IOT & TRUST

Researchers Conference Booklet

BERLIN, FEBRUARY 22ND AND 23RD

ALEXANDER VON HUMBOLDT INSTITUTE FOR INTERNET AND SOCIETY

IOT & TRUST

Researchers Conference Booklet

BERLIN, FEBRUARY 22ND AND 23RD

ALEXANDER VON HUMBOLDT INSTITUTE FOR INTERNET AND SOCIETY

CONTENT

INTRODUCTION

PROF. DR. DR. INGOLF PERNICE &
PROF. DR. DR. THOMAS SCHILDHAUER, HIIG

If you have been following the predictions on the number of internet-of-things (IoT) devices made by the media and outspoken industry authorities, you will most likely have come across some astronomical figures: in 2010, Hans Vestberg (formerly at Ericsson) predicted 50 billion devices by 2020, and Dave Evans of Cisco supported this number in his 2011 white paper. A year later, IBM and McKinsey went far past these estimates and predicted 1 trillion devices in the near future.

It is 2017 now and we are far off these sky-high numbers. It seems that we are closer to what Gartner, a technology research consultancy, assessed in 2015, namely that the world currently uses between 6 and 7 billion IoT devices. Notwithstanding the numbers, many view the IoT as a paradigm-shifting set of technologies that ought to transform almost every aspect of our daily lives. It allows for the increased automation of different processes, sensor-actuator interaction and decision-making systems in general. IoT devices and networks can be fully independent of human interaction. The move from the internet of computers to the internet of things depends on social acceptance, i.e. trust in these increasingly autonomous systems. Hence, the concept of trust can and must play a pivotal role for the future of the IoT.

The Humboldt Institute for Internet and Society (HIIG) is taking this opportunity to explore the role of trust in the adoption of new technologies and to highlight the relationship between the IoT and trust. Since 2016, an interdisciplinary research project at HIIG has been focusing on the IoT and its relationship to (a) eGovernment and (b) entrepreneurship. A team of five researchers is looking into legal and societal implications, technology adoption and implementation, and the convergence of research questions originating from various research disciplines, such as economics, engineering, law, sociology and computer science. Again and again, trust has emerged as an overarching and recurring concept.

That is why we have decided to make trust a central element of an interdisciplinary conference. The HIIG aims to broaden our perspective and that of our peers on the evident interrelation of IoT and trust. In February 2017, we invited leading experts from diverse academic and occupational backgrounds — ranging from industry experts to distinguished researchers — and gave them an opportunity to present their ideas and current research in progress. Our goal was to identify the challenges, opportunities, and limits of the adoption of the IoT in various fields as an increasing number of IoT applications are being developed for consumers, the industry and public administration.

In this booklet, we have compiled the contributions of the conference's participants. Our gratitude goes to Ms Berger, Mr Blind and Mr Niebel, Mr Fox, Mr Hölzel, Ms Loh, Mr Michel, Ms Neumann, Mr Schrape, Mr Schröder, Mr Tech and Mr Weber for their papers, and Ms Hoffmann for her introductory keynote. This booklet is meant as a snapshot of various perspectives on the IoT, indicating what academics and practitioners are currently concerned with. It also shows which overlaps different schools of theory and academics from diverse fields tap into when conducting research on this new suite of technologies. In short, this booklet provides nine exciting and interdisciplinary theses on the IoT and trust.

Coxhead, P. (2012). *Internet of Things — An Introduction.* IBM, UK.

Evans, D. (2011). *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.* Cisco Internet Business Solutions Group, white paper.

Gartner (2015). *Gartner Says 6.4 Billion Connected „Things" Will Be in Use in 2016, Up 30 Percent From 2015.* Gartner Symposium/ITxpo 2015, press release.

McKinsey (2013). *Disruptive Technologies.* McKinsey Global Institute, May 2013.

Vestberg, H. (2010). *CEO to shareholders: 50 billion connections 2020.* Ericsson, press release.

ESSENTIAL QUESTIONS FOR THE IOT & TRUST

TRUST & TECHNOLOGY: A PHILOSOPHICAL PERSPECTIVE

DR. JANINA LOH, UNIVERSITY OF VIENNA

1 | TRUST AND TRUSTWORTHINESS

Since the time of the ancient Greek philosophers, trust has been situated between the poles of ignorance and knowledge, between the dissemination of information on the one hand and control on the other. This is the first element I would like to stress: Trust is an in-between concept in that it is not needed in contexts when there is complete knowledge, and is not possible in situations when there is no information at all. Accordingly, "[t]rust is relevant 'before one can monitor the actions of [...] others' (Dasgupta 1988, 51) [...]. One must be content with them having some discretionary power or freedom [...]. Hence, one cannot reject being vulnerable" (McLeod 2015, 4).

A second element I would like to highlight is that trust requires a fundamentally optimistic view regarding the trusted individual (McLeod 2015, 3-5). Imagine you call a plumber because you have a defective water pipe. You trust the plumber to really be a plumber, that is, someone who will not rob you. But you expect (and not trust) the plumber to know the rules that define the role of being a plumber, which means primarily that she knows how to repair defective water pipes. Apart from that, you genuinely have to trust the plumber to interpret these rules according to the case in question and to use good judgement in exceptional circumstances. This is where trustworthiness comes into play: We deem the plumber to be trustworthy not because of our expectations regarding her knowledge of the rules that define her role as a plumber, but because of our assumption that the plumber is equipped with the capacity for judgement. The crucial point is that there are no objective guidelines that tell us what good judgment is in general and how often someone should be allowed to fail to exercise good judgment and still be deemed trustworthy. Judgement as practical reasoning (i.e., more than rationality) depends on the context (e.g., is it a friend or the plumber), on the experience the trusting person has with the trustee in question, and on the level of justified expectations that regulate and circumscribe the concrete sphere of trust in this situation.

This notion of trust implies that we primarily trust people and not things. This third element follows from the capacity to judge, which usually is regarded as a human competence.

To sum up: Trust is an optimistic attitude that someone holds toward a person in a situation of uncertainty that said person is equipped with the capacity for judgment.

2 | HANNAH ARENDT'S PERSPECTIVE ON TRUST

In this section, I attempt to elaborate on this understanding by taking a closer look at Hannah Arendt's perspective on trust. In The Human Condition (1958), Arendt outlines a theory of action and differentiates between three types of activity: labor, work, and action. Put briefly, activities of labor are repeated processes without a clear beginning and a definite end that are directed at self-preservation and reproduction. The results of labor are consumable. Activities of work, on the other hand, require a vision that drives them and that defines their beginning and consequences. The results of work are durable objects that become part of and constitute the world of human existence.

Actions—the genuine human form of being active—include words and deeds. Human beings are only able to act together. Actions are located between human beings insofar as one person can only begin an action but is not able to control its consequences. People are individually responsible for starting an action, but only collectively responsible for the outcome of that action. Whenever we truly act, we don't actually know what we are doing due to the unpredictability and irreversibility of the course and results of an action. To be precise, there is no definite end to or result of one action, as actions cannot be viewed in isolation. Instead, actions are genuinely interconnected: One action gives birth to further actions. Most importantly, true action involves judgment. One cannot act without judging (practical reasoning, not pure rationality). Adolf Eichmann is Arendt's most famous example of a person that only repeats things in parrot fashion and exclusively does what she is being told to do (1963).

Against this backdrop, it becomes clear that trust is not needed in contexts of labor and work (because, following Arendt's understanding of these terms, the results of labor and work are per se completely controllable and predictable) and it is not possible in Eichmann-like cases, i.e., where someone just follows rules and speaks in empty phrases, lacking personal judgment altogether; this is because such a person is potentially able to do anything she is being told to do. More pointedly: Such behavior confronts the trusting person with something more like an uncontrollable force of nature than a person using judgement. Trust is (following Arendt) possible and necessary only in cases of true action, meaning that we need to trust due to the unpredictability of actions, and it is possible to trust because the involved persons have the capacity for judgment.

To sum up: Due to the capacity for judgment that materializes in the actions of human beings, we are able to trust whenever we do not possess complete knowledge (as opposed to cases of labor and work where we—following Arendt—in fact do possess full knowledge), and we naturally trust as long as we are not confronted with a person that does not use judgement altogether.

3 | TRUSTING THINGS

The passage above hopefully explains the difference between justified expectations due to knowledge about roles, rules, and laws on the one hand, and genuine trust due to the assumption of the capacity for judgment that interprets these roles, rules, and laws on the other. Since judgment is generally regarded as a human competency, Arendt would agree that we commonly only trust people and not things.

If we say that we trust our car to function properly, we actually trust the people who built the car. Our trust does not apply to them having the necessary knowledge to build a functioning car (this we justifiably expect), but to interpreting their roles as car manufacturers and designers adequately, to making good judgments in situations of uncertainty, and to being able to navigate within the rules and laws that define their professions. However, under normal circumstances, it is absolutely sufficient to "only" rely on justified expectations. According to this notion, trust is essentially bound to the capacity for judgment; every entity that is thought to be equipped with the capacity for judgment is potentially trustworthy. The claim to "trust your own car" is therefore only a metaphorical usage of the term "trust," insofar as one is actually saying that she holds the justified expectation that the car will function properly.

When it comes to intelligent artificial systems, the case is slightly different: Depending on the definition and degree of judgment, some artificial platforms might (in a rudimentary sense) be called at least potentially trustworthy. Take, for instance, a system for regulating traffic (this example applies to the internet of things as well) that scales safety-relevant factors such as weather conditions via sensors and uses this information to control and regulate traffic by applying restrictions on overtaking or by redirecting the traffic (Djeffal 2017). If we say that we trust these systems, we actually mean that we hold a justified expectation that they will work adequately. Trust is not necessary in this case. Yet at the same time, such a system for regulating traffic has a higher autonomy in its decision-making processes than a conventional car. It processes data without direct human intervention, reacts autonomously to specific circumstances, and may even adapt its behavior.

