia-White-Paper.pdf (April 2018).

Keechang Kim
Professor Kim studied law at Seoul National University (LLB), Chicago Law School (LLM) and Cambridge University (PhD). He teaches contract, tort, e-commerce law at Korea University Law School. He is a Member of the Korean Bar Association, with frequent involvement (either as an arbitrator or as an expert witness) in international arbitrations. He is currently serving as an advisor to Culture, Media and Telecommunications Team of Legislation Research Commission of the National Assembly of Korea. His publications include Inconvenient Truth of the Korean Internet (2009). He has been leading the Open Web Movement in Korea, which advocates standard compliance in internet technology. He is currently a director of Open Net Korea, a charitable foundation promoting individual's rights and freedom in the cyber space.

His research interests are internet and the law, encryption and information protection technology and regulation of online transactions.

Return to Table of Contents

IOT SECURITY CONSIDERATIONS IN 5G

16 October 2018

Marcus Wong, Huawei Technologies (USA)

With Phase 1 of the 3GPP 5G Standards mostly finalized as of June 2018, the network equipment vendors can start building the products so that the operators can start commercial deployment of the "official" version of the 5G networks. However, because 5G is much bigger than anyone had anticipated, 3GPP has divided 5G standards in phases so that the network operators can start rolling out their networks for offering 5G services. Phase 2 is due for completion in December of 2019. While Phase 1 of 5G is focused on the use cases that is primarily known as the Enhanced Mobile Broadband, Phases 2 is about Massive Machine Type Communications and Ultra-Reliable and Low-Latency Communications [1].

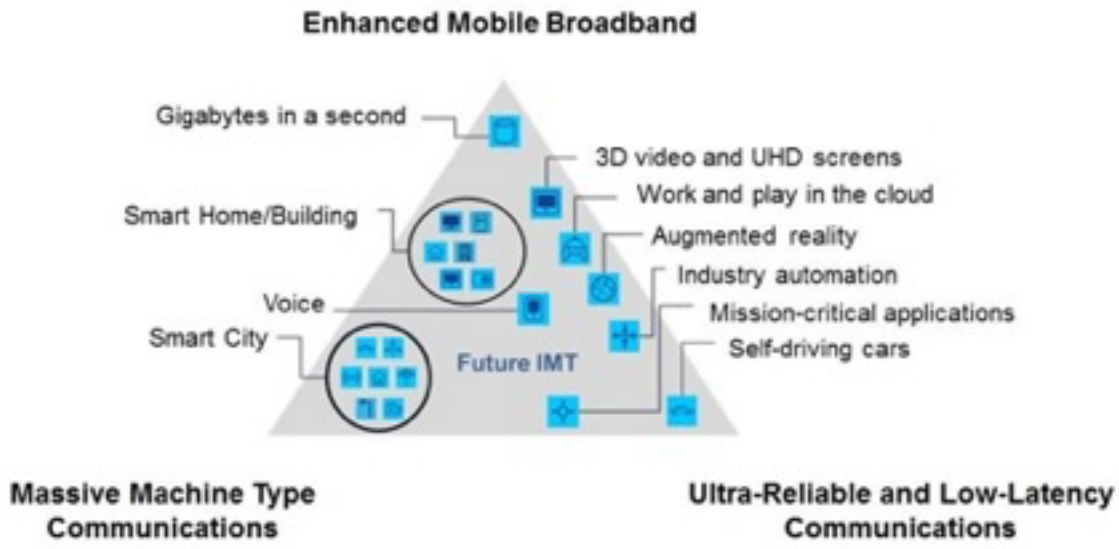


Figure 1. ITU-defined 5G Use Cases

Security, being of the utmost importance for the network operators, is enhanced in Phase 1 of 5G, taking an evolutionary approach with enhancements in a number of areas [2]: cryptographic algorithm enhancements, unified authentication framework, on-demand

security policies, and subscriber identity privacy protection. For the most part, the initial 5G network security is identical to that in LTE. Furthermore, additional enhancements will be afforded in Phase 2 to provide the needed security to support Internet of Things (IoT) in both Massive Machine Type Communications and Ultra-Reliable and Low-Latency Communications.

Security aspect of Machine Type Communications, also known as Machine-to-Machine (M2M) and later has become known as what is called IoT today, has long been studied and supported in 3GPP as early as in Release 8 (R8) with various enhancements in later releases. Since the coming of the age of mobile broadband with the release of LTE in R8, the Internet and mobile convergence has taken a giant leap forward, blurring the lines to the oblivion with faster network speeds as well as wider bandwidth. Whether it is called M2M or IoT and whether it is in Release 8 or Release 16, the security goals are the same: to ensure the security of IoT devices and services.

