Setting a Privacy and Security Comfort Zone in the Internet of Things

Barbara Endicott-Popovsky[1(✉)], Scott David[1], and Martha E. Crosby[2]

[1] University of Washington, Seattle, WA, USA
{endicott, scott.david}@uw.edu
[2] University of Hawaii at Manoa, Honolulu, HI, USA
crosby@hawaii.edu

Abstract. This paper seeks to raise awareness of the potential benefits and detriments resulting from sensor intrusion in the Internet of Things (IoT). The conclusion of this paper is that the IoT has been rendered inevitable as the result of a confluence of historical trends, but that we can make choices regarding its fundamental architecture that can tip the balance of harm and benefit more toward individual or institutional rights and obligations. Once the choices are "baked in" they will be more difficult to alter in future IoT iterations. It is hoped that collective attention to the issues raised in this paper will help to guide these decisions so that the IoT systems we build will result in fewer surprises.

Keywords: Internet of things · Information on top · Insight on time

1 Introduction and Background

1.1 Technology in History

Throughout history, people have created technology to leverage their capacities. Leverage increase and risk reduction are not cost free. Costs include the costs of acquiring or using the technology and the "cost" or loss of liberty when a dependency is developed on the technology. Once we start using hammers, houses are designed to be built with nails, eliminating alternative technologies. Also, various costs of technology are borne by individuals outside the direct supply chain. For example, neighbors of the auto factory experience the noise and pollution of the factory, unregistered alternative energy sources are crowded out, etc. It is typical that reduction of risk in one area frequently requires risk increases somewhere else.

Technology helps mitigate risks. For example, stop lights can mitigate traffic accidents. There are multiple risks borne by individuals and society associated with home heating. Some are immediate risks of comfort and health to the family, while others are broader risks of energy crises on a global level. The thermostat helps to mitigate some existing risks in new ways, but also introduces new risks and benefits associated with the entirely separate world of data commodities, one that is not yet fully developed and therefore more difficult to weigh.

Today's thermostat is a socio-technical feedback loop that is loosely coupled to the information network of the energy markets. Information associated with energy

D.D. Schmorrow and C.M. Fidopiastis (Eds.): AC 2015, LNAI 9183, pp. 722–734, 2015.
DOI: 10.1007/978-3-319-20816-9_69

consumption for home heating is tied to energy information systems subject to security and privacy violations, introducing new risks.

Rules and technical controls are meant to make some element of feedback loops more certain. For instance, when entering a crossroads, drivers perceive other drivers and adjust speed or braking behavior to take their action into account. The red light creates a standard convention to render the behavior of others more predictable, much as the technology of thermostats renders the temperature more predictable by controlling the behavior of a boiler, and therefore more reliable. We need rules and tools to control the new security and privacy risks created by feedback loops connected to information networks.

1.2 IoT Makes the World a Keyboard

The Internet of Things is being realized as the cost of wireless networking, and of data collection, transfer and processing have gone down. As a result, the once unknown details of interactions of people and things can now be collected, transferred and processed for trivial cost and provide insight into consumer behavior. Where that insight has the potential to harm the interests of an individual or entity it is viewed as an "intrusion." In fact, insight and intrusion are two perspectives on the same phenomenon of heightened information.

If you have ever been camping or lived in a home with wood heat, you know that the first person to wake up in the morning stokes the fire to warm up the campsite made cold by inattention during sleep. The colder the campsite, the greater the urgency to get the fire going. The fire and the people form a primitive feedback loop, through which the sensation of cold leads to fire building behaviors, and the achievement of heat signals that those behaviors can stop.

The first electrical thermostat automated the process by providing an artificial heat sensor to replace the human sense of cold and connection to a boiler to replace the wood stove. Such devices were used in settings where consistent temperature had to be maintained, such as incubators for poultry and later human residences. In each case a "feedback loop" was automated to increase efficiency and lower costs.

When the systems operate reliably, they achieve great savings of resources and mitigation of human suffering and inconvenience and increase productivity. That reliability is being threatened by the potential security and privacy breaches that result from being connected online.

1.3 Tech Feedback Loops

Humans have configured a myriad of such feedback loops to increase their comfort, safety and convenience in the physical world. Each of these systems detects a situation through sensors and then performs an assigned task, through "actuators." They are typically one dimensional devices, programmed only to sense a limited range of phenomenon and to actuate a limited response. Each is directed at addressing a specific

physical "risk" in the physical world where risk includes inconvenience (heating and elevators) and harm (fire or street crossing).