To sum up: Intelligent artificial systems challenge our understanding of trust, which is traditionally restricted entirely to humans. This is because such systems have increased levels of autonomous behavior, which could allow us to ascribe to them a quasi-form of judgment. Effectively, this opens two doors that we can step through: (A) we can either categorically refrain from trusting things—even the smartest things—altogether. (B) Alternatively, we can define a threshold to a degree of judgment that allows us to call at least some very intelligent artificial systems potentially trustworthy.

4 | RISKS OF TRUSTING

As we have seen, trusting a person entails certain risks. The most obvious and serious risk of trusting lies in the danger of betrayal or fraud. In the example of the system for traffic regulation, this means that if we select option A and do not trust the system but instead trust the people who built it, the risk of fraudulent behavior is intimately connected to the involved human beings. Since the system is not equipped with the capacity for judgment—although it in fact might be very autonomous—it is not by definition able to "betray" those who rely on it. It might suffer severe internal malfunctioning, which may lead to catastrophic results. Under perspective A, however, the functioning of the system has nothing to do with trust, but rather with justified expectations. Fraud remains an inherently external danger to the system that compromises the integrity of the system, insofar as someone controls it for personal aims, for instance (Djeffal 2017).

If we choose option B and regard the system as capable of judgment in a limited sense (judgement as rationality or as minimal practical reasoning), the possibility of fraudulent behavior is not restricted to the human beings who built the system. Since we, under this perspective, trust the system to judge adequately in some very limited contexts, our trust may be betrayed by the system, and not only by the human beings involved. The external dangers (system integrity, data security) remain external insofar as they involve human beings. Additionally, however, the external factors become internal as well, since the system itself has now become an object of trust.

To sum up: The brief reflections here show that there is always a price to pay for trusting someone (or something). Before deciding whether to opt for option A or B, we should be sure that we would be happy with the consequences that might follow from our decision.

REFERENCES

Arendt, Hannah (1958): The Human Condition. University of Chicago Press.

Arendt, Hannah (1963): Eichmann in Jerusalem: A Report on the Banality of Evil. Viking Press.

Dasgupta, Partha (1988): "Trust as a Commodity". In: Gambetta, Diego (ed.): Trust: Making and Breaking Cooperative Relations. New York: Basil Blackwell, pp. 49-72.

Djeffal, Christian (2017): "Das Internet der Dinge und die öffentliche Verwaltung. Auf dem Weg zum automatisierten Smart Government?". In: DVBL.

McLeod, Carolyn (2015): "Trust". In: Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/trust/ [2/14/17].

TRUST, DATA PROTECTION & THE IOT

JONATHAN FOX, CISCO

DESIGNING FOR PRIVACY AND TRUST

We trust based on our understandings and beliefs.

There was a time when we believed we were anonymous (or, at least, not identifiable) at our choosing when we went online. That is, you could go online and no one would know where you surfed, what interests you had, or who you were. Sharing information about yourself (true or otherwise) was an overt act. An act of commission and participation.

We also believed that the internet was free. That, like the TV or radio, it existed with at cost or minimal cost to the consumer, the user.

These beliefs were fundamental to how we thought of, trusted, and behaved online in its early days, and it has shaped our thinking about and trust in the internet to this day.

Unfortunately, these beliefs were false, and the trust they engendered has proven misplaced. For that reason, I consider these beliefs to be myths, and not merely myths, but the fundamental myths of the internet.

We now know that on the internet you are anything but anonymous—unless you take very specific measures—and that it is not free. It is not that those beliefs were completely wrong at the time. They weren't—but over time our ability to collect, transmit, and decipher data into information has changed. What was once true and understood about how information was processed is no longer true today.

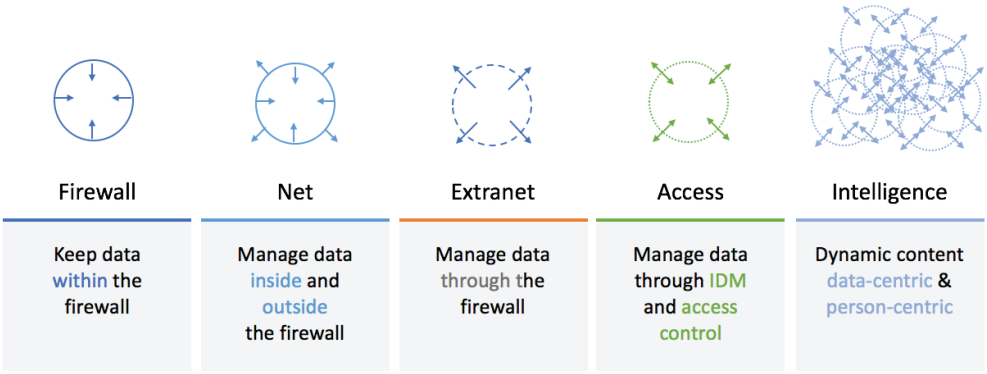
This is the challenge of trust. Things change, and the change is often gradual—like the proverbial frog in the pot of heating water that doesn't notice the water's gradual heating until it is too late and the water is boiling. Behavior that was once predicated on one set of beliefs continues to be conducted as underlying principles change, often without full recognition of the change or the chance to realign, reset, or renegotiate the conditions of trust. Often this change, like for the frog, is gradual and not sudden. When this change happens and we are not aware of it, don't agree with it, or are helpless against it, that is when trust is broken.

So, what does this have to do with privacy? We are in a time of change.

We are in the fifth stage of the information age. At this stage, there are multiple, often seam-

less, overlapping handshakes of data across the network to provide services based on identity, preferences, and personalization technologies. We trust these services to do what we want and to protect the personal information required to make them efficient and delightful.

WE ARE IN THE FIFTH STAGE OF THE INFORMATION AGE



We call this stage the intelligence stage. It is dynamic and both data centric and person centric. It is the stage in which we have transitioned from the information economy to the personal information economy, and from information services to personal information services.

This stage offers great opportunity to produce both innovation and value, but it also produces greater and greater challenges to the notion of privacy and trust. Things are constantly changing at the speed of the imagination; as quickly as ideas are transformed into reality.

This also means that the fundamentals on which we have based our trust in technology and how that technology processes our personal information are changing as well.

These new ways of processing information—especially personal information—require new ways of thinking about the controls and measures to ensure privacy. It is no longer enough to have a hard-coded firewall and lock on the door. We must find ways to realign and retain that trust. There are those who do not think it is excessive to say that the future of the internet, as a place we want to inhabit for play and for business, depends on it being a trustworthy locale, and that much of this trust starts with how our privacy and personal information are managed.

PRIVACY ENGINEERING IS...

Privacy engineering is one of the paths to enabling trust and building technology that protects privacy. It offers a methodology for ensuring that privacy is a forethought and not an afterthought, and for ensuring that the necessary controls are put in place to meet the privacy requirements presented by this new age of computing. We can look to privacy engineering to find ways to preserve privacy and trust as we continually move forward into new worlds that offer new opportunities for using technology to enhance our lives.

Privacy engineering is the "how" of privacy-by-design. It is a combination of discipline, innovation, and information gathering. It encompasses discipline in that it brings to bear the rigor of engineering on the task of embedding privacy requirements into the development and design process; hence, privacy can be factored into the conception of a project rather than bolted on at the end. It is innovation in terms of thinking and striving to find new ways to use data to gain results. And, it is a matter of gathering information so that assessments can be made and controls and measures put in place.

But to get to privacy engineering, we need to talk and think differently.

In engineering, there are functional requirements and nonfunctional requirements (or quality attributes). Functional requirements can be designed and coded to. Nonfunctional requirements or quality attributes cannot be coded or designed to. Privacy as a concept is a nonfunctional requirement or a quality attribute—at least it is when it is explained to engineers or system designers as a subjective legal construct.

THINK OF THE FIPPS AS ACTIONABLE TERMS

Data: What data is involved? Are they sensitive?

Purpose: How and why is the data being processed?

Means of collection: How is the data being gathered?

Notice: Where was notice presented? What was in the notice?

Choice/consent: What kind of choice is the owner of the data given?

Transfer: Is it possible to transfer the data to third parties or another system?

Access, correction, deletion: How can data be corrected or removed?

Security: How is the data being kept from unauthorized access?

Minimization: Is the data collected the minimum necessary to achieve the intended purpose?

Proportionality: Is the processing of the data proportional to the need, purpose, and sensitivity of the data?

Retention: Is the deletion strategy defined and enforced within the system or the enterprise? If so, how?

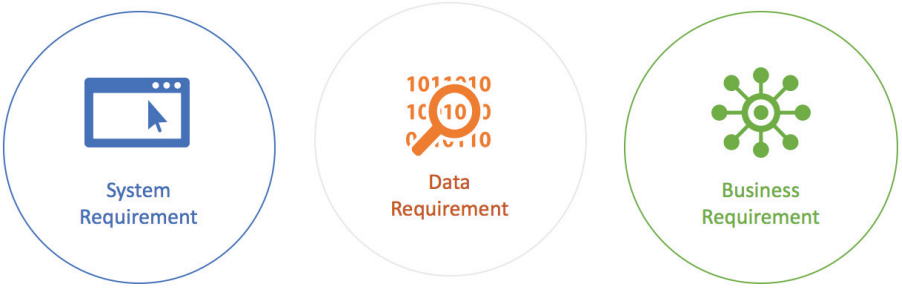
Third parties: If third parties are involved, what is the relationship?