IoT by definition is the network of devices, whether they are embedded in sensors, appliances or automobiles, that enables other things or devices to communicate. These devices are designed to be low cost, low power, and low throughput devices while having communications capabilities such as wired connection using Ethernet or wireless connections using WLAN, Bluetooth, 3G, 4G or 5G technologies. The nature of these devices poses a number of security challenges:

- Physical constraints, low power, low cost, and lack of physical security
- Theft and physical tampering
- DoS/DDoS attacks on the networks
- Unsecure credentials (hardcoded, defaults, etc.), Unsecured interfaces (web interface, open ports), Unsecured configurations
- Unprotected data paths
- Protocol weakness
- SW implementation errors
- Difficult to update firmware, OS, or security patches

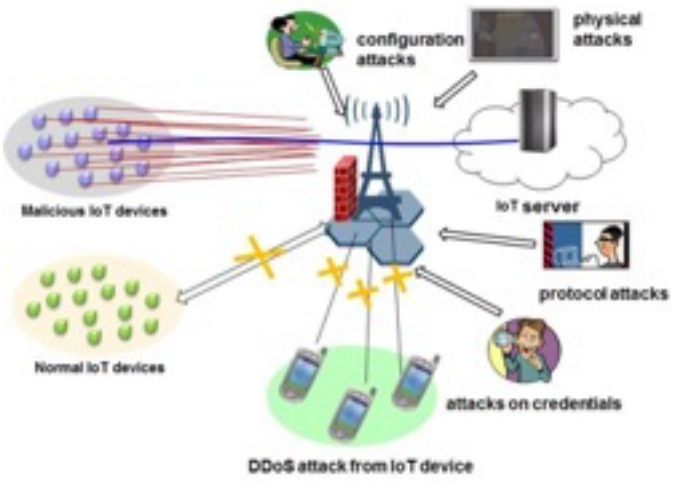


Figure 2. IoT Attacks and Threats

Recent reporting of attacks on the Internet and IoT devices connected to the Internet [3] has been largely attributed to poor security designs that allowed hackers to take advantage of, launching massive and sustained attacks that crippled or slowed down a number of websites including that of Amazon, Netflix, etc. Other attacks that gained notoriety include Stuxnet attack between 2010 and 2014, "Cold in Finland" in 2016,"Mirai botnet" in 2016 and similar "Cold in Finland" attack [4].

To meet the challenges and the requirements, let's look at some potential security options, including "lightweight" security. Lightweight of course should not be associated with less secure as it would defeat the purpose of the security solution being applied. The goal of lightweight security is not to compromise security by having lower security levels than that of the commonly acceptable (i.e. 128-bit security or equivalent) level or to which the protection level for a particular services is designed for. For example, it would be overkill to design a fool-proof encryption solution for a remote rain sensor that reports whether it is raining or not, a report that consists of one-bit of information with a value of either "1" or "0". On the other hand, it is not as simple as protecting the trivial and perhaps harmless data being communicated by the sensor, but imagine there are millions of these sensors sending the same report over a wireless network, at best, it causes congestion of the network and at worse, it is a legitimate case of denial-of-service attack. It is rather a design of security that takes into consideration the constraints, use cases of IoT devices, attack vectors, as well as many other aspects. While many security solutions have been incorporated to secure IoT for 4G and earlier, research for IoT security enhancements is still ongoing for 5G. A sample of such options is being explored here. Though these lightweight security considerations alone do not constitute a complete security solution, but are meant to be used in conjunction with other security measures.

Lightweight cryptographic security solutions include design and consideration for cipher algorithm, hash algorithm, authentication algorithm, pseudorandom number generators, and other techniques to live within the constraints of IoT devices. One such algorithm is a block cipher, one that takes a fixed size input and produces a fixed size output (e.g. AES), by a team of researchers from Ruhr-University in Germany, Technical University Denmark in Denmark, and Orange Labs in France [5]. The cipher takes advantage of hardware implementation and achieves comparable security as AES but with much higher efficiencies in terms of power consumption, hardware footprint, code size, and RAM use. Other lightweight cryptographic algorithms [6] are also being researched, studied, and considered for standardizations in ISO/IEC 29192 [7] and possibly other standards such as 5G. These algorithms include block ciphers, stream ciphers, public key algorithms, and message authentication codes, to name a few.