The Internet of Things is knocking at their door. As processors and radios have gotten smaller and cheaper following Moore's law (2x processor concentration every 18 months) [1], it has become possible to include sensors, processors and transmitters on increasingly prosaic items, to the point where they can be included in food packaging and other single use (disposable/recyclable) items.

This makes it possible to include monitoring equipment in a much greater variety of contexts. As measurements are more relevant, they become more valuable. Relevance is related to risk and leverage opportunities. Data that can best inform my future actions to maximize leverage and reduce risk are most valuable to me, and can also be of most value to those who might wish us harm.

1.4 What We Should Expect of IoT?

Trust is earned. A system must be reliable and serve stakeholder needs to be trusted; however, reliability is not enough since something can be reliably harmful. There is not yet a single performance metric that will answer the question for all stakeholders, "is this system measure relevant to my risk and leverage analysis."

As technology has advanced, it has become cheaper to connect devices. It is at the point where it costs only pennies to add radio technology to a device, depending on the range and bandwidth required, therefore manufacturers are making decisions to include these sensor devices, why not? Moore's law in IoT is driving legal and policy that needs to be revisited periodically to refresh to ensure that we are not introducing overlooked harms.

1.5 Death of Secrecy

Privacy was easy when data wasn't connected. The default was privacy. Secrecy is dead or dying with networked information, but privacy doesn't have to die with it. You don't look into other peoples windows and neither should you look in on other's information. The internet of things will challenge our current notions of secrecy and invite us to employ more positive respect in the provision of privacy (not just an accident), and it will also invite us to act with more intention to understand how our actions affect others and future generations. A call for responsibility and maturity.

As networked information technologies have whittled away at secrecy, we have seen privacy and security diminish. This is not, however, inevitable, but rather a result of our continued reliance on approaches to privacy and security that were developed when there was more secrecy. Our risks have changed, but not our risk mitigation strategies. Faced with rapid change, we look to our old institutions for risk mitigation answers, but the institutions stand mute, completely unable to self-adjust to the new risk circumstances.

Public records of divorces have always been available in county records, but putting them online makes them more accessible. Zillow showed house prices, and

contemporary articles talked about privacy intrusions, even though it's public information [2]. One person's intrusion becomes another's insight.

Previously, it was easy to tell if you were "producing" data. With IoT, your participation in the data production process will be less obvious to you. So, how do you know if you are protected from harms? How do you know if someone is intruding on your privacy? Publishing private facts? Defaming reputation? Those are traditional torts. What about new emerging harms? The authors assert that expansion of IoT suggests further demise of secrecy.

The challenge is that data is a dual use technology. It can be used for good or ill. In fact, there are situations in which one party's good is another's bad. When institutions can better tell who you are, that can be both intrusive and empowering depending on how the insight is used by the institution.

1.6 Leverage, Privacy and Security Enhanced or Hindered by IoT?

The question is how can those data flows be rendered reliable? One approach is to render the data non-existent by collection and right-to-be-forgotten type limitations, but these ignore the fundamental value proposition of greater insight that we all enjoy and will seek. They are nostalgic strategies that seek to preserve the type of privacy that was an artifact of accidental secrecy, but which is now dead in the era of networking and ubiquitous simultaneous data collection.

We are information seeking-beings. Every day we seek high quality information on which we can rely. Much of that information involves the current behavior of others. Traffic reports are not useful if we only know about 50 % of the cars, predictions of energy use are not useful if only know about 50 % of houses. Thus we need to have a balance between knowing and not.

It is possible to measure your fuel use directly, but to measure it relative to others, the data about your use has to be compared to that of others. Many communities' energy providers have already had programs through which people are informed about their energy use with others. The latter intrusion is the reason to consider who is handling data about you. Who do you trust, an entity with power with which your interests align, or an entity with medium market power and therefore limited resources to compete reliably.

When a third party is involved, the concept of trust arises. How can you be sure that the insights gathered for you won't be used in ways that harm you?

Giving the system 1000 eyes could be seen as extending neighborhood watch to all of those artificial eyes, thus increasing security. One could see if any part of the system is acting unreliably such as gas leaks, or electricity blackouts, etc. that could be detected quickly. This could help us build more robust systems—thus increasing trust and therefore security. However, these effects are as yet accidental and not designed in. Security and privacy are accidental outcomes in these scenarios.