Accountability: Are responsibilities defined and the internal enforcement mechanisms in place? What are they? Who "owns" the program? How is it managed?

To engineer for privacy, it needs to be broken down into components that can be evaluated, architected, designed, and coded to. It needs to be framed as requirements for personal information, such as the purposes it is used for, how it is being collected, how notice is presented, how are choice and consent (if necessary) enabled, how transfers are managed, and so on, including mechanisms for access and correction, processes for deletion, measures for security;, decisions on minimization, proportionality, retention, use by third parties, and accountability.

Privacy also needs to be thought of not merely as a system or product requirement, but also as a business requirement and a data requirement.

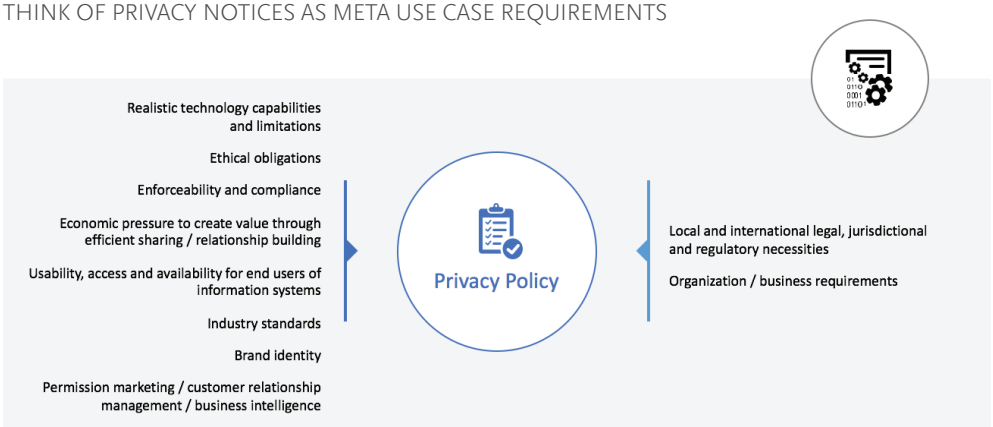
A REQUIREMANT OF WHAT?



It must be thought of as a data requirement since privacy requirements travel with the data and privacy involves the whole data lifecycle, which usually extends beyond the immediate system of the product that processes it.

It must be thought of as a business requirement since privacy does not stop at the edges of a system, but involves an entire enterprise and the larger ecosystem that produces the applications, programs, or whatever it is that is processing the personal information involved.

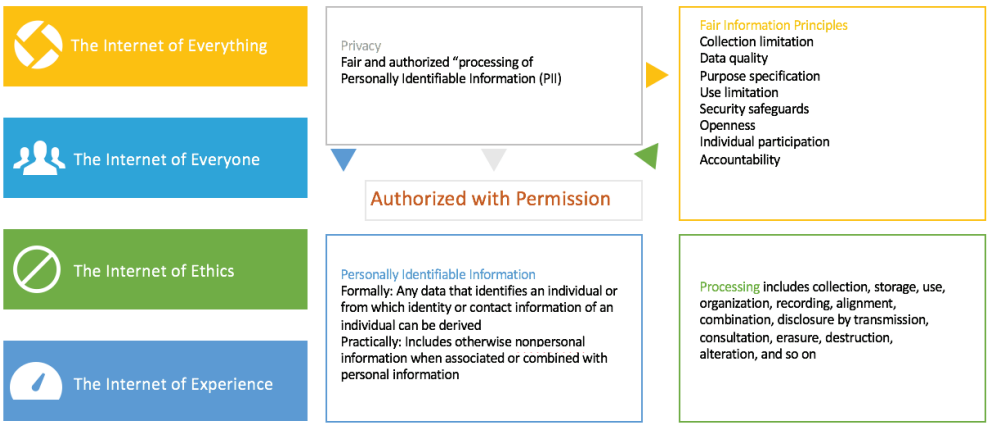
THINK OF PRIVACY NOTICES AS META USE CASE REQUIREMENTS



As part of privacy engineering, we need to think about privacy policies and notices differently. Privacy policies and notices are really meta-use case documents for how an enterprise processes personal information and ensures the privacy of those whose personal information is entrusted to the products, systems, and applications produced by the enterprise. Unfortunately, while written for many different audiences (regulators, customers, and employees among others), privacy policies and notices are not written for engineers.

To earn and maintain trust and privacy as we move forward and mature in the age of intelligence, we also need to think in terms of not merely the internet of things, but the IoE (Everything, Everyone, Ethics, and Experience), since the connected world is not just about "connecting" things.

IOT AND PRIVACY – SHOULD WE REFRAME AS IOE?



The internet of everything looks at the internet of things as objects or internet-enabled things.

This includes factory sensors, global positioning systems, wearable devices (Google Glass, Fitbit, etc.), and "smart" technology that tells you when it's time to order food or when it's time for a medical checkup.

The internet of experience isn't only about what the technology can do for us, but also what experience we want. Who should control these experiences? Who should regulate them? Are the experiences the same for people of all ages? Must all these billions of micro-experiences be recorded, tracked, saved, and audited?

The internet of ethics challenges us to ask what our ethics are in a world of devices that do not recognize our cultural barriers. But cultural norming varies greatly from household to household. We must have a truly robust, cross-cultural, and cross-generational discussion about the Internet of Ethics that considers many different perspectives. For example, consider the following design question: How do we translate "soft" ethical concepts into tangible and measurable requirements in an IoE environment? Can we?

The internet of everyone is where privacy (as a notion of the authorized processing of personalized identifiable information according to fair legal and moral principles) lives. If the internet of everything and the data associated with it offer a quantitative distinction, the internet of everyone presents a qualitative difference.

So, remember this—the IoT is the IoE—the internet of everything, everyone, ethics, and experience.

To achieve and maintain trust in this age of intelligence and the IoT (which really is the IoE), it takes a village. Privacy engineering is as much about engineering a product or system as it is about engineering an enterprise. It takes focused leadership, budget, executive buy-in, and finesse. It requires accurately mapping out an organization's current situation, understanding how well the organization is currently implementing the necessary controls and measures to mitigate risk or to create opportunity, and then not only defining and documenting the existing situation, but also continuously identifying remedies when unacceptable risks and opportunities for innovation are discovered. Ultimately, it takes organizational fortitude, perseverance, and alignment.

All that said, this is not new. Innovation and technology have long given rise to challenges on how we manage privacy, and throughout time there has been a need to find new paths for doing so.

It is no accident that Warren and Brandeis's 1890 law review article the "Right to Privacy", which was the first articulation of privacy as a legal right, came shortly after Kodak introduced the equivalent of an instamatic camera, which allowed the common person to capture and record images. This made the possibility of being photographed in unflattering or compromising situations real, and it was substantially different from merely being observed doing something untoward by a random person without means of recording or publicizing the event. Nor is it an accident that as governments began to contemplate the use of large databases to provide services to their citizens in the late 1960s, the Fair Information Practice Principles, the principles that form the basis of all privacy laws worldwide, were developed.

Privacy engineering is the latest in a long line of innovations that have been developed to find ways to protect privacy and trust as technology finds new and different ways of processing personal information. It will also not be the last.

NECESSITIES & POSSIBILITIES OF REGULATION

PROF. DR. ROLF H. WEBER, UZH ZURICH

Thesis 1 | As an emerging and gradually developing global internet-based information architecture facilitating the exchange of goods and services, the internet of things (IoT) requires at least a general normative framework.

Thesis 2 | An adequate political understanding of legitimacy makes it necessary to implement instruments that try to achieve equal bargaining powers and adequate proceedings allowing for the representation of all stakeholders.

Thesis 3 | A normative framework should be designed such that the rules are fair and firmly rooted in a structure that enables all stakeholders to communicate, coordinate, and cooperate in a kind of forum.

Thesis 4 | Transparency, which also represents an element of ethics and trust, must be established in relation to the elaboration of rules, the decision-making processes, and the formal procedures.

Thesis 5 | The accountability of all involved stakeholders should be based on standards that hold the acting bodies accountable, on information being more readily made available to accountability holders, and on the imposition of some sort of sanction attaching costs to the failure to meet standards.

Thesis 6 | IoT infrastructure governance must encompass the following criteria: robustness of the technology and the business, availability of infrastructure, reliability of IoT functions, interoperability (connectivity) of networks, and right of access to the infrastructure.

Thesis 7 | Ethical features merit more attention, particularly trust (exceeding the traditional notions of reliance and confidence), social justice, autonomy (i.e., informed consent), the social contract concept, the blurring of contexts (private vs. public) and the non-neutrality of IoT metaphors.

Thesis 8 | It is very unlikely that an international regulator creating a normative framework for the IoT will be established (even if the International Telecommunication Union has become active), and such a regulator might not even be suitable in view of the rapid technological changes requiring a fast-moving standard-setting body.

Thesis 9 | The European Commission was the first supranational body to try to work out an IoT governance framework, but there was a loss of momentum at a relatively early stage. The United States (Federal Trade Commission) and countries in East Asia (China, Japan) are actively seeking to develop a regulatory framework.

Thesis 10 | As in the case of the traditional internet, nongovernmental organizations—mainly standardization associations—appear to be the most appropriate bodies to develop harmonized principles that are acceptable around the globe in order to achieve a suitable degree of legal interoperability.

Thesis 11 | Privacy issues have been and will likely remain the most critical aspect of the growing IoT and will require the development of new designs for protection.