One-time-pad (OTP) is the most secure form of cipher technique there is. Its security lies in the fact that each message being protected with a unique key stream that is used exactly once, making traditional crypto-analysis of plaintext and cipher-text essentially useless. Not traditionally considered as a lightweight security technique, but because of the "single-use and throw-away" nature of the key stream used to protect the message being

communicated by IoT devices, OTP is also “light” in the sense that it is a simple XOR operation of the OTP with the OTP. On the downside, OTP needs to be coupled with an efficient or lightweight key stream generator (e.g. hash algorithm) or an efficient key distribution scheme.

Recently, Blockchain technology has gained traction as a security tool for smart contract, among other things. It is used in cryptocurrency, but it is also being considered for IoT. The case of using Blockchain in IoT is also very strong. Not only Blockchain relies on a decentralized architecture that is inherently resilient to single point of failure, it also has mathematically provable immutable and incorruptible characteristics. In IoT security, Blockchain can provide a clean-state proof, an integrity snapshot of the network’s initial state of both the network and the IoT devices that can include software, hardware, firmware, configuration file, security policy, network activities, device location, IP address, user behavior, file system, etc. At run time, it can provide continuous data signature verification to determine whether the network is not compromised, and whether the clean-state proof is still valid. This feature is also particularly helpful for managing and control software for potential attacks on the devices or on the network.

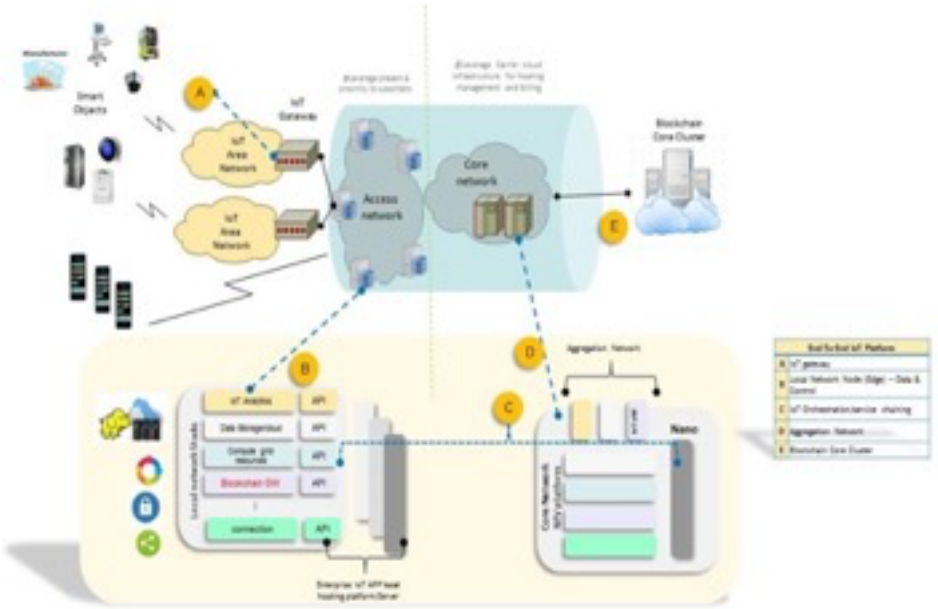


Figure 3. Blockchain and IoT

Many other security solutions are possible, including many network-based solution that emphasize the greater capabilities of the network in securing IoT. In conclusion, this article has only scratched the surface of the potential research and solutions briefly looking into lightweight cryptography, OTP, and Blockchain technology for securing IoT in 5G and beyond. While research in IoT security has come a long way and the resulting technologies are making its way into the standards, much more still needs to be done. There is a fine balancing act as far as IoT security is concerned, taking into consideration IoT devices

bound by the limitation of cost, efficiency, power, and security. The constraints are clear and the security goals are clearer. Much more needs to be done to make Internet of Things more ubiquitous and secure than ever. As 5G has just begun, stay tuned.

References:

1. ITU-R: "IMT Vision – Framework and overall objectives of future development of IMT for 2020 and beyond", September, 2015.
2. 3GPP TS 33.501: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspect; Security Architecture and procedures for 5G system (R15)", June, 2018.
3. Wall Street Journal: "Hackers Infect Army of Cameras, DVRs for Massive Internet Attack", September, 2016.
4. ZDNet: "Five nightmarish attacks that show the risk of IoT security", June, 2017.
5. Proceedings from Cryptographic Hardware and Embedded Systems – CHES 2007: "PRESENT: An Ultra-Lightweight Block Cipher", September, 2007.
6. Internet Architecture Board Whitepaper: "Lightweight Cryptography for Internet of Things", March, 2011.
7. International Standards Organization: "ISO/IEC 29192 Information technology – Security techniques – Lightweight Cryptography", January, 2015.

