IoT safety and security as shared responsibility

Vinton G. Cerf
Vice President and Chief Internet Evangelist, Alphabet Inc.
Address: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: vint@google.com

Patrick S. Ryan
Strategy & Operations Principal, Alphabet Inc.
Address: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: patrickryan@google.com

Max Senges
Research Program Manager, Alphabet Inc.
Address: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: maxsenges@google.com

Richard S. Whitt
Corporate Director for Strategic Initiatives, Alphabet Inc.
Address: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: whitt@google.com

Abstract

What happens when everyday standalone devices and machines acquire network interfaces? The somewhat obvious result will be an unprecedented number of "things" connected to the Internet. It is less obvious what this means for the governance of the Internet when this occurs. With the "Internet of Things" (IoT) the Internet's loosely coupled governance structures are already adapting to accommodate the evolution of the Internet's use. As the governance structure continues to develop, users' safety must be the first priority for all hardware and software providers. In the context of the Internet of Things, this paper proposes a definition of digital safety as distinct from security and discusses how multistakeholder governance can be applied to address safety challenges. The paper also considers the integration of "old" industries and the transformation of their governance into the multistakeholder model as their products and services are coming online. We consider how the thousands of manufacturers who traditionally produced analog, not-connected physical "things" adapt to become stakeholders in the Internet and how that changes the way that we think about Internet Governance. The particular interest of this paper is how to address safety issues that become much more prominent with the spread of Internet-enabled physical environments.

The authors of this paper have written this project in their personal capacities as an academic contribution. The views reflected may not be the official position of the authors' employer.

Key words: Internet of Things (IoT), Internet Governance, safety, security, multiple stakeholders.

Citation: Cerf V.G., Ryan P.S., Senges M., Whitt R.S. (2016) IoT safety and security as shared responsibility. *Business Informatics*, no. 1 (35), pp. 7–19. DOI: 10.17323/1998-0663.2016.1.7.19.

Introduction

What happens when everyday standalone devices and machines acquire network interfaces? The somewhat obvious result will be an unprecedented number of "things" connected to the Internet. It is less obvious what this means for the governance of the Internet when this occurs. With the rising phenomenon known as the "Internet of Things"

(IoT) this scenario is unfolding right now, and the Internet's loosely coupled governance structures are already adapting to accommodate it. Billions of devices are increasingly online, beginning with smart phones and now ranging from our cars to video security systems to our thermostats at home [8]. One question is how the thousands of manufacturers who traditionally produced analog, not-connected physical "things" become stakeholders in the Internet and how that changes the way that we think about Internet Governance. The particular interest of this paper is how to address safety issues that become much more prominent with the spread of Internet-enabled physical environments. We also look at the integration of "old" industries and the transformation of their governance into the multistakeholder model.

The Internet has no single stakeholder, and no single category of actors who bear the primary responsibility for its governance. Instead, this is a shared responsibility among all stakeholders. We argue that challenges brought to the Internet by the IoT will be solved by the same multistakeholder mechanism that governs the Internet itself. Indeed, because as the "things" currently on the Internet do not clearly belong to any single stakeholder, governing the Net continues to be a matter of shared responsibility [3]. Additionally this existing governance framework must now take into account machines that become more "autonomous" (i.e. "smart" through machine learning etc.). In this context we believe that the concept of *digital safety* is particularly relevant as a concept for all stakeholder groups' shared responsibility.

1. Moving from digital security to digital safety

The freedom to innovate inherently includes the responsibility to protect the legitimate interests of users and of the integrity of the ecosystem that connects them. This premise holds true especially as the Internet proliferates into physical spaces and as the enabling of next-generation protocols and artificial intelligence continues to grow.

1.1. New players on the field

Billions of new interconnected things provide for many more opportunities to exploit vulnerabilities. These problems are popping up in platforms like Internet-enabled Closed Circuit Television (CCTV) devices. Because today's CCTV devices are digital cameras that process high volumes of video data, they have nontrivial computer processing and memory capacity. These devices can and have been used increasingly as elements of botnets for large attacks. There are more than 245 million security cameras installed in the world, and their significant footprint throughout the Internet has led to various recent denial of service attacks. [9].

1.2. How responsibility is shared today

How do the Internet's denizens share responsibility today? The private sector plays its part. Companies like Cisco, Facebook, Google and Verizon all depend on the trust of users and therefore have strong incentives to maintain data securely, but also to keep children and loved ones safe from dangers of online fraud, identity theft, and predators. Governmental entities, as other stakeholders, hold an important responsibility because of the need to enact laws and regulations to deter and punish bad behavior and enforce norms with laws and regulations as a backstop. Additionally, civil society groups and non-governmental organizations played key roles in the development of the Internet and continue to analyze and evaluate private-sector practices and to establish norms, expectations and principles for behavior online. And crucially, the Internet's users must bear responsibility and learn to use tools that enable a safe and secure online experience.

1.3. Inconvenient tradeoffs and sharing responsibility

Some stakeholder groups may need to trade inconvenience for security and safety. An illustration of this is the use of two-factor authentication. This illustration applies to users and for private-sector entities that employ their use. On the Net, user authentication is usually some combination of three factors: (1) something that the user knows (e.g., a password), (2) something that the user has with them (e.g. a USB key, perhaps an app on a phone), and/or (3) something intimate to the user (e.g., something biometric like a fingerprint or iris scan). Most systems today use just one factor, but the use of two (or even more) factors provides much stronger security. With multiple-factor authentication, a nontrivial additional inconvenience is inserted in the user's experience to help prove that the users are who they say they are.

Because three-factor is less common today, we'll elaborate further on the case of two-factor authentication. Most logins are accomplished by a username and password, a form of single-factor authentication. In certain cases, a *second* factor can be used, and this delivers an additional code to the user by SMS, phone call, by

a USB device or an app. While more secure, this second factor can also bring some inconvenience to users. For example, if a user is in a rush and logs into her bank account and puts in her ID and password, it can be frustrating if she also has to find her phone in order to receive a text with the additional code. It can even be more inconvenient if a company-issued key is required to be inserted in the computer---if an employee does not have the key with her, then the work may not be accomplished. Still, even with these inconveniences, users are increasingly willing to tolerate the struggle (and companies are increasingly requiring it) because they realize that it is intended to help keep them and their data safer online. As such, the use of two-factor authentication is a good example of how a user contributes to the Internet security environment, even at the expense of their personal time and convenience. Said another way, users who are employing two-factor or three-factor authentication have implicitly acknowledged the *shared responsibility* that they have with the private sector in maintaining the safety of their data.