Thesis 12 | Traditional confidentiality must be further developed into a more advanced anonymity concept relying on cryptographic solutions in order to achieve properties like unlinkability, undetectability, and unobservability.

Thesis 13 | Privacy should not only be protected by law but also by technology, for instance by privacy-enhancing technologies, privacy-by-design concepts, and data protection management programs.

Thesis 14 | Quality of data is to be ensured by taking the environment in which it is collected into account; quality of context must also play a more important role.

Thesis 15 | New types of privacy infringements will pose a threat if automated devices make it necessary to place a higher level of trust on these devices than on manually entered human data (in the insurance business, for example).

Thesis 16 | The emergence of the IoT has altered the cyber-threat landscape because this phenomenon entails the ever-expanding integration of (generally) poorly secured devices (things) into networks by connecting to the internet and to each other and because the deployment on a massive scale of such inherently vulnerable devices creates exponentially more vectors for attack.

Thesis 17 | The increased level of security risks in view of a wide array of external and internal agents, as well as of threat tools and threat types, calls for a reconsideration of the legal parameters of cybersecurity.

Thesis 18 | Vulnerabilities stem from a lack of transport encryption, insufficient authentication and authorization, insecure web interface, and insecure software and firmware; the risks relate not only to the insufficient control of devices, but also the massive and rapidly growing amounts of stored data generated by smart objects.

Thesis 19 | Despite the fact that it has provided an internationally recognized framework for harmonization and exerts an influence on current EU cybercrime legislation, the Budapest Convention appears to be largely outdated and in great need of reform.

Thesis 20 | The recently adopted Network and Information Security (NIS) Directive is the first EU-wide legislation on cybersecurity with the objective of achieving minimum harmonization in order to make the online environment more trustworthy. NIS security should enable networks and information systems to resist any action that compromises the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data.

Thesis 21 | The main objectives of the NIS Directive are improved national cyber-security capabilities, improved EU-level cooperation, and the introduction of better security and incident notification requirements.

Thesis 22 | The problem with the NIS Directive is that many terms (such as "appropriate and proportionate technical and organizational measures") are subject to interpretation. This is due in part to a weakening of operators' obligations in the legislative process.

Thesis 23 | While regulatory activities such as the NIS Directive will impact the emphasis on security, IoT-specific legislation would hardly be viable.

Thesis 24 | Alternative regulatory approaches that include all stakeholders (multistakeholderism) are needed: Generally accepted rule-making procedures can help to establish increased credibility with regard to the actions that are taken, and consequently help to contribute to a higher level of trust.

COMMERCIALIZING THE IOT THROUGH TRUST?

THE SOCIOECONOMICS OF PUBLIC TRUST IN OPEN COLLABORATIONS & THE IOT

DR. JAN-FELIX SCHRAPE, UNIVERSITY OF STUTTGART

The term "open," used in phrases like "open science," "open innovation," and "open government," has become part of the standard vocabulary in modern society. Today, projects of all kinds flaunt the attribute of openness and its associated promise of more decentralized and democratic organizational or coordination structures.

An important starting point for explaining the popularity of the openness paradigm is the rapidly increasing relevance of open source projects in software development since the turn of the millennium. In the social sciences, accustomed to regarding intellectual property rights as drivers of innovation processes, this increase was initially met with surprise. However, not long thereafter, open source was acknowledged as an emerging production model based on voluntary and self-directed collaboration among equals that could break with well-established forms of socio-economic coordination, such as the market or hierarchy. In that context, the concept of "commons-based peer production" gained traction. Hailed as a technically effective collaboration among large groups of individuals [...] without relying on either market pricing or managerial hierarchies to coordinate their common enterprise" (Benkler & Nissenbaum 2006: 381), the concept was to be accompanied by "systematic advantages [...] in identifying and allocating human capital/creativity" (Benkler 2002: 381) and has been increasingly applied in adjacent fields, such as the production of material goods ("maker economy"), or hardware and the service sector (e.g., Rifkin 2014).

However, observations of open source projects have shown that the growth of developer communities goes hand in hand with the formation of distinct hierarchical decision-making patterns, that leading IT companies are increasingly gaining considerable influence over important projects, and that firmly established projects are not run by intrinsically motivated volunteers who are "satisfying psychological needs, pleasure, and a sense of social belonging" (Benkler 2004: 1110), but are based on the contributions of employed developers. For example, in the Linux kernel project, often referred to as a typical open source project, more than 85 percent of the commits were made by programmers who "are being paid for their work" (Corbet & Kroah-Hartman 2016: 12). In light of this, the oft-made claim that open source communities are radical, subversive alternatives to proprietary development are essentially blanket statements that do not hold. This raises the question of which of these projects might actually live up to the "promises of openness, freedom, and democracy" (Kranich & Schement 2008: 563).

Against this backdrop, I will present a systematic overview of the institutionalization of open source projects in their capacity as an integral part of the global software industry, as well as their socioeconomic contexts and their role in the emerging Internet of Things (see also Schrape 2016):

- I begin with a reconstruction of the genesis of open source as utopia, method, and innovation strategy, followed by the identification of four ideal-type variants of open source projects (Fig. 1).

- Afterwards, I examine why open source projects have largely lost their subversive potential while nonetheless representing a socio-technically stabilized form of collective invention.

- Finally, I discuss the significance of open collaboration for the Internet of Things (IoT), which will, like the existing web, heavily rely upon open source technologies and open standards.

FIGURE 1. IDEAL-TYPE MANIFESTATIONS OF OPEN SOURCE PROJECTS

	Corporate-led collaboration projects e.g., Android, WebKit	**Elite-centered project communities** e.g., Linux Kernel	**Heterarchical infrastructure projects** e.g., Apache HTTP	**Egalitarian-oriented peer production communities** e.g., Arch Linux
Work organization	mainly hierarchical	mainly hierarchical	horizontal – meritocratic	horizontal – egalitarian
Strategic management	Individual companies/ consortium of firms	Project founder/ Project management	Board of directors of the foundation/ Steering group	Streering committee/ core team
Funding	Participating firms	Corporate donations/ smaller private donations	Primarily contributions from companies	Primarily smaller private donations
Participant pool	Staff from the participating companies	Employed and (few) voluntary developers	Employed developers, company representatives	Primarily voluntary developers

Concerning the internet of things, scalable and customizable open source infrastructures, to be used across multiple architectures, could get rid of many of the current constraints that have limited the IoT's mainstream appeal (Weinberg 2015). Yet at the same time, even though open source software is generally deemed more secure, as anyone can inspect the code, the case of the encryption software OpenSSL points to the potential risks of the open source model and shows that this degree of trust in open collaboration is not justified in all cases.

Until 2014, OpenSSL, which is used in many software systems and platforms, was essentially developed by one full-time programer assisted by a small, voluntary core team and received little financial support from the industry—although nearly all sophisticated software architectures rely on the OpenSSL library. In that context, new features were constantly integrated into OpenSSL, yet the level of maintenance work was not bolstered accordingly. In 2012, this culminated in an oversight that led to the major "Heartbleed" vulnerability, which was not discovered until 2014 (Stokel-Walker 2014).

Therefore, much can be learned from the socioeconomics of "classical" open source projects about the institutionalization of industry-wide modes of open collaboration in the context of the emerging IoT. In the last two decades, open source projects have contributed to more flexible cooperations between developers from divergent contexts, to project-specific cooperation between market participants (who may be in direct competition otherwise), as well as to internal organizational production modi—all of which has made the software market as a whole more permeable. At the same time, however, open source code per se will not necessarily result in more transparent coordination patterns or more reliability than in other working contexts, in a disintermediation in the established modes of economic resource distribution, or an overall democratization of innovation processes. Nonetheless, a continued corporate adoption of open source could give rise to a higher public acceptance or trust in smart devices, automatization, big data, and the IoT in general (Dickel & Schrape 2016).

REFERENCES

Benkler, Y. (2002): Coase's Penguin, or, Linux and ‚The Nature of the Firm. In: Yale Law Journal 112, 369–446.

Benkler, Y. (2004): Intellectual Property: Commons-based Strategies and the Problems of Patents. In: Science 305(5687), 1110–1011.

Benkler, Y./Nissenbaum, H. (2006): Commons-based Peer Production and Virtue. In: Journal of Political Philosophy 14(4), 394–419.

Corbet, J., & Kroah-Hartman, G. (2016). Linux Kernel Development Report. San Francisco: The Linux Foundation.

Dickel, S./Schrape, J.-F. (2016): Materializing Digital Futures. In: Ferdinand, Jan-Peter et al. (Eds.): The Decentralized and Networked Future of Value Creation. Dordrecht: Springer, 163–178.

Kranich, N./Schement, J.R. (2008): Information Commons. In: Annual Review of Information Science and Technology 42(1), 546–591.

Rifkin, J. (2014): The Zero Marginal Cost Society. New York: Palgrave Macmillan.

Schrape, J.-F. 2016: Open-Source-Projekte: vom Nischenphänomen zum integralen Bestandteil der Softwareindustrie. In: WSI-Mitteilungen 8/2016, 603–612.

Weinberg, B. (2015): The Internet of Things and Open Source. In: Podnar Žarko, I., Pripužic K., Serrano M. (Eds): Interoperability and Open-Source Solutions for the Internet of Things. Lecture Notes in Computer Science 9001. Cham: Springer, 1–5.