Marcus Wong has over 20 years of experience in the wireless network security field with AT&T Bell Laboratories, AT&T Laboratories, Lucent Technologies, and Samsung's Advanced Institute of Technology. He is certified CISSP.

Marcus has concentrated his research and work in many aspects of security in wireless communication systems. Marcus joined Huawei Technologies (USA) in 2007 and continued his focus on research and standardization. Marcus has held elected official positions in both WWRF and 3GPP. He also served as guest editor in the IEEE Vehicular Technology magazine. As an active contributor, author, and publisher, he has shared his security research on a variety of whitepapers, book chapters, and speaking engagements.

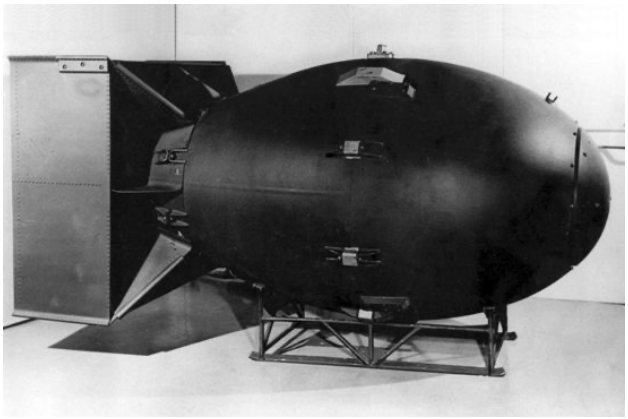
Return to Table of Contents

UP TO WHOSE STANDARDS?

16 October 2018

Niels Ten Oever

The society of the future will be built on the standards and technologies of today and tomorrow. This means that design choices of today can have serious ethical impacts in the future. This article examines approaches of integration human rights considerations in technical standards.



Atom Bomb There is a long history of scientists and engineers foregrounding the ethical aspects of their work, ranging from Einstein's precautions about the atomic bomb to current day discussions about the lack of public availability of academic publications. But even where the impact of a new technology, such as a bomb, seems obvious – especially with hindsight – it hasn't always been perceptible while the technology is still under development. In fact, only when the atomic bombs' destructive power was unleashed on the world did physicists develop a culture of ethical responsibility towards research.

It's been argued by cryptographer Phillip Rogaway that computer scientists and cryptographers are still only beginning to go down the path already travelled by physicists. To realize their impact on society, and to maintain, in light of this impact, a structured approach to assessing (in the best case even mitigating) effects of their research actions.

Somebody else's problem? At this point some engineers might think: 'but technology is neutral,' or 'is this really my job, can I not leave this to the lawyers?'

20th century historian of technology, Melvin Kranzberg, argued against such excuses. 'Technology is neither good nor bad; nor is it neutral,' is the first of Kranzberg's laws of technology. It elegantly illustrates how technology in and of itself has no agency, but that it provides another ordering to reality, which in turn has a direct impact on people's lives.

Lawyers can perhaps assess the legality of certain technologies, or the contracts governing their sale or use, but similarly to security considerations, ethical or human rights implications cannot be left to lawyers alone. Modern communications technologies are often layered and part of an otherwise complex system. We need enlightened engineers, so let's delve into the starting points of enlightenment.

Ethics? Rights? Impacts?

Human rights have a long history which culminated in 1947 in the Universal Declaration of Human Rights. The declaration in turn is codified in international human rights treatieswhere treaties focus on obligations for states.here were also a set of instruments developed in the 1970s to analyze the applicability of human rights to the private sector.

By the year 2000, the United Nations (UN) Global Compact and Corporate Social Responsibility emerged as guiding principles for human rights. In 2001,further iterations led to the adoption of UN Guiding Principles for Business and Human Rights. Today, these principles are a de facto authoritative global standard for holding the private sector accountable for their impacts on human rights.

Choosing human rights as the moral framework is aligned with international developments and adopts a language for morality and ethics which is immediately recognizable to consumers and private persons. It is the most straight-forward, tried and tested and recognized framework to use for assessment.

The question still remains: How this could be done in practice? Luckily, there are examples.

Routing it right

The Internet Engineering Task Force (IETF) makes standards for networking protocols, ensuring that our data packets can be efficiently passed from one device to the other. In its sister organization the Internet Research Task Force (IRTF) there has been ample discussion on the impacts of networking protocols on human rights.

The Human Rights Protocol Considerations Research Group (HRPC) as well as plenary discussions have given rise to concrete a framework for human rights assessments. The document called RFC8280 outlines the relationship between Internet protocols and human rights, provides an overview of literature on the topic and illustrates the relation between specific rights, such as 'freedom of expression' or 'privacy,' and specific technological

features, such as ‘internationalization’ (making a standard usable for individuals of many different linguistic backgrounds, including those that do not use latin alphabets).