1.7 The Intimacy of the Grid

As early as 1997, work was being done on computing and emotions. An example is the work of Rosalind Picard at MIT [3]. Reliability and predictability of response enables us to make emotional connections with machines. We want to trust the environmental controls on which we depend. We benefit physically and emotionally if those systems are more reliable and predictable. Thermostats are heat and needed for comfort and survival is a good example. How do we consciously design in the emotional affectiveness of reliability and predictability in this new world of IoT?

1.8 New Forms of Leverage Emerging

What will default structures be for new data and information systems? Systems to date are just baby steps toward a new world of ubiquitous information at all levels. That world is driven by the desire to monetize through advertising, but we don't need to just apply direct monetization rules to all data use. Many uses are not monetized like data that support epidemiology or understanding of social issues.

New possibilities include carbon footprint data for better insight into your energy use which will give better insight into energy use alternatives and better insight into energy use by you relative to others. But that information could also be used to affect your costs—how much you may be allowed to use in the future or what you may pay for fuel. Perhaps you may be compelled to lower your consumption by having an external authority directly lower the thermostat. On the positive side, to lower costs of what you pay, you need to empower the supply chain that feeds you energy. This could enable a local utility to purchase more effectively if they know your pattern of use, creating a benefit to both you and the utility, but it should require your cooperation.

Data about your fuel use is already mixed with data about all use of your fuel supplier. You appear as a part of the gallon purchase by your fuel supplier, and his wholesaler, and how much is produced by APEC. With greater data availability, you will be able to distinguish your use and your impact on the supplier.

2 Risk in the Age of the IOT

2.1 A. New Environment New Risk

Thermostats control local environment against risks from the temperature environment. We have new environments now and new risks. What is the nature of the feedback needed in this information environment? Privacy and security can be viewed as the absence of reliability. Unreliable electricity is a blackout. Unreliable water is a flooded basement. Data is not yet sufficiently boring to be considered reliable. In fact, we don't even have ways to measure reliability of its flows. We need to make data boring – like a thermostat.

2.2 Trust and Individual Outsourcing

This is a time of tremendous distribution of outsourcing causing us to trade new risks for old. Just as businesses once did their own shipping, payroll, tax preparation, data processing, airline reservations. They now outsource those tasks to networks of third party service providers. Individuals also "outsource" those functions to new third party networks on which they depend. We once used travel agents, now we book travel online; we once did our own taxes but now a majority outsource that function to a third party. This opens us up to new risk exposure and proliferation of information about us.

2.3 New Information Risks

With transition to digital, our risks are increasing, so that they include not just physical risk, but also information risk. There was a time when your money could only be stolen in a robbery of your person or your bank by theft of cash or valuables deposited, usually through use of the instrumentality of physical threat of a gun or knife, now data theft is the instrumentality of choice to enable monetary theft with zero physical threat. In this sense, robbery has become different. It is arguably safer for victims with reduced threat of violence, but it is more difficult to detect online and no less economically harmful.

2.4 Exponential Growth of Data

Not only has information become more important, it is also more available as the price of sensors and of networking sensors together have decreased. The rate of capacity of global information collection, transfer and storage has been said to be increasing exponentially [4]. The Internet of Things (IoT) is a concept that is meant to anticipate the emerging setting where the many devices and objects with which we interact can be given a sensory capacity and an actuator capacity to capture and transmit (and sometimes process) data about their environment. Where that environment includes humans, a portion of that data will be "about" that human activity. We need to include in our design conceptualizations that privacy considerations should factor into any application.

2.5 New Responsibilities

Individuals and organizations won't voluntarily assume additional costs unless there are clear benefits. We have an example with the environmental movement and how long it has taken for recycling and limiting energy consumption limitation to become emerging norms that affect behavior beyond mere market or monetary considerations. Individuals now will pay more for green power and organic foods, will spend time and effort to sort their recycling, will turn down their thermostats at night or when out of the house, and purchase fuel efficient cars in a blend of reactions to non-considerations. Similarly, we need to raise awareness of IoT privacy concerns similarly to encourage

new behaviors and responsibilities on the part of both individuals and the organizations collecting data.