LIMITS OF INTERFIRM COLLABORATION & TRUST IN SMART FACTORY SYSTEMS

DR. ROBIN TECH, KONSTANZE NEUMANN, WENDELIN MICHEL, HIIG

IT'S DIFFICULT TO TRUST A SMART FACTORY SYSTEM

Smart factories represent a culmination of various technologically advanced systems that revolve the internet of things (IoT). The IoT embraces the notion of interconnected things, thus going beyond the interconnectedness of computers. In an industrial setting, the level of digitization surpasses the levels of so-called cyber-physical systems architectures, as it encapsulates not just machines but virtually all objects that are relevant for a factory to work properly. The industrial IoT (IIoT) is therefore an extension of factory digitization that seeks to interconnect geographically dispersed machines and to endow these systems with the intelligence to solve problems (Gilchrist, 2016). The autonomy to make decisions independently of human intervention is at the center of the notion of smart factories.

In this brief work-in-progress paper, we examine the intricacies of interfirm collaboration in smart factory environments, i.e., we identify what stands in the way of a firm's collaboration with external partners when operating a smart factory. This seems quite necessary, because the promise of greatly enhanced processes and lower costs stands in contrast with the fundamental challenges that arise from the complexity of these systems. To investigate the settings necessary to fully implement a smart factory concept—i.e., a close-knit network of collaborating partners—we turned to new institutional economics. More precisely, the two bedrock concepts of information asymmetries and transaction costs assist us in the characterization of (a) the general setting of the actor networks and (b) their relationships with each other. This characterization of the relationships between various smart factory actors is also what the debate on the IIoT still lacks. It is crucially important to identify the sources of complexity that lead to information asymmetries, which ultimately increase the uncertainty of partners that necessarily have to collaborate in order to establish a functioning smart factory system.

The questions that guide our investigation therefore read: (a) Who are the relevant stakeholders and collaboration partners in smart factory environments?; (b) What are the uncertainty factors that make the implementation of a smart factory system less likely?; and (c) What trust-building mechanisms can reduce collaboration uncertainties?

CONTROL, COMPLEXITY, AND COLLABORATION

To appropriately describe and identify factors that affect interfirm collaboration, we first examine the mechanisms that govern control over these factors. From a focal firm's perspective, this is best described through the notion of locus of control (Wijbenga & van Witteloostuijn, 2007; Korunka et al., 2003; Boone et al., 1996). The locus-of-control paradigm allows us to map a focal actor's level of influence over a certain factor, i.e., his or her ability to manipulate specific characteristics.

In a smart factory environment, the key characteristic is complexity. The overall system's complexity has multiple dimensions that can roughly be divided into product complexity (e.g., Novak & Eppinger, 2001; Hobday, 1998), internal complexity (e.g., Hobday, 1998), and external complexity (e.g., Grover & Said, 2007; Goodhart, 1998).

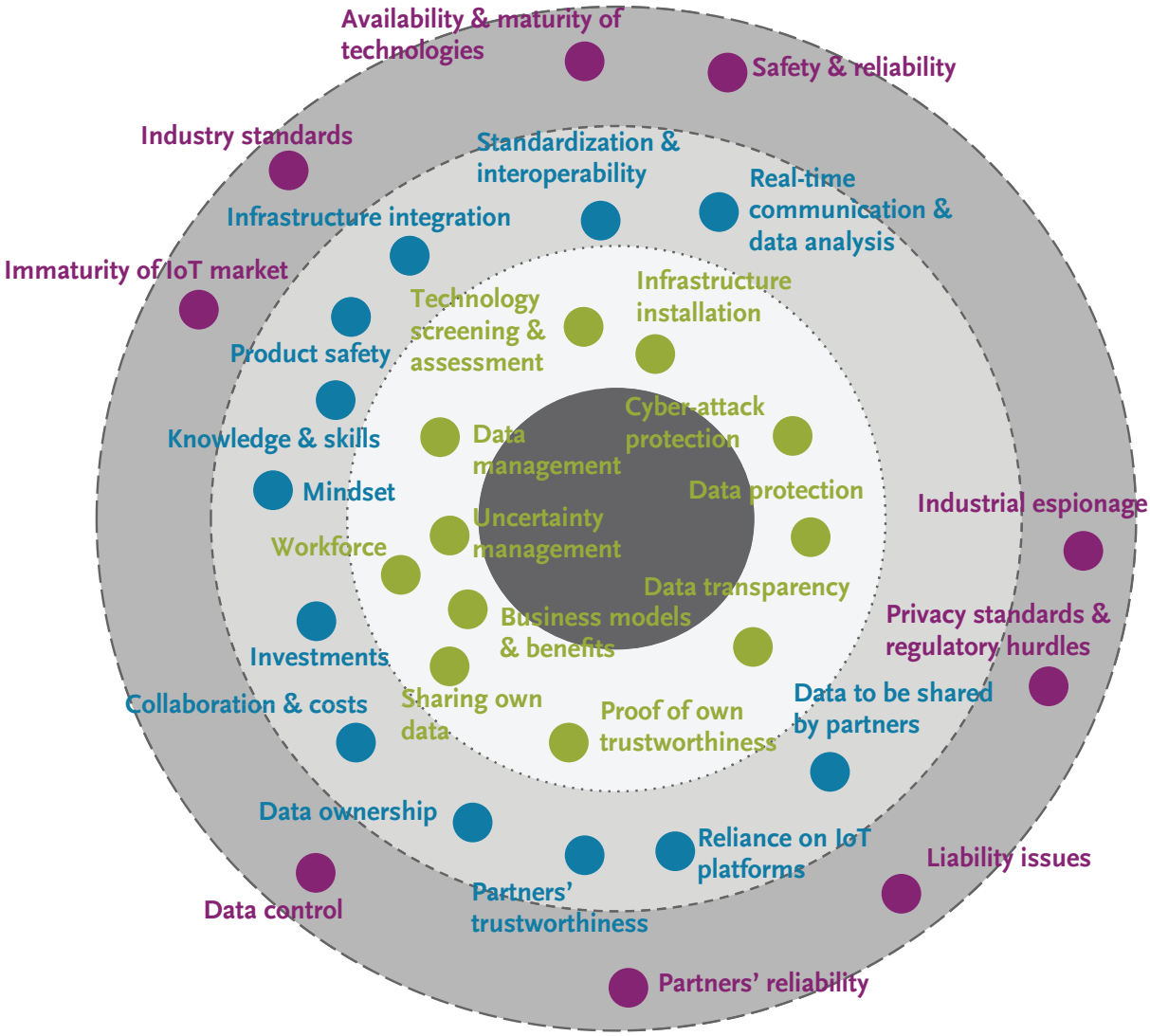
The collaboration between smart factory actors is indirectly governed by the level of complexity, as it affects information asymmetries (Leland & Pyle, 1977) that ultimately increase transaction costs (Williamson, 2000; Furubotn & Richter, 1998). If transaction costs offset—or if it is feared that they will offset—potential gains from implementing a smart factory, the system will likely not be introduced. It is thus imperative to prepare and manage a collaborative network of actors with the goal of reducing transaction costs.

METHOD

Building on the theoretical framing, we conduct desk research on smart factory actors and complexity factors. This included publications by smart factory firms and suppliers of IIoT technologies, such as Predix by GE or Mindsphere by Siemens—two major industry equipment and service providers. By examining their value propositions and system architectures, we were able to identify a preliminary set of archetypical smart factory actors and complexity factors. Building on these sets, we designed a workshop setting that allowed for five different expert panels. Each panel was comprised of up to nine experts, ranging from cyber-physical systems and IT infrastructure researchers to executive-level managers and engineers from companies such as Deutsche Telekom, Zeiss, and Cisco Systems. These experts were directly involved in the implementation of IIoT systems, or at least expressed an interest in setting up smart factory systems in future. They extended the list of complexity factors and further substantiated the actor network setups. As a next step, in-depth expert interviews are planned. This will involve semi-structured one-on-one interviews with decision makers who are directly in charge of opting for or against the implementation of smart factory systems in their company. These interviews will, so we hope, add another level of inquiry to our study and validate the preliminary findings from the panels. They will also seek to shed light on practical mitigation strategies to reduce uncertainty and build trust between actors.

PRELIMINARY FINDINGS

We found a total of 32 complexity factors that are relevant to actor networks in a smart factory system. These factors were mapped on a locus-of-control framework to display the ability to manipulate the factors from a focal firm's perspective. Figure 01 depicts factors that are directly related to inherent characteristics of the product—e.g., real-time communication and data analysis. It also shows firm-internal complexities—e.g., business model considerations and mindsets—and external factors such as standardization and industrial espionage.


Availability & maturity of technologies
Safety & reliability
Industry standards
Standardization & interoperability
Real-time communication & data analysis
Infrastructure integration
Immaturity of IoT market
Infrastructure installation
Technology screening & assessment
Product safety
Cyber-attack protection
Knowledge & skills
Data management
Data protection
Mindset
Industrial espionage
Uncertainty management
Workforce
Data transparency
Privacy standards & regulatory hurdles
Business models & benefits
Investments
Data to be shared by partners
Collaboration & costs
Sharing own data
Proof of own trustworthiness
Data ownership
Reliance on IoT platforms
Liability issues
Partners' trustworthiness
Data control
Partners' reliability

REFERENCES

Boone, C., Brabander, B., & Witteloostuijn, A. (1996). CEO locus of control and small firm performance: An integrative framework and empirical test. *Journal of Management Studies,* 33(5), 667-700.

Furubotn, E. G., & Richter, R. (1998). Institutions and economic theory: The contribution of the New Institutional Economics. Ann Arbor: University of Michigan Press.

Gilchrist, A. (2016). Introducing Industry 4.0. In *Industry 4.0* (pp. 195-215). Apress.