It is important to remember this shared responsibility when deconstructing any security incident. When Sony failed to protect users' data from exposure in a major breach in 2014, Sony was immediately assailed for having abrogated its duty to protect users [15]. To be sure, Sony bears its share of responsibility for the breach, but just as importantly, government, civil society and the technical community should accept some responsibility for having acquiesced to a system that failed in the dramatic way that it did. In the case of the Sony breach, the users may not have been empowered with a failsafe mechanism for recovery from Sony's failure. For example, if Sony's users could have set up 2-factor authentication on their PlayStation's e-payment system, perhaps the breach of Sony's data would have been reduced, if not rendered inconsequential. As a practical matter, it is unlikely that any breach would have been capable of simultaneously breaching the security of the core and the security at each of the millions of users' individual two-factor devices.

It may be the case that two-factor authentication was not an option for Sony's users. In any case, the onus for finding a way forward remains one that includes *all* stakeholders. We believe that the policy environment will develop to the point where technology like two-factor authentication will be a best practice that is so widely adopted that it becomes a *de facto,* compulsory standard, one that users are demanding just as much as civil society or the technical community. In the future, users will be demanding these additional features.

For a standard to become the *de facto* requirement, the cost of *not* implementing the standard will need to clearly be higher than implementing it. How is this calculus determined? It is done in various ways, sometimes by peer pressure, other times by judicial or legislative fiat. By analogy to another field, consider the case of glaucoma testing by optometrists during any regular eyeglass checkup. The chances of any individual getting glaucoma are very low, less than 1%. However, the consequences are very high (resulting in permanent blindness) and the test for glaucoma is extremely inexpensive: only a couple of dollars. This produces a cost/benefit analysis that is clear. For this reason, by a mix of lawsuits, lawmaking and pressure from hospitals, it first became *de facto* and then *de jure* standard that optometrists must include glaucoma tests in their regular checkups. That's why every time a patient gets a regular eyeglass exam there is often (if not always) a glaucoma test (e.g., the dilation of eyes and/or the short pulses of air). We believe that this phenomenon will apply to technologies like two-factor authentication, which are increasingly affordable, and it is increasingly clear that the consequences of breach are too high for society.

Of course, any company or organization clearly has a responsibility to protect their users and to protect their data. This responsibility should not be minimized. However, the many post-incident sirens that rang for more stringent laws and better enforcement mechanisms demonstrate a scenario that is better for sensationalism than it is for practicality. Of course, standards and laws are very important. However, we must not let this rigidity of our rules and systems make us lose focus of a more holistic view of Internet security, one that moves beyond the quality of the lock at the door but emphasizes a more complete view of the role that all stakeholders have in the Internet community. The press sensationalized the attack against Sony, but there was little exposure of the kinds of measures that either Sony or users could have taken to minimize the risk. As it turns out, Sony may have been able to purchase digital certificates with a two-factor option from DigiCert to validate the certificates by a hardware token [19]. If this is the case, even if the leaked certificate information had been made available, a two-factor option would have provided a "failsafe" to minimize the damage. This protective role is a *shared responsibility* to create and maintain a safe and secure environment online. It's not that all stakeholders share the same responsibility at all times, but without question, the responsibility is rarely, if ever, exclusively vested in a single stakeholder's scope of responsibility.

1.4. Digital safety distinguished from online security

We propose a clear distinction between the concepts of *digital safety* and *online security*. We think of digital safety as a principle that protects users from harm which may be caused by increasingly semi-autonomous systems that are amalgamations of services from various developers. An example of this could be the employment of "fail-over" (or perhaps "fail-safe") solutions in case part of the system is dysfunctional. In our model, fail-over systems are not designed to defend from any breach. Instead, they are designed to assume that there may be a breach, and the fail-over kicks in to provide a solution.

By contrast, online security is the work that is put into protecting the system against malicious actors, rather than the ways that the systems act to protect users when there is a problem. Because fail-over is not a defense in and of itself, good security to prevent the need for fail-over is also important. This is a crucial contrast to "traditional" security-development practices, which are more tolerant towards system errors given that the consequence is "only" virtual or informational (e.g., "Alert! There has been a security breach!") rather than protecting users from material and physical harm. Looking at this another way, we propose the following taxonomy to distinguish *safety* from *security:*

✦ ***digital safety*** is the protection of the user in his or her environment, with technical mechanisms and policies that protect the users from being harmed by improper operation of the device;

✦ ***online security*** is the protection of the *physical network, operating systems* and *content* from exposure, modification or functional damage, utilizing a combination of software and hardware mechanisms.

In the above taxonomy, both categories could include pre-emptive as well as fail-over action. A garage door opener offers an example in which safety is paramount. Normally, the garage door can be opened with a signal from a smartphone or a radio-based key device. If this fails for some reason, it is important – for safety – that the door can be opened manually by releasing it from the motorized control. This is usually accomplished with a physical release mechanism. Usually this mechanism is only accessible from inside the garage. The failure of the controls does not trap the user but, at the same time, the system is secure in that the door does not open from the outside. The user is safe, the garage is secure.

One can imagine other intelligent devices such as thermostats that can be controlled and monitored remotely. For safety, it should not be possible to allow the temperature to be set above some maximum level. The same standard might also apply for a water heater. Even if a command is sent to try to exceed limits, a fail-safe design would inhibit exceeding fixed limits. For security, it should not be possible—or at least, easy—for an unauthorized party to control or monitor the thermostat. One might use two-factor authentication to achieve the security objective.