RFC8280 illustrates the relationships between particular protocols and human rights, presenting specific assessments of IPv4, HTTP, XMPP, DNS, VPNs and ends with concrete Guidelines for Human Rights Considerations, a questionnaire with explanations and examples that allow standard developers to interrogate their technologies and their potential impacts.

The Guidelines for Human Rights Considerations aim to be general, but not too general, and specific, but not too specific. They build upon an already existing corpus of knowledge inside the IETF with respect to values enshrined in IETF technologies (see e.g. RFC3935), and previous, impactful documents with a narrower focus on ‘privacy’ (e.g. RFC6973).

To know and to show

Engineers often need to balance between different outcomes while they are optimizing their solutions. To get the right optimization it is important that all indicator values are known, or the experiments will lead to sub-optimization or simply no optimization at all. The work at the IETF stresses the importance of using human rights considerations as part of those indicators–mapping potential negative or positive impacts and documenting the design choices can significantly help address impacts that might arise.

Such mappings are also a selling point: as value chains become increasingly complex, consumer information is all the more important. Recognising your technical design choices for what they are, a way of influencing individuals and communities, makes the future safer and more relatable.

If we look at networking protocols again, a group of engineers is now structurally analyzing technical documents for their human rights impact and seeking to understand how negative impacts can be mitigated and positive impacts can be strengthened, using HRPC as their platform. This brings the end-user perspective closer to the development of technologies on lower layers in complex technologies.

The ability of scientists and engineers to analyze today’s technologies on their human rights impact will inevitably lead to a future in which rights and freedoms are more respected.

References:

OHCHR, HR/PUB/11/04, Guiding Principles on Business and Human Rights.
Phillip Rogaway, The Moral Character of Cryptographic Work, Essay written to accompany an invited talk (the 2015 IACR Distinguished Lecture) given at Asiacrypt 2015 on December 2, 2015, in Auckland, New Zealand.
RFC8280, Research into Human Rights Protocol Considerations, https://tools.ietf.org/html/rfc8280

RFC6973, Privacy Considerations for Internet Protocols.
https://tools.ietf.org/html/rfc6973
RFC3935, A Mission Statement for the IETF, https://tools.ietf.org/html/rfc3935

Niels ten Oever is a PhD candidate in the Datactive Research Group at the Media Studies department at the University of Amsterdam. His research focuses on the evolution of the notion of public interest in the Internet architecture.

His other research interest include global governance innovation and how invisible infrastructures provide a socio-technical and socio-technical ordering of our societies and how that might influence the distribution of wealth, power and possibilities.
Previously Niels has been Head of Digital for ARTICLE19 where he designed, fundraised, and set up the digital programme which covered the IETF, ICANN, IEEE and ITU. Before that Niels designed and implemented freedom of expression projects with Free Press Unlimited. He has a cum laude MA in Philosophy from the University of Amsterdam

---

Return to Table of Contents

FUNNY PAGES: IN THE FUTURE

16 October 2018
Bob Mankoff

"In the future, everyone will have privacy for fifteen minutes."

Return to Table of Contents

ABOUT THE IEEE STANDARDS EDUCATION E-MAGAZINE

A PUBLICATION FOR THOSE WHO LEARN, TEACH, USE, DEPLOY, DEVELOP AND ENJOY STANDARDS!

Technical standards are formal documents that establish uniform engineering or technical criteria, methods, processes and practices developed through an accredited consensus process. The purpose of this publication is to help raise awareness of standards, show the importance of standards, present real-world applications of standards, and demonstrate the role you can play in the standards development process. Knowledge of standards and

standards activities can help facilitate your professional engineering practice and improve technological developments to meet the needs and improve the lives of future generations. Standards are:

- developed based on guiding principles of openness, balance, consensus, and due process;
- established in order to meet technical, safety, regulatory, societal and market needs;
- catalysts for technological innovation and global market competition.
- Knowledge of standards can help facilitate the transition from classroom to professional practice by aligning educational concepts with real-world applications.

IEEE is committed to:

- promoting the importance of standards in meeting technical, economic, environmental, and societal challenges;
- disseminating learning materials on the application of standards in the design and development aspects of educational programs;
- actively promoting the integration of standards into academic programs;
- providing educational materials about standards needed in the design and development phases of professional practice.
-

Serving the community of students, educators, practitioners, developers and standards users, we are building a community of standards education for the benefit of humanity. Join us as we explore the dynamic world of standards!

Return to Table of Contents