Goodhart, C. A. E. (1998). Financial regulation: Why, how, and where now?. New York, NY: Routledge.

Grover, V., & Saeed, K. A. (2007). The impact of product, market, and relationship characteristics on interorganizational system integration in manufacturer-supplier dyads. *Journal of Management Information Systems,* 23(4), 185-216.

Hobday, M. (1998). Product complexity, innovation and industrial organisation. Research Policy, 26(6), 689-710.

Korunka, C., Frank, H., Lueger, M., & Mugler, J. (2003). The entrepreneurial personality in the context of resources, environment, and the startup process—A configurational approach. *Entrepreneurship Theory and Practice,* 28(1), 23-42.

Leland, H. E., & Pyle D. H. (1977). Informational Asymmetries, Financial Structure, and Financial Intermediation. *Journal of Finance,* 32(2), 371–387.

Novak, S., & Eppinger, S. D. (2001). Sourcing by design: Product complexity and the supply chain. Management science, 47(1), 189-204.

Wijbenga, F. H., & van Witteloostuijn, A. (2007). Entrepreneurial locus of control and competitive strategies — The moderating effect of environmental dynamism. Jour*nal of Economic Psychology,* 28(5), 566-589.

Williamson, O. E. (2000). The new institutional economics: taking stock, looking ahead. *Journal of Economic Literature,* 38(5), 595-613.

STANDARDISATION & REGULATION AS TRUST-BUILDING MECHANISMS FOR THE IOT

PROF. DR. KNUT BLIND, TU BERLIN & FRAUNHOFER FOKUS &
CRISPIN NIEBEL, TU BERLIN

The Internet of Things (IoT) has become an oft-debated topic in recent years. Technological advances have made the emergence of such an integrated digital ecosystem all the more foreseeable in the near future. However, despite the arrival on the market of devices that one could describe as belonging to the world of IoT, they are fragmented, limited in their use, and have not fully permeated every aspect of our lives as they should do in order to work optimally.

Naturally, there are still technological limitations and issues of compatibility. As time progresses, more sophisticated technological developments will arise. However, the practical feasibility of the IoT is still problematic, and most importantly, it will all be to no end if the world does not play along. This is where the notion of trust comes in. In order for the IoT to work to its full potential, it requires absolute integration and acceptance, as this is inherent to its pervasive and cross-device functionality. Yet the IoT is different from many previous digital developments. At times referred to as Industry 4.0 in Europe, the IoT represents an entirely different paradigm of life (see Trappey et al. 2016). With such a powerful web of interconnectedness, security and privacy concerns rise to unprecedented levels (Li et al. 2016, Sicari et al. 2015, Weber 2010). This lack of trust has been exacerbated by news of the hacking or theft of online information, the exponential increase in the gathering and storage of private information, and a lack of transparency, as well as by the fact that large portions of the population are overwhelmed by the digital environment.

In order to tackle these issues of trust related to the IoT, a useful approach would be to establish trust-building institutions. Here, different approaches are possible. In general, public institutions can establish top-down regulations. However, self- or co-regulatory approaches driven by the stakeholders themselves are also possible, for instance, through standardization (see Bartolini et al. 2016). Indeed, regardless of issues of trust, standards will play a central role in the IoT in terms of practical functionality and interoperability. Only with a common technical infrastructure laid out through standards will the devices be able to interact and communicate with one another. Furthermore, regarding monetary concerns, such a standard would make the most sense if implemented at the international level (allowing for exports and global value chains). Thus, as standards are an essential component of the IoT, it would be beneficial to incorporate security and privacy-related features into the needed interoperability standards or to develop additional security and privacy standards. Such standards would follow the WTO criteria and should be transparent in nature. As a result, they would

be accessible to consumers and build trust in IoT-based products. Furthermore, not only individual consumers, but also organizations or companies have a vested interest in strong security and privacy mechanisms to protect confidential information such as trade secrets. Hence, all stakeholders would have an interest in such standards.

Issues naturally arise when creating standards for such a heterogeneous environment, and the IoT might require multiple standards. However, it would be efficient to have a limited amount of standards, or at least compatible standards and parallel underlying mechanisms, in order for privacy and security aspects to be as uniformly applicable as possible. This would limit discrepancies and possibilities for malicious attacks targeting gaps and inconsistencies.

REFERENCES

Bartolini C., Lenzini, G, Robaldo, L. (2016), 'Towards legal compliance by correlating Standards and Laws with a semi-automated methodology', *28th Benelux conference on Artificial Intelligence (BNAIC)*.

Crabtree, A. ,Mortier, R. , (2016) 'Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control', Available at SSRN: https://ssrn.com/abstract=2874312.

Li, S., Tryfonas T., Li, H., (2016) 'The Internet of Things: a security point of view', *Internet Research, Vol. 26 Iss 2, pp. 337-359*.

Sicari, S., Rizzardi A., Grieco L.A., Coen-Porisini A. (2015), 'Security, privacy and trust in Internet of Things: The road ahead', *Computer Networks, Vol. 76, pp. 146-164*.

Trappey A.J.C., Trappey, C.V., Govindarajan U.H., Chuang A.C, Sun J.J. (2016), 'A review of essential standards and patent landscapes for the Internet of Things: A key enabler fort Industry 4.0', *Advanced Engineering Informatics*.

Weber R.H. (2010), 'Internet of Things- New security and privacy challenges', *Computer Law and Security Review (pp.23-30)*.

Yan. Z., Zhang P., Vasilakos A.V. (2014), 'A survey of trust management for Internet of Things', *Journal of Network and Computer Applications 42, pp. 120-134*.

IN LAW WE TRUST —
IN IOT WE TRUST?

TRUST & TECHNOLOGY: A MULTILEVEL PERSPECTIVE

PD DR. ARIANE BERGER, FU BERLIN & DEUTSCHER LANDKREISTAG

1 | INTRODUCTION

Trust is a human emotion. The concept of trust describes the expectation not to be disadvantaged by the action of the other. In relation to the government, the citizens rely on a government functioning properly. This means, first of all, that decisions are reached in a lawful and appropriate manner. Whether trust is created between two people depends on factors that are routed in the counterpart and on whether these factors are reflected in communication between these two people. The citizens establish trust in a functioning administration by observing a competent expert acting in the respective area of his responsibility, the so-called Amtswalter. Additional factors - surrounding factors - creating trust are such as an effective organisation and rational decision-making procedures.

The digitisation of the administration impacts these trust-building factors. The importance of a human being deciding on certain administrative questions will diminish in the course of increasing digitisation and the expansion of e-government. The "digitally dressed" government confronts the citizen differently than "a traditional, old-school administration". The human expert in administration, the Amtswalter, fades into the background. Trust in the correctness of human decision turns into a trust in the correctness of the technically generated decision. This will necessarily change the foundations of trust between citizens and their government. The less an administration can be observed and experienced in real world, the less can the human expert in an administration contribute to trust. The factors for ensuring trust must therefore be supplemented. It is here, where the (federal and state) legislator is called upon to react to these developments.

In the course of this presentation we will, first, examine whether and to what extent the German Constitution has incorporated the notion of trust. This may put us in the position, second, to answer the question of how the legislature has to react to the developments in the relationship of trust between citizens and their government caused by digitisation.

In a next step, third, recent administrative developments in the field of digitisation will be outlined briefly. The focus here is on the introduction of the electronic file management (so called E-Akte), the issuance of partial and fully automated administrative acts as well as the envisaged creation of a nation-wide digital information gateway (so called Portalverbund). We will do so with a view to reveal those areas and the respective conditions where the "human factor" may be replaced or supplemented by algorithms. We will also identify the areas where the "human factor" remains indispensable. Finally, challenges and opportunities for the emergence of a new, digital trust shall be sketched.

2 | THE GERMAN CONSTITUTION AND TRUST

In German constitutional law there is no uniform, generally recognised system of trust. However, both the fundamental rights and freedoms and the basic principles of state structure contain various trust-building factors, which are to be presented here - at least briefly.

2.1 | FUNDAMENTAL RIGHTS AND FREEDOMS

The fundamental rights of the German Grundgesetz take particular account of the aspect of confidentiality as a special element of trust. At this point, reference is made to the general right of personality of Art. 2 (1) i.c.w. Art. 1 para. 1 Grundgesetz, which was further developed by the Federal Constitutional Court into a digital fundamental right. Subsequently, the general right of personality covers the right to ensure the confidentiality and integrity of information technology systems.

On the legal front, it is discussed whether a fundamental right of data protection should be included in the German Constitution. The constitutions of some of the individual Länder contain, in part, very detailed supplementary rights, for example a right to the creation and participation in digital basic services and the protection of the digital privacy. The developments in the field of Big Data also challenge science and practice to explore the freedom of fundamental rights and to develop a digital freedom code. Confidentiality, data protection and IT security are important trust-building factors. However, they describe only one aspect of the trust relationship between the citizens and their government.

If, in the context of fundamental rights, further reference is made to the importance of the "human factor", a link to the guarantee of human dignity in Article 1 of the Grundgesetz may be associated. In its jurisprudence on Article 1, the Federal Constitutional Court assumes that the person "should not be made an object". This is a first indication that administrative decisions, which are produced purely technically, do not at all suit human beings. For this reason, the fully automated government machine must be regarded as inhuman. This raises the question whether and to what extent the basic principles of state structure also emphasize the human factor.

2.2 | BASIC PRINCIPLES OF STATE STRUCTURE

Here, the rule of law and the principle of democracy are also considered. Both principles contain a requirement of accountability. It urges the legislature that digitisation should not lead to intransparent administration and misrepresentation of competences. To this extent, the basic principles of state structure ensure the trust-building environment, without, however, regulating the human factor itself.