In short, digital safety focuses on the end user and his or her interests and health, while online security focuses on protecting other aspects of the network or the device itself. Of course, for some device failures, there could be an effect that might cause a safety issue for the user, for example an unauthorized intruder operating a device in a way that causes it to catch fire. Various security challenges are taken to a new level in the context of IoT because of the increased possibility of penetrators to access the actual equipment used to sense, actuate and control it. While these devices are online, and might be penetrated through that path (e.g. local radio, local network), direct access is an additional hazard. Additionally, the software might be altered to do everything it is supposed to do for device operation and then generate spam, denial of service attacks or other harmful attacks. The user would not be aware of the problem if the device operation did not show any signs of tampering. With regard to safety, the real concern is that these highly complex IoT ensembles (consisting of hardware, software, and firmware) may have bugs. Alternatively, a bug-free system could still generate unforeseen constellations and outcomes in such a way as to interfere with safe operation.

1.5. Linking permissionless innovation and shared responsibilities

In an environment of permissionless innovation, any entity is able to utilize the network to bring novel products and services to countless users. This incredible opportunity brings with it, simultaneously, the prospect that permissionless innovation could inflict harm upon users. We suggest that a balance exists, then, beyond the perceived "good" or "bad" of permissionless innovation. Instead, there is a three-way intersection between permissionless innovation, freedom of action, and the accompanying responsibility that everyone shares to protect users. There is ample room at this intersection for the community to devise novel solutions.

One possibility to ensure that innovators can experiment and pioneer new solutions and products would be

to promote a stronger culture and acceptance of beta-testing access to cutting edge early versions of features and products. A "beta test" is a way to support experimentation by interested early adopters by offering a new set of functionalities in exchange for an understanding that things may not work perfectly [5]. However, it is important that this expectation is clearly and transparently communicated to the users (and done with the user's endorsement and ideally, their enthusiasm). A more open approach between the private sector and the users about the nature of their products and the possible risks to them might be one way to limit liability for innovators while promoting experimentation, and to ensure that users are aware and agree to handle the risks. Such a system may never be fully adopted in any law or any court decision, but industry might band together to promote an open standard for beta testing and a system for communicating it to users. This kind of thing exists to some degree in the context of Creative Commons, which publishes a voluntary system that publishers can use to contract with users for the use of their works.

How does the multistakeholder community respond to a call to action if there is a global Internet security incident? One excellent illustration is the Conficker Working Group. In 2009 the Conficker botnet was by far the most sophisticated botnet of its time. In a matter of weeks, the botnet had infected millions of computers, including government, business and home computers in all 193 countries. The Conficker Working Group (*http://www.confickerworkinggroup.org*) was rapidly (and informally) assembled, and made up of private sector actors such as Microsoft and Symantec, academic researchers, and NGOs such as ICANN and the ShadowServer Foundation. Various government representatives also engaged in the groThe Conficker Working Group carried out its work with no formal mandate, and operated under no formal entity structure. It was a loosely coupled group of representatives from all sectors that banded together with the sole purpose of quickly stopping the spread of Conficker. The fact that the group had no mandate, no budget and no formality allowed it to form and to act quickly and deliberately. To stop one of the strains, the collaborators "coordinated with over 100 countries and blocked over 50,000 domains per day" over the course of less than three weeks [7]. This kind of mobilization and responsiveness was made possible because of the loosely coupled and informal nature of the governance system that came together to address the problem.

2. Application to the Internet of Things

For the Internet's first twenty-five years of commercial operation, the network has largely consisted of user-operated end points and servers. This has also been described as the "end to end" model, which means that most "intelligence" occurred at the edge of the network, i.e., at the devices that connect to it. Today, the physical environment itself is coming "alive," and it is thriving and growing in a cloud of networked devices. This is the Internet of Things (IoT): a mental construct, or ordering principle we are using to describe effort to take the Internet to the next physical level. Indeed, the IoT is really just the Internet itself, but with one very different feature: online activities will not be only informational but include interactions with "things" in all contexts of life and often having physical consequences. Additionally these interactions will increasingly be determined by some form of machine intelligence that lets "things" coordinate semi-autonomously.

IoT has been defined as "a pervasive and self-organizing network of connected, identifiable, and addressable physical objects through the use of microprocessors" [18]. IoT's pervasiveness rings in Cisco's recent branding of the "Internet of Everything." This sounds more inclusive as it describes the networked connection of people, process, things, and data. Things are all inanimate physical objects and devices, like sensors, consumer devices, and enterprise assets, while process is how to manage the way that people, data, and things work together [6]. As David Kirkpatrick explained, "we are extending the connectivity of the Net to a much wider world-wide-web that includes the manifold physical objects of the world, letting them speak back to software that makes sense of what those objects tell us" [12]. Thus, as Neil Gross has opined, the Internet may continue to grow around the globe as an "electronic skin" that touches all aspects of life: "In the next century, planet earth will don an electronic skin. It will use the Internet as a scaffold to support and transmit its sensations. This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, ERGs, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways, and fleets of trucks, our conversations, our bodies – even our dreams" [10].

However we choose to describe the future Internet, it is big, and the things using it are no longer only human.

This may seem axiomatic now, and as IoT phenomenon takes off, the policy environment will need to adapt in order to accommodate the shift.

2.1. IoT policy challenges

A host of policy challenges exist by the rise of the Internet of Things. Luckily most of these fall into an existing law or policy process without the need for new, customized legislation. For example, the network standards developed for IoT, with attendant questions about interoperability and proprietariness, can have a home with standard-setting organizations like the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and/or other non-governmental organizations. Similarly, concerns about generating ubiquitous connectivity involves dealing with national and international bodies allocating radio spectrum.

We identify two new major policy challenges in the context of the emergent IoT: (1) the integration of "old" industries and the transformation of their governance into the multistakeholder model and (2) digital safety, which is not entirely new but becomes exponentially more widespread as connectivity continues to involve more physical spaces.

2.2. Integrating "old" industries into the multistakeholder governance mesh

On the one hand, traditional businesses are digitizing their means of production and they need to ensure safety and other good practices towards their employees (as well as towards the users of the products). On the other hand the products (or "things") produced are now Internet enabled and hence the companies become part of the existing Internet governance ecosystem. This second category is also known as the "industrial Internet" (or Machine to Machine networks or "industry 4.0" in Germany). The promise of the industrial Internet is in the potential to set up value networks in manufacturing, logistics, maintenance and business that have increasingly complete information capture, flow, sharing and productivity. In the industrial sphere of the IoT it is mainly the private sector that owns the facilities and is responsible for securing them. Hence manufacturers and businesses will be held responsible to ensure that their production, work and deployment environments are safe. In this context, the government's traditional role will be important for rule-setting. From there, interests of workers are represented and company practices are scrutinized by unions. Finally, the judicial system, public scrutiny and peer pressure are responsible for enforcement.