2.6 IoT Increases Outside Risk by Raising Number of Interactions

Interaction volume is increasing rapidly with IoT. Interactions are indirect since "things" don't exercise discretion, but are programmed, semi-autonomous automatic systems. In the past two decades, technology advances have caused our information environments to become richer, as higher connection speeds and tech have lowered prices, enabling the placement of processing and sensor technologies at increasingly smaller scales. We all benefit from these advances, and all have had to adjust to the implications of being increasingly monitored and observed.

True that data an enormous pile of data is now available to big search engines like Google that can mine for correlation, creating new and increasingly intrusive information, but at least having it in one place better enables audit than if it were in a million places. Like AT&T in 1960's, some natural monopoly is emerging which usually invites regulation. While regulation to preserve privacy may be needed, careful consideration must be given in design because initial reactions to block information flies in the face of creating valuable insights that individuals may wish to have. As stated earlier, a balance must be found between insight and intrusiveness when designing a regulatory regime.

2.7 Interactions Breed Risks and Requires Metrics

We all have more interactions and more perceived risk than ever. Every one of us has this problem, all people and institutions have security challenges, privacy challenges, and unknown risk, cost and liability challenges with IoT. The key is how to create metrics that might provide meaningful ability to measure the level of trust in a system and look to measures of identity integrity.

What is identity integrity? In the physical world, I can recognize my body, my family members, my possessions, my car, my house and other physical objects that are recognized to be within "my control." That is more difficult with intangibles. I own shares of stock of corporation X, I cannot present myself at their office and ask to take home a desk or some office paper—these don't belong to me even though I may "own" a portion of the company. In fact, being a shareholder doesn't even give me a right to be present in their office without permission. Stock rights are specific intangible rights, carefully described under law, regulation and private contract.

Consider the recent headlines describing privacy breaches and harms [5]. Each is a breach of either an input or output channel, in other words an expressive or perceptual channels. When think of it this way we may be able to discover some means of providing tangibility to our personal intangible information. It exists somewhere and is subject to being bounded in some way. This is just the beginning of teasing out the nature of our data presence that will eventually be subject to similar laws, regulation

and private contracts that take into account the new nature of the risks and benefits associated with IoT; however, we are a long way from that enlightened view.

3 Solutions

3.1 Privacy is an Operations Problem in IoT Solved with Operational Approaches

How can an individual possibly act to achieve privacy in the context we have just described? How can a company or government protect its interests? By focusing on the actions of privacy and security—seeing them as operations problems–we can design, develop and deploy systems that give greater privacy and security. Consider that all privacy and security violations involve a breach of the input or output channel for data. Reflecting Nissenbaum's contextual appropriateness and distribution norms [6]. While individual and company "calibrations" of these channels may differ, they do so by degree not of kind. If we can deliver channel integrity, we take care of the emergency phenomenon of privacy and security. To do so requires employing reliable systems. Those systems are composed of equipment, software and entities (individuals and organizations) that must be chosen wisely for their ability to take on responsibility to achieve privacy and security expectations. For equipment and software, seek reliability. For entities, seek reliability.

A reliable operator will render service predictable. The big data players have a stake in terms of money and regulation; we can leverage their self-interest to achieve reliability. Do you want a bit player or a significant player to handle your data? The risks are mostly from unauthorized use. Most companies have an interest in preventing unauthorized use in order to deliver reliable services to their B2B and B2D customers. If there is a problem, who can best negotiate with the government, you or the company? Who can best negotiate with another company – you or the company?

3.2 Create a DMZ for Security. Render Externality Innocuous

Sharing information is not a binary issue, not an "either/or." There are myriad levels of sharing in different contexts. As a result, information can be shared in more or less privacy preserving ways. For example, feedback relative information to you on your energy use relative to neighbors, without revealing their identities, and vice versa. This would inform you and others with minimal intrusion. Considering the challenges of coordinating such a broadly distributed system, there are ways to preserve interests and also achieve sharing goals if design intention is there at the beginning.

3.3 Hoarding and Stewardship. Achieve Interdependence

Expect others to abide by their responsibilities set forth in privacy preserving policies, not only is this the best solution for individuals, it is also the only responsible approach when it comes to scarce resources such as energy. No one person gets to be beyond

regulation if they are using scarce resources. Hoarding is discouraged and stewardship responsibilities are dominant.

3.4 Achieve the Perspective: My Insight is Your Intrusion

Leverage of information is now available to inform interactions which were never available previously. (The authors couldn