A further constitutional principle of the administrative organisation is the so-called Amtsprinzip. The Amt is the smallest organisational decision-making unit, which is tailored to the task of exactly one person. This structural principle contains not only the commitment

to small-scale and labor-based administrative decisions. The purpose of the Amtsprinzip is to measure tasks so that they can be perceived by exactly one person, the Amtswalter. This person gives the administration a human face. From this point of view the human expert in administration is the central trust anchor.

2.3 | CONCLUSIONS SO FAR

By means of the Amtsprinzip, the constitution provides the hinge between the governmental organisation and the sphere of the human being. The constitution thus points out that state decisions are humanly mediated decisions. The human factor is therefore not quantité négliable. The (federal and state) legislator has to take this into consideration sufficiently in the design of eGovernment. The more the responsible Amtswalter falls into the background, the greater the demands on the trust-building environment, especially on the aspects of accountability and confidentiality. Whether the legislator has succeeded in expanding this compensatory relationship is to be examined in the following.

3 | TRUST AND EGOVERNMENT

The current administrative reforms, the eGovernment, affect all sections of the decision-making process. They start at the moment of application, extend to the entire administrative procedure up to the final decision. The aim of the law is to ensure a work without any media brakes.

3.1 | DIGITAL GATEWAY (PORTALVERBUND)

The draft of a new so-called Onlinezugangsgesetz provides for a Federal Digital Gateway (Portalverbund), which is intended to serve the citizen as a first access to the administration and then forward the citizen to the responsible administrative authority. Such a digital gateway is not a new invention. There are already various administrative gateways. The Behördenruf 115, the points of single contact (Einheitlicher Ansprechpartner) as well as various so-called Behördenfinder should be mentioned. These gateways are now to be merged into a single federal gateway.

The introduction of this federal gateway changes the familiar communication relationship between citizens and government and is therefore also relevant for trust building. There is a risk that citizens will no longer be able to clearly identify the responsible authority. This de-territorialisation of government therefore presents dangers for the organisational clarity of accountability required by constitutional law. This also has an impact on legal protection: Legal protection is ensured through the fact that the responsibility of the government`s administration is transparent. There is no trust without accountability.

3.2 | ELECTRONIC FILE MANAGEMENT (E-AKTE)

Another reform project is electronic file management, the so-called E-Akte. By 2020, the authorities of the Federation and the Länder are to keep their files electronically. The organisational benefit of the e-file is to ensure work without any media brakes. This, in turn, can increase the traceability of the administrative decisions, and in particular the legal documentation of

decision-making processes. A work without any media brakes can bring efficiency advantages. Also, the automation of procedures may promote the feeling of neutrality and objectivity of administrative decisions. The introduction of the e-file can therefore lead to a gain in trust.

However, the work without any media brakes leads to a loss of the human factor in the communication between citizens and the government. The surrounding trust-building factors are therefore of particular importance.

3.3 | AUTOMATED ADMINISTRATIVE ACT

A further step of the eGovernment-reforms is the section 35a of the Administrative Procedures Act (VwVfG), which came into force on 1 January 2017. According to this section and under certain conditions, an administrative act may be issued automatically. This way the route has been opened for fully technical administrative decisions.

The conditions under which an automated administrative act is permissible are by no means as clear as it appears at first sight. However, the legislator would like to express the following: The more legal assessments are required by the application of law, the less a person can be replaced by a subsumption machine. Almost everyone would agree with it. However, the assumption can be made that intelligent algorithms - at least in the near future - can also represent legal assessments. This is to be set at this point. The question is whether these reforms are sufficient to compensate for the loss of human contacts.

3.4 | CONCLUSIONS SO FAR

Further trust-building factors are outlined here, however briefly. The more a person resigns as a decision-maker, the stronger the weight of the supervisory body. Regulatory control procedures gain weight. The administrative process reforms of the so-called Widerspruchsverfahren led to a significant depreciation of the self- control procedures. This must be rethought in view of digitisation and eGovernment. Furthermore, digital trust requires authentication, data protection and IT security. The administrative procedural law regulates the question of authentication so far only to some extent. Here, signature and authentication systems have to be developed. The legislature has so far failed to achieve a uniform regulation.

4 | CONCLUSIONS AND OUTLOOK

The citizens rely on a government functioning properly. The citizens establish trust in a functioning administration by observing a responsible expert. The more the human factor withdraws as a result of increasing automation, the greater the weight of the trust-building environment. The legislators are required by the Constitution to respect the need for accountability in the design of eGovernment. Further trust-building factors are effective administrative self-control as well as authentication, data protection and IT security. The current administrative reforms show that there is a legislative need to catch up on those areas. However, recent reforms also show that digitisation can strengthen administrative functions and increase digital trust.

TRUST & SMART GOVERNMENT

PROF. DR. MEINHARD SCHRÖDER, UNIVERSITY OF PASSAU

1 | Prima facie, trust is not a concept readily found in our constitution. To the contrary, the Basic Law can be read as a document of distrust against the unlimited power of the state. In the tradition of Locke and Montesquieu, the separation of powers, fundamental rights, and judicial review are core elements of our constitution.

2 | However, the Federal Constitutional Court frequently speaks of trust when interpreting the constitution, e.g.:

- Trust may be "worthy of protection" under the rule of law when people have "trusted in the statutory regulation and having made plans based on this trust";
- Member states of the European Union "deserve particular trust" regarding "compliance with the principles of the rule of law and human rights protection"; they benefit from a "principle of mutual trust";
- The "possibility of examining the essential steps of the election promotes justified trust in the regularity of the election".

3 | As the last quote implies, citizens' trust is important for a state. Indeed, trust can be seen as one of the prerequisites the state lives by, and not only something that applies in elections. Obviously, the Federal Constitutional Court considers trust to be something that may be influenced by law – "healthy distrust" has to be dealt with by establishing appropriate legal safeguards.

4 | Citizens' trust in public administration and government cannot be created by law alone. Trust implies subjective expectations with regard to a certain issue, e.g. good administration, and is influenced by a variety of parameters, including the evaluation of the trustee's prior performance.

5 | "Smart government" is an umbrella term for the involvement of information technology in public administration and government. It encompasses a diverse range of things, many of which already exist, such as electronic forms, company registers or court files, the vast use of sensors (e.g. in "intelligently connected" buildings and roads), or the use of intelligent or virtual glasses or electronic tags. So, like "government 4.0", the term "smart government" refers a vision rather than a concrete project.

6 | Not all forms of smart government require new laws. Existing laws may be "technology-neutral" and allow the implementation of smart technologies; in other cases there may be a sufficient legal basis for other technologies in the authorities' discretion to design an administrative procedure.

7 | In spite of the variety of phenomena called "smart government", three connections with the idea of trust seem obvious:

- First, citizens give their trust to a government in elections. When smart government implies that decisions are taken autonomously by machines on the basis of algorithms, this is likely to raise questions of whether there is sufficient democratic legitimation.

- Second, emphasising the necessity of legal safeguards, any form of smart government must be designed to honour justified trust in the protection of fundamental rights and the laws protecting them. The constitutional framework of fundamental rights, which has to be respected by all public authorities, notably contains the right to informational self-determination and the right to the confidentiality and integrity of information technology systems. Therefore, smart government solutions are easier to implement in areas where no personal data are being processed.

- Third, recalling the subjective element of trust, any form of smart government must be measured by its success, i.e. its contribution to fulfilling administrative tasks. The evaluation of the use of a modern technology is based on (subjective) criteria such as the efficiency or citizen-friendliness of administration.

8 | The legal framework as the source of trust and the success of smart government are interrelated in several ways:

- Interferences with fundamental rights may be justified by the (envisaged) better fulfilment of administrative tasks.

- The legal framework sometimes leads to solutions that are trustworthy but unsuccessful, as several attempts to promote electronic communication between state and citizen show.

9 | Transparency is considered one of the best ways to create trust. In the field of smart government, transparency encounters several obstacles:

- Most citizens are not IT experts, and are either not interested or not able to technically understand how smart government works.

- Some, if not many, smart government solutions are not created by public authorities themselves, but by private companies which may enjoy legal protection of their intellectual property and business secrets. Some may consider these companies less trustworthy than the state.

10 | There are too many forms of smart government to judge either their constitutionality or their trustworthiness as a whole. To prove itself worthy of trust in good administration, a smart government will neither ignore the chances of innovative technology nor raise expectations without being able to fulfil them.

SPECIAL CIRCUMSTANCES FOR IOT & TRUST IN THE HEALTH SECTOR

JULIAN HÖLZEL, HIIG

1 | INTERNET OF THINGS APPLICATIONS FOR HEALTH

For some time now, promises around the so-called internet of things have also entered the health sector (Islam et al. 2015). We can see a multitude of new "services," "apps," and "devices" gaining traction in both the personal and public health care sectors. A number of "smartwatches," "fitness trackers," and similar devices are competing on the market, offering to monitor heart rate, blood glucose, movement, or other data about individuals' bodily functions. This can be uploaded to "clouds" for the personal evaluation of one's health status or to share latest achievements in running distances or similar with "friends" or the public.

However, more serious applications are also being developed through so-called "smart devices". These devices are usually characterized by a set of general properties which enable the "smartness" of the device. The most common feature is the sensory interface, through which the devices may observe and record a specific part of their environment in order to create an ever-updated, thus dynamic, model of the real world. This model then enables the device to draw conclusions, which may lead to actions, accomplished by a second interface, the actuator. However, conclusions about the state of the world and subsequent decisions are complex processes that oftentimes collide with the limited local resources of the device. Usually, these shortcomings can be overcome by integrating the device within a network that enables remote access to a set of more powerful and diverse resources, such as storage, computing power,or even human expertise. Local small-scale models may be transferred to or integrated in remote and more complex models, which allow for more complex decisions.