Another challenge exists in the introduction and integration of traditional industries into the Internet Governance ecoystem. Tthis is significantly harder because of the sheer volume of new stakeholders that IoT brings with it, and the heterogeneity of policy challenges. Nevertheless we are faced with the task of introducing methods of and expertise from multistakeholderism gained in the Internet governance context to political and private sector spheres (manufacturing, city development, consumer electronics). These traditionally enjoyed more limited focus within the variety of local and global stakeholders into their decision making practices. Concepts like stratifying and delineating conflicts so that the "tussle" in this part of governance is productive and can be addressed and then solved by the right multistakeholder constellation (in the right layer) naturally become ever more important and more challenging.

2.3. Role of privacy in the discussion

From the user perspective, who controls what information about the user and her environment is a new question when applied to a world of connected things. And whether that information is adequately protected from misuse by government or private actors is a natural follow-on concern. As just one example, can one plausibly "opt out" of being involved with the devices and sensors that help comprise one's very environment? And is privacy only an issue where objects meet subjects?

Although the focus on our paper is on the distinction between safety and security, many of the consumer-protection agencies that handle consumer safety are also responsible for protecting privacy. We won't address this topic exhaustively here, although we believe that the IoT will likely see the entrance of many consumer-protection agencies into the field of governance on many topics, including privacy. In Europe, for example, there are several directives and rules that involve the digital market that are aimed at broadly protecting consumer rights, including privacy. Some of these include Directive 2011/83/EU on consumer rights; Directive 95/46/EC on the protection of individuals with regard to the processing of personal data; Directive 2000/31/EC on certain legal aspects of information society services; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and many others. Although analysis of the relevance of these laws and their effect

on IoT is research for another day, we believe that it is relevant to identify some of the areas of exploration in the privacy space.

The move from a "small data" to a "big data" world necessitates several changes. For example, not all data will be personally identifiable, and instead, data growth will focus on the environment, infrastructure, and on the behavior of other devices and things on the Internet. Some data may fall into a gray area where predictions or revelations about individuals may be possible. The focus should be not on the collection of data, but whether it is harmful (e.g. use vs. collection). Because of this shift in use of the Internet, concepts like notice and choice will be less useful in the future, as will "data minimization" rules [2]. In this environment, distributed intelligence in the network can identify and protect against threats, even as it can also seed and spread threats throughout the user's environment.

2.4. Competing policy frameworks

Much like the Internet itself, the global cloud of things challenges national boundaries and barriers. The IoT also is not a single system, but comprises many overlapping networks of open, closed, and partially open systems. The multiplicity of different architectures and applications suggests no centralized governance structure; most is private company or user property, some is public on the Internet.

One way to look at the competing policy frameworks is through the lens of the Internet Governance Forum (IGF). The IGF has been in operation since 2006 and has met annually at the invitation of a host country. A multistakeholder advisory group (MAG), led by a chairman appointed by the UN Department for Economic and Social Affairs (UNDESA), organizes the annual meeting, deciding among proposed topics which will be on the agenda. A variety of formats are used to allow issues to be articulated and various perspectives to be shared.

The Internet Governance Forum (IGF) has looked at the IoT on various occasions. There is a Dynamic Coalition on the Internet of Things, but, to our knowledge, the experts so far concluded that no special IoT governance is warranted because it is "just" another Net application. If so, should responsibilities even be discussed in this early stage of IoT deployment? We think now is the right time exactly because it is still possible to adjust trajectories and inform choices. We argue that debate about how to share responsibility for IoT safety should happen at all levels and by all actors. That said we agree that because the benefits and harms of an IoT world are difficult to detect in the early stages, policymaking needs to be both flexible and future-proof.

3. Evolving Internet Governance

Because the Internet is a shared environment, its governance is a shared responsibility. Put more succinctly, the form of the Internet Governance Forum should follow its function. So what could a shared responsibility regime for IoT safety look like? We have previously argued that "forum follows function" in the context of the Internet Governance Forum [4]. This means that the IGF has the ability to perform the the functions to (1) identify emergent IoT safety challenges, (2) facilitate the creation of multistakeholder working groups that set out to develop solutions and to (3) monitor the effectiveness of these solutions allowing for open analysis and discussion, critiques and proposals for amendments or new recognition of problematic phenomena.

Traditional regulatory practices struggle to keep pace with the speed of innovation on the Internet. A more traditional "top-down" governance approach would stifle the very user benefits that stakeholders seek to enhance. This means that, far from any a single "one stop shop" for Internet governance, the informal practices that brought the Internet to the amazing state of constant growth and evolution today will, itself, continue to bring new and innovative governance systems along for the ride. Governments are important, but they do not play an exclusive, top-down, dominant role. Instead, governments participate on an equal footing as representatives of their respective constituents. These constituents – from the private sector to civil society to technical experts – are often in a tussle with governmental representatives and other relevant stakeholders on an issue by issue and sometimes case by case basis. Through an inclusive and transparent process, this helps create a truly global governance sphere.

What areas are each of these groups likely to advocate in the IoT context? A few of these roles include the following:

✦ **Government.** Set a high but implementable bar for protecting citizens, with two objectives: enforcement (e.g., consumer protection as well as health & safety concerns) and education (for example, phishing requires a sensitivity from the consumers that no system can absolutely protect).

✦ **Private sector.** Build the most secure systems possible, and share the education objective on how best to use tools available. Solicit ways to involve users as partners in providing better safety and security.

✦ **Civil society.** Represents the user and public-interest perspectives. Civil society plays a key role in verifying that checks and balances for governmental institutions are functioning and in keeping up with technological innovation. It also ensures that the line between government and the private sector is maintained. Additionally, there is also an educational objective to spread digital literacy, and this includes educating users about safety and security. Finally, civil society is on the front lines to protect human rights in dangerous parts of the world, and to educate citizens to be save and secure online.

✦ **Technical community.** The "technical community" makes sure that the standards are advancing properly (e.g., work of the IETF) and that protections and best practices (like DNSSEC) are implemented in the Internet's critical infrastructure. Although each group has its own educational mandate, the technical community also shares some similar educational objectives as civil society to educate all stakeholder groups (and in particular, users) on the proper design and functioning of various systems.

As we think further about the meaning of safety, it is useful to identify how these concepts can be found in different ways in the different layers of the Internet. In this vein, we believe that it is most sensible to look at the evolution of the Internet (and its governance) from the perspective of a "layered model" [4]. As we look at the different parts of each network layer, the resources (and hence the stakeholders) are a variable mix of private and public actors. Only in the logical layer is the resource largely a shared, public commons. As a result, in all the layers (except logical), the blend of private and public goods means that responsibility for safety issues remains with a mix of private and public actors. By contrast, the logical layer operates under a different governance regime than the others, one that accounts for this material difference. There, responsibility for safety matters lie with the pertinent multistakeholder governance community as a whole (rather than distributed among the stakeholders). We elaborate on the layered model as it applies to IoT below.

3.1. Placing IoT within the existing governance model

How do governance matters related to IoT relate to governance of the rest of the Internet? In Figure 1 we build on a model we previously proposed, but modified to include sample stakeholders who are specifically relevant to IoT governance. As we will see in our description below, the most important area of activity for governance of IoT will be in the content layer.

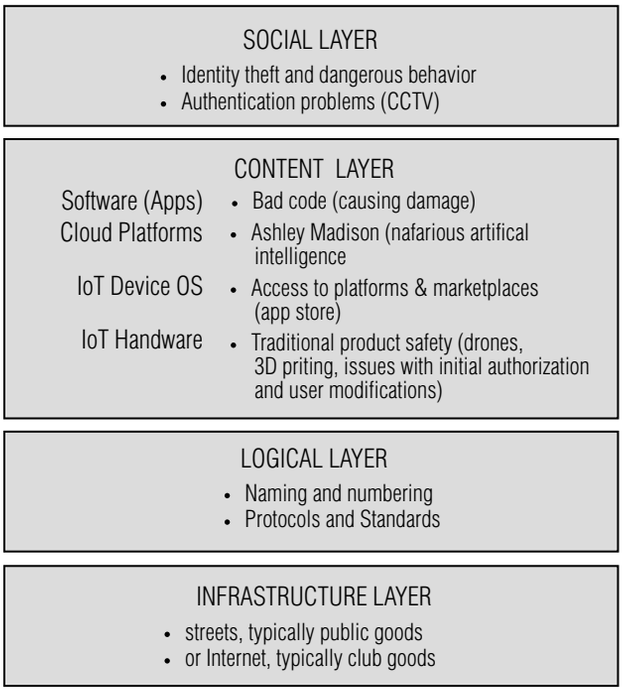

Fig. 1. Layered model of Internet Governance adapted to Internet of Things

The infrastructure layer at the base of Figure 1 is the physical foundation for the network. The rights-of-way, poles and areas shared with other providers are sometimes described as a "club good" provided by private ISPs, and it has converged with infrastructure supplied by public entities like power, water, streets and lighting. Governance practices of the physical layer are relatively well established, even if new innovations are challenging some of those traditions (e.g., regulation for things like High Altitude Platform Services). Above the infrastructure layer, the logical layer demonstrates a more robust history of multistakeholder governance models, with active groups like ICANN, IETF, IEEE and others. Adaptation of these groups to IoT-specific stakeholders should participate with the relevant institutions.

Most of the challenges related to IoT governance will occur in the content layer and above. Because of this tendency, the institutions that currently handle governance in this layer will need to be strengthened in order to address the arrival of IoT devices into the governance landscape. In the context of IoT, we prefer to refer to this layer as the "user and interaction layer" because the intent is to capture activities that include "traditional" web, virtual services, and services that have things attached to them or depend on connected sensors and devices. We expect that many governments will argue that the addition of sensing and actuating things to the network may require a heightened analysis when it comes to user safety.

With consumer safety issues becoming more important, we may see more active participation by a myriad of consumer-protection agencies in the heart of Internet governance. Here, no new special safety challenges arise with IoT. Obviously, consumers will continue to do silly things like using hair-dryers while sitting in a tub of water. On some level even this kind of problem will be less important with smarter devices (e.g., a hair dryer with sensors that turns off when there is too much moisture), but there will always be an opportunity to discuss where the lines of demarcation are in the "shared responsibility" of manufacturers to make devices that anticipate user errors, and the users themselves who must use devices responsibly.

3.2. Polycentric governance mechanisms

Recently, the logical layer has received a lot of attention because of the study of polycentric governance mechanisms as identified by Nobel Laureate Elinor Ostrom [14]. One of the many contributions that Ostrom brought with her work is to point out that complexity is not the same as chaos in polycentric governance systems. Polycentric governance is characterized by an organizational structure where multiple independent actors mutually order their relationships with one another under a general system of rules. There is no single stakeholder positioned to drive the Internet's future; instead, all stakeholders should act within their areas of expertise (in a "polycentric" way") and hold account for their area of responsibility. These stakeholders press forward in a spirit of interdependent cooperation and stewardship in the same way as the majority of the standards for the Internet, itself, have developed at the IETF.

3.2.1. The bazaar of Internet Governance

One of the best examples of how technology can be developed in a loosely coupled governance environment was penned by computer programmer Eric Raymond. Raymond's essay, "The cathedral and the bazaar" [16] outlines different approaches to software engineering, the "cathedral," which represents a top-down hierarchy, and the "bazaar" representing a flatter, more democratic (albeit chaotic) process for software development. This is a useful way to analyze the philosophy of the Internet's development as compared to older telecom industries (e.g., Bell Labs). In essence, the "bazaar" method for software writing is not unlike how Wikipedia works: the system is open, exposed, subject to comment by anyone who has an opinion. Raymond's central claim is that "given enough eyeballs, all bugs are shallow," which, essentially, means that broad dissemination and discussion of coding provides better pThe equivalent of the bazaar in standard-setting organizations is the the Internet Engineering Task Force (IETF) – an open, volunteer-based standards-setting environment without any formal corporate "personality," where engineers have developed the core functionality that enables packets to transfer throughout the Internet. All IETF designs are freely accessible, and all IETF processes are published in their entirety on the Internet. If anything, reading the IETF website can be a bit onerous if only because it might feel like there's too much information available. Notably, the publications are all available and readable in any format, and it's expected that anyone, anywhere, can participate in the IETF process. As Harald Alvestrand describes, the IETF depends on an entirely open process, which means that "any interested person can participate in the work, know what is being decided, and make his or her voice heard on the issue. Part of this principle is our commitment to making our documents, our WG [working group] mailing lists, our attendance lists, and our meeting minutes publicly available on the Internet" [1].

Drawing from analogies throughout the open-standards space, the IETF is a true meritocracy: If members of the IETF community determine that an engineer's ideas have value, those ideas are adopted and incorporated into the Internet's suite of standards. Ideas that are dated or counterproductive, on the other hand, fester and fail. As famously stated by David Clark of the Massachusetts Institute of Technology: "We reject kings, presidents and voting. We believe in rough consensus and running code" [11]. By contrast, many top-down, government-centric systems rely on appointments by governments and formal committees, just as worldwide development of standards under the PTT model did.

3.2.2. Safety is already a shared responsibility

Importantly, it's not only the Internet where shared responsibility occurs. One example is in the way people organize themselves for home and neighborhood security. Here, the government plays a role via creating legal disincentives for criminals and enforcement through police, as well as the establishment of safety standards and codes. The private sector also participates via private security guards; alarm monitoring systems; theft-deterrent fencing, and the like. Civil society plays its own role through

mechanisms like neighborhood watch programs and collective actions by individual neighborhoods. Further, there is a question of education and user choice as well – e.g., some people choose to lock their door, some don't; some people choose to use deadbolts, others don't.

3.3. Mapping IoT to the current governance system

In this last section we will take a look at the governance environment we want to work towards, especially as concerns IoT safety. Before we discuss the features of a good governance system, allow us to elaborate on what we see as ambition for future technologies and IoT in particular. We hold a user-centric conception of technology meaning that the Internet of Things should further human development and increase the well-being of users. All technology is a means to further scientific advancements and innovation not only for its own sake but to further a people-centred Information Society and richer, more just governance and economic conditions. Lawrence Lessig elaborated on this theme by distinguishing between technologies of access (to knowledge and services) and technologies of control (empowering institutions to better monitor and control users) [13].

If technology is user-driven, what kinds of experiences will users have when IoT goes mainstream? On an abstract level, most IoT benefits are generated through applications of systems. For example, networked sensors and traffic signals lead to more efficient traffic flow in a smart city, temperature sensors and smart distributed heating and cooling systems lead to energy savings in smart homes and similarly agricultural sensor networks allow for more targeted watering and fertilizing resulting in higher yields and higher sustainability.

We may find a significantly different and rapidly evolving constellation of responsibilities when analyzing the consumer oriented sector of the IoT, as this area will include notions of increasingly smart home products. As noted earlier, these roles may be increasingly filled by consumer-protection agencies and by consumer-focused civil society efforts. While responsibility for safety is not always easy to assign in bigger infrastructure, there is at least relatively clear ownership and hence control of the system in question (e.g, a road, factory, etc). In the consumer space, however, the multitude of connected devices and their interaction may create new safety threats. Additionally, the end uses are increasingly involved in the customization and in hacking the deployment of the product. Also, "prosumers" – consumers who produce and consume media, and who hack their devices – will continue to increase, and this trend complicates the task of communicating safety flaws of products.

In *Figure 2* we map the IoT governance world to the model that we have previously presented. Stakeholder groups such as automotive companies, consumer protection agencies and public safety will increasingly express themselves in the governance sphere. These and other groups will play an increasing role in (i) designing and defining safety standards, (ii) ensuring products and services are safe to use and (iii) dealing with safety hazards once they happen.

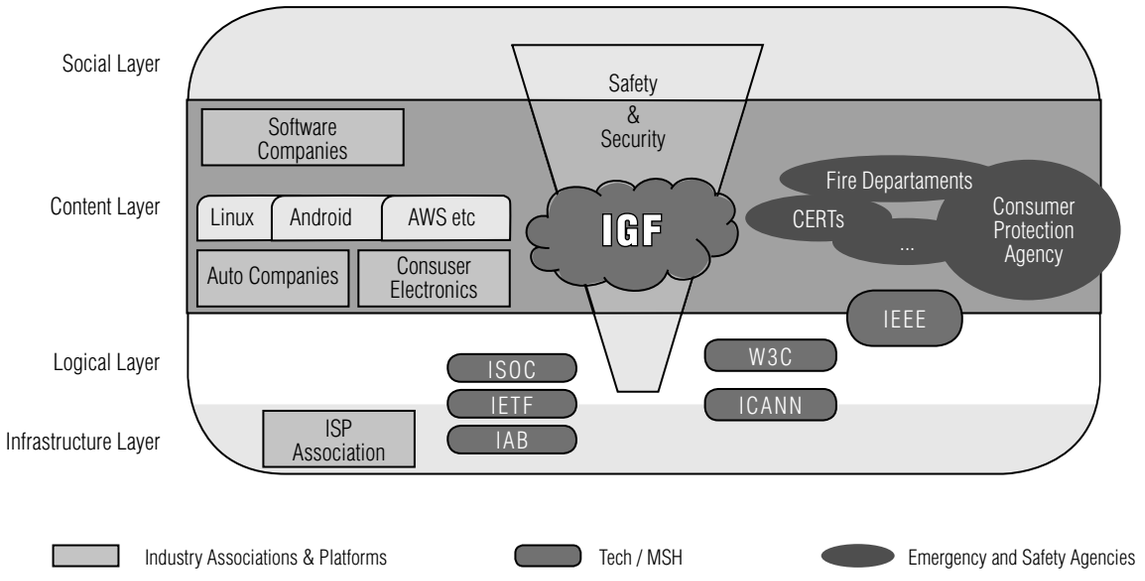

Fig. 2. IoT safety governance ecosystem

The approach described above provides additional groups within each of the layers to show on what layer agencies that deal with IoT issues would interface with colleagues. As in other aspects of Internet governance, this construct leads to a dynamic, interwoven and hypertextual network of commitments between stakeholders that agree to develop and implement solutions together. This informal and decentralized method is, in our assessment, more effective and adequate than other (more traditional) approaches like trying to develop and ratify a hypothetical *Treaty on Cyber Safety or a hypothetical Treaty on Safety of the Internet of Things*. Among the many reasons, this approach allows for faster updates, more experimentation with new solutions and flexibility to address unique cultural, contextual and political contexts. These kinds of treaty proposals are not outlandish. We saw 193 nations struggle with how to implement (or not implement) Internet security measures by force of treaty at the World Conference on International Telecommunications (WCIT-12). The attempts seen at WCIT-12 and other measures are likely going to continue [4].

There are some stakeholder institutions that are worth singling out because of the role we expect them to play in IoT safety, and in particular, the role of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). The first CERTs were started almost 30 years ago and today there is a network of CERTs around the world, and one of their main activities is addressing internet security/safety incidents. CERTs provide technological activities in the cyberworld that are comparable to firefighters or emergency natural disaster response teams in physical world. The mandate of both CERTs, and other public-safety groups, may expand to include IoT emergencies, and hence their funding base should include all traditional private sector players that embrace connectivity in their products.

Conclusion

The advent of the Internet of Things gives us a tremendous opportunity to examine the very real issues at the heart of protecting the legitimate interests of users. An increased understanding of the distinction between the network, operating systems of things, application software and usages – especially when it comes to the security and safety of human users – will allow a crisper creation of solid multistakeholder practices in both virtual and physical worlds.

Many research questions of course remain open: What responsibilities does the general public inherit from the use of Internet enabled devices to protect others from dangerous behavior and against abuse (e.g. the fence around the swimming pool that is required by law in some jurisdictions)? Will the concept of negligence and causation change in the context of the Internet of Things? What are the consequences of a failure to update a safety critical software in a timely way? These and many other questions are certain to arise as the population of Internet-enabled devices increases and becomes a working part of our daily lives. ■

References

1. Alvestrand H. (2004) *A mission statement for the IETF. IETF*, Request for Comments 3935. Available at: https://www.ietf.org/rfc/rfc3935.txt (accessed 01 February 2016).
2. Andrade P.L., Hemerly J., Recalde G., Ryan P. (2014) From Big Data to big social and economic opportunities: Which policies will lead to leveraging data-driven innovation's potential? *The Global Information Technology Report 2014: Rewards and Risks of Big Data*. INSEAD, Cornell University, the World Economic Forum, pp. 81–86.
3. Cerf V.G., Ryan P.S., Senges M. (2014) Internet Governance is our shared responsibility. *I/S: A Journal of Law and Policy for the Information Society*, 10 ISJLP 1 (2014). Available at: http://ssrn.com/abstract=2309772 (accessed 01 February 2016).
4. Cerf V.G., Ryan P.S., Senges M., Whitt R.S. (2014) A perspective from the private sector: Ensuring that forum follows function. In: *Beyond Netmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem* (W.J.Drake, M.Price, eds). Center for Global Communication Studies, Annenberg School for Communication at the University of Pennsylvania. Available at: http://ssrn.com/abstract=2489348 (accessed 01 February 2016).
5. Chesbrough H., Van Alstyne M. (2015) Permissionless innovation. *Communications of the ACM*, vol. 58, no. 8, pp. 24–26.
6. Cisco (2012) *Tomorrow starts here*. Press release. 10 December 2012. Available at: http://goo.gl/vlKOfJ (accessed 01 February 2016).
7. Conficker Working Group (2010) *Conficker Working Group: Lessons Learned*. June 2010 (Published January 2011). Available at: http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf (accessed 01 February 2016).
8. Faddell T. (2015) Nest CEO Tony Fadell on the future of the Internet. *Wall Street Journal*, 26 April 2015. Available at: http://www.wsj.com/articles/nest-ceo-tony-fadell-on-the-future-of-the-internet-1430104501 (accessed 01 February 2016).
9. Gayer O., Wilder O., Zeifman I. (2015) CCTV botnet in our own back yard. *The Incapsula Blog*, 21 October 2015. Available at: https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html (accessed 01 February 2016).
10. Gross N. (1999) The earth will don an electronic skin. *Bloomberg Business Week*, 30 August 1999.
11. Hoffman P. (2012) The Tao of IETF: *A novice's guide to the Internet engineering task force*. Available at: http://www.ietf.org/tao (accessed 01 February 2016).
12. Kirkpatrick D. (2013) Why an Internet of everything event? 'It's the world waking up'. *Techonomy*, 3 May 2013.

13. Lessig L. (2002) The future of ideas: *The fate of the commons in a connected world*. Vintage Books.
14. Ostrom E. (2009) *Beyond markets and states: Polycentric governance of complex economic systems.* Nobel Prize Lecture, 8 December 2009. Available at: http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf (accessed 01 February 2016).
15. Pettersson E. (2015) Sony to pay as much as $8 million to settle data-breach case. *Bloomberg Business*, 20 October 2015.
16. Raymond E.S. (2000) *The cathedral and the bazaar*. V. 3.0. Available at: http://www.catb.org/esr/writings/homesteading/cathedral-bazaar/ (accessed 01 February 2016).
17. Ryan P., Falvey S. (2012) Trust in the clouds. *Computer Law & Security Review*, vol. 28, no. 5, pp. 513–521.
18. Schindler H.R., Cave J. (2013) *Towards a dynamic and trustworthy Internet of things.* Rand Europe Research Brief, 88-9742-EC.
19. Westby J. (2014) *Instead of a real response, perennially hacked Sony is acting like a spoiled teenager.* Forbes, 17 December 2014. Available at: http://www.forbes.com/sites/jodywestby/2014/12/17/sony-earns-cyber-troglodyte-award/#2fc4f7f96942 (accessed 01 February 2016).
20. Whitt R.S. (2013) A deference to protocol: Fashioning a three-dimensional public policy framework for the Internet age. *Cardozo Arts & Entertainment Law Journal*, no. 689, pp. 754–756.

Интернет вещей: безопасность и защита как коллективная ответственность

В.Г. Серф
вице-президент, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: vint@google.com

П.С. Райан
директор по стратегии и операциям, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: patrickryan@google.com

М. Сенгес
менеджер исследовательских программ, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: maxsenges@google.com

Р.С. Витт
корпоративный директор по стратегическим инициативам, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: whitt@google.com

Аннотация

Что произойдет, если отдельные технические устройства приобретут сетевой интерфейс? Очевидно, что результатом будет беспрецедентное количество «вещей», подключенных к сети Интернет. Менее очевиден ответ на вопрос, что это будет означать для управления Интернетом. В свете концепции Интернета вещей (Internet of Things, IoT) взаимодействующие управленческие структуры уже приспосабливаются к тому, чтобы соответствовать эволюции применений Интернета. Однако, поскольку структура управления продолжает развиваться, безопасность пользователей становится приоритетом для всех поставщиков технических и программных решений. В контексте Интернета вещей в данной статье предлагается определение цифровой безопасности, отличающееся от защиты данных, а также обсуждается то, как управление, затрагивающее различных заинтересованных лиц, может применяться для обеспечения такой безопасности. В работе также рассматриваются вопросы интеграции «старых» отраслей и трансформации управления ими в «мультистейкхолдерную» модель по мере того, как их продукты и услуги становятся онлайновыми. Обсуждается, как тысячи производителей, традиционно производящие не связанные между собой «вещи», адаптируются к роли стейкхолдеров Интернета и как это изменяет наше представление об управлении Интернетом. Особое внимание в статье уделено тому, как это связано с вопросами безопасности, которые становятся все более актуальными в связи с широким распространением Интернет-ориентированных физических устройств.

Авторы выполнили данную работу в академических целях, на основе своего видения рассматриваемых вопросов. Мнение авторов может не совпадать с официальной позицией их работодателя.

Ключевые слова: Интернет вещей, управление Интернетом, безопасность, защита, множественные стейкхолдеры.

Цитирование: Cerf V.G., Ryan P.S., Senges M., Whitt R.S. IoT safety and security as shared responsibility // Business Informatics. 2016. No. 1 (35). P. 7–19. DOI: 10.17323/1998-0663.2016.1.7.19.

Литература

1. Alvestrand H. A mission statement for the IETF // IETF, Request for Comments 3935. 2004. [Электронный ресурс]: https://www.ietf.org/rfc/rfc3935.txt (дата обращения 01.02.2016).
2. Andrade P.L., Hemerly J., Recalde G., Ryan P. From Big Data to big social and economic opportunities: Which policies will lead to leveraging data-driven innovation's potential? The Global Information Technology Report 2014: Rewards and Risks of Big Data // INSEAD, Cornell University, the World Economic Forum. 2014. P. 81–86.
3. Cerf V.G., Ryan P.S., Senges M. Internet Governance is our shared responsibility // I/S: A Journal of Law and Policy for the Information Society, 10 ISJLP 1 (2014). 2014. [Электронный ресурс]: http://ssrn.com/abstract=2309772 (дата обращения 01.02.2016).
4. Cerf V.G., Ryan P.S., Senges M., Whitt R.S. A perspective from the private sector: Ensuring that forum follows function // Beyond Netmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem / W.J. Drake, M. Price, eds. Center for Global Communication Studies, Annenberg School for Communication at the University of Pennsylvania. 2014. [Электронный ресурс]: http://ssrn.com/abstract=2489348 (дата обращения 01.02.2016).
5. Chesbrough H., Van Alstyne M. Permissionless innovation // Communications of the ACM. 2015. Vol. 58. No. 8. P. 24–26.
6. Tomorrow starts here // Cisco press release. 10 December 2012. [Электронный ресурс]: http://goo.gl/vlKOfJ (дата обращения 01.02.2016).
7. Conficker Working Group: Lessons Learned. June 2010 (Published January 2011). [Электронный ресурс]: http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf (дата обращения 01.02.2016).
8. Faddell T. Nest CEO Tony Fadell on the future of the Internet // Wall Street Journal, 26 April 2015. [Электронный ресурс]: http://www.wsj.com/articles/nest-ceo-tony-fadell-on-the-future-of-the-internet-1430104501 (дата обращения 01.02.2016).
9. Gayer O., Wilder O., Zeifman I. CCTV botnet in our own back yard // The Incapsula Blog, 21 October 2015. [Электронный ресурс]: https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html (дата обращения 01.02.2016).
10. Gross N. The earth will don an electronic skin // Bloomberg Business Week, 30 August 1999.
11. Hoffman P. The Tao of IETF: A novice's guide to the Internet engineering task force. 2012. [Электронный ресурс]: http://www.ietf.org/tao (дата обращения 01.02.2016).
12. Kirkpatrick D. Why an Internet of everything event? 'It's the world waking up' // Techonomy, 3 May 2013.
13. Lessig L. The future of ideas: The fate of the commons in a connected world. Vintage Books, 2002. 384 p.
14. Ostrom E. Beyond markets and states: Polycentric governance of complex economic systems. Nobel Prize Lecture, 8 December 2009. [Электронный ресурс]: http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf (дата обращения 01.02.2016).
15. Pettersson E. Sony to pay as much as $8 million to settle data-breach case // Bloomberg Business, 20 October 2015.
16. Raymond E.S. The cathedral and the bazaar. V. 3.0. 2000. [Электронный ресурс]: http://www.catb.org/esr/writings/homesteading/cathedral-bazaar/ (дата обращения 01.02.2016).
17. Ryan P., Falvey S. Trust in the clouds // Computer Law & Security Review. 2012. Vol. 28. No. 5. P. 513–521.
18. Schindler H.R., Cave J. Towards a dynamic and trustworthy Internet of things // Rand Europe Research Brief, 88-9742-EC. 2013.
19. Westby J. Instead of a real response, perennially hacked Sony is acting like a spoiled teenager // Forbes, 17 December 2014. [Электронный ресурс]: http://www.forbes.com/sites/jodywestby/2014/12/17/sony-earns-cyber-troglodyte-award/#2fc4f7f96942 (дата обращения 01.02.2016).
20. Whitt R.S. A deference to protocol: Fashioning a three-dimensional public policy framework for the Internet age // Cardozo Arts & Entertainment Law Journal. 2013. No. 689. P. 754–756.