Recently, the interested public learned of a "smart device"—a pacemaker—that had been delivered with a base station. This base station could be installed in the patient's home and served as a communication gateway of the implanted pacemaker to the internet. This enabled the pacemaker to send data about the individual's heartbeat, along with other information detected via sensors, to a personal physician. The rationale was to minimize in-office visits, which would otherwise be necessary. On 9 January 2017, the FDA issued a safety communication concerning this system. Due to certain vulnerabilities in the base station, an attacker would be able to issue arbitrary commands to the implanted pacemaker device, such as inappropriate electrical shocks to the patient's heart.

2 | TRUST: ENABLING ACTION

Before we dive into specific trust issues of IoT applications in public health, a quick glance at the general notion of trust is advisable. As a study by Rousseau et al. informs us, there are a few traits ascribed to the notion of trust within all disciplines. Trust, as they understand it, is the "willingness to be vulnerable under conditions of risk and interdependence," which enables choice and action (Rousseau et al. 1998: 395). However, to sufficiently distinguish this understanding from the notion of hope, we have to add that this voluntary vulnerability is accompanied by "positive expectations" regarding the outcome of the behavior in question (Rousseau et al. 1998: 395).

Although trust is a highly contested concept (Shapiro 1987), we can identify a few basic traits that the notion of trust is ascribed by most disciplines (Rousseau et al. 1998: 395). Behavioral approaches such as business administration (Zand 1972) and economics (Bromiley/ Cummings 1995) see trust as strategy which enables cooperation under uncertain conditions (Engel 1999: 5).

Taken by themselves, uncertain conditions would lower the chances of entering a cooperative relationship where they pose a risk to the interests of the parties. However, to maintain the chances for personal gains from cooperative behavior, the parties can resort to trust as a mechanism to rationalize their choice. When developing a working definition of trust, we can thus differentiate between the conditions in which it is needed and consequences of its occurrence. Decisions can require trust if there is a risk to personal interests due to uncertain conditions. Its consequence is the ability to decide and cooperate under uncertain conditions (Engel 1999: 5).

For our purposes, this leaves us with the task of examining the specific risks that accompany the use of IoT in healthcare.

3 | SPECIFIC TRUST ISSUES IN THE HEALTH SECTOR

As we try to identify these specific risks, we can once again reflect on the capacities of IoT devices under the circumstances of health care and the interests of the involved actors. For the purposes of my presentation, I will only look into the interests of the patients. Oftentimes, and as seen in the example of the interconnected pacemaker, IoT devices feature two interfaces that allow communication from and to the real world, sensors and actuators. The sensory interface "reads" its respective environment and thus creates data, in our case certain health data. As IoT devices are networked devices, this data is potentially readable by all endpoints of the respective network, which invokes the patient's privacy interests, and therefore requires his or her trust in the existence of appropriate security measures. The second interface, the actuators of the device, transforms the internal status of the machine back into the real world. In our case, the pacemaker was able to induce the heart rhythm ac-

cording to the commands executed on the device. Just as sensor data is remotely readable in a networked device, every endpoint in this network is potentially able to initiate commands to the device remotely (Oltsik 2014: 5).

Here, the patient's interest is in their physical integrity: Since actuators can have immediate effects on bodily functions, the patient trusts in the existence of appropriate security measures. Both dimensions of trust in the existence of appropriate security measures enable the patient to act under uncertain conditions. Since he or she would not be able to assess the appropriateness of security measures that are implemented truly in his or her interests, trust helps the patient to take the risk of having such a device implanted.

4 | LAW AND TRUST

What is the role of law in this relationship? As we have seen, trust enables decision-making and action under uncertain conditions. However, we have not inquired yet into the sources of this trust. Economists explain the importance of trust with the condition of information asymmetry under opportunity risk. In many cases, acquiring information will be impossible or prohibitively costly. Oftentimes, a stable transactional relationship and, thus, stabilized expectations between the parties can serve as a valid source of trust. However, there are relationships that fail to stabilize with regards to trust, as trust-building transactions may be too scarce or the involved risks too high. Here, law is able to generate "generalized trust" (Engel 1999: 14), as it sets a framework of legally stabilized expectations (Engel 1999: 48).

Legal requirements regarding security measures in medical devices, which protect the patient's interest in maintaining physical integrity, have been established already since the 1990s with the Directive on Active Implantable Medical Devices and, more generally, in 1993 with the Medical Device Directive. A medical device is any non-custom-made instrument to be used by human beings for the purpose of, among other things, monitoring and treating diseases. Such devices may only be placed on the market or put into service if they bear the CE marking, which is to be granted after a positive assessment of conformity with the essential requirements for such devices. These essential requirements, which aim to ensure that the patient gains a high level of health and security, take account of the generally acknowledged state of the art. As the scope of this regulation also covers the software necessary for its proper application, these essential requirements would also be applicable to software during the lifetime of the device as indicated by the manufacturer. More specifically, this encompasses software validation according to the state of the art. This requirement, however, does not necessarily lead to increased security, as software validation would not cover unintended functions implemented in software.

We also see the emergence of specific standards concerning security, like EN 80001-1:2011. This standard describes appropriate measures of risk management for medical IT networks.

It regards all IT networks that incorporate medical devices as defined in the Medical Device Directive as medical IT networks. Although these standards are not legally binding, they often have broadly comparable effects because they are used as a measure to determine fault and negligence in tort law.

One detail in this regulation clearly shows the specific function of law as a source of trust in this relationship. The scope of regulation is limited to medical devices that are not custom-made. Customization would increase pre- and post-contractual communication between manufacturer and patient and thus would stabilize expectations or, in other words, trust. Batch-produced goods oftentimes lack this trust-generating mechanism and therefore call for legal regulation, especially with the high risks for customers illustrated here.

REFERENCES

Bromiley, P., & Cummings, L. L. (1995). Transactions Costs in Organizations with Trust. *Research on Negotiation in Organizations,* 5, 219-250.

Engel, C. (1999). *Vertrauen: Ein Versuch.* Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter.

Islam, S. M., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, 678-708.

Oltsik, J. (2014). The Internet of Things: A CISO and Network Security Perspective. Cisco Systems, Tech. Rep.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review,* 23(3), 393-404.

Shapiro, S. P. (1987). The Social Control of Impersonal Trust. *American Journal of Sociology,* 93(3), 623-658.

Zand, D. E. (1972). Trust and Managerial Problem Solving. *Administrative Science Quarterly,* 229-239.

CONCLUDING REMARKS

DR. CHRISTIAN DJEFFAL & DR. ROBIN TECH, HIIG

The contributions above show that the IoT and trust give rise to fascinating questions that can be approached from different practical perspectives and different academic disciplines. The conference proved how rich the thinking on the IoT already is. The respective panels discussed conceptual questions, questions relating to public applications and eGovernment, as well as the commercialisation of the IoT. Although a lot of reflection on many issues has occurred already, all the participants agreed that important challenges lie ahead. The fact that there is great appetite for future research can be seen from the huge interest expressed in attending the conference, but also from the discussions that took place during it.

This need for new research starts with the very concepts of the IoT and trust. The role of knowledge in the definition of trust was central to our discussions; it might be interesting to do further research in this regard. Another fascinating discussion was to what extent trust is an internal or external state. What is even more interesting is the relationship between the IoT and trust and its practical implications. One question, which is as interesting as it is complex, is whether a conscious choice of design elements will help to solve some of the regulatory challenges we are facing. Privacy and security by design could be solutions to some of the problems. Yet there are also challenges associated with regulating and standardising the technology in an effective manner. For example, the conference participants discussed which stakeholders are, and which ought to be, participating in the standard-setting process. These regulatory challenges have been pointed out from different angles. From a legal perspective, there is a need for further development in areas like cybersecurity law or data protection law.

There are also potential challenges and opportunities when dealing with the commercialisation of the IoT. Issues like interoperability and openness will determine the look of the IoT and also influence the space for creativity and innovation. Especially in the context of Industry 4.0, we see that the IoT allows for collaboration, but this collaboration depends on trust-building mechanisms to allow for the effective exchange of data — a prerequisite for the IoT. Continuously seeking to understand the factors that determine trust in the Industry 4.0 context will be an important challenge. The open software and open hardware communities will most likely play a pivotal role in the context of the IoT as well.

The reflections on the IoT and trust in the public context are special and specific because they deal with its application by public administrations. Yet the way in which the IoT will be implemented in public spaces may have serious repercussions for digitisation. Many questions that have been asked about the constitution, the state and technology will have to be

rethought. We might one day discover that the societal approach to technology is a key question. This might lead to a scenario in which the societal stance on these issues will be considered a constitutional element. Smart government and public ehealth will be components of this general framework.

One point that emerged from the conference is that there is more work to be done. It also became clear that the IoT paradigm is in constant flux and that there is no single academic discipline and no single stakeholder able to take on these issues. What we need is an exchange between different actors in society, including academia, and a transdisciplinary approach. With this in mind, we will continue to further the knowledge about the IoT and trust.

Published May 2017
by Alexander von Humboldt
Institute for Internet and Society

EDITORS
Ingolf Pernice
Thomas Schildhauer
Robin Tech
Christian Djeffal

Alexander von Humboldt
Institute for Internet and Society gGmbH
Französische Straße 9
10117 Berlin
Germany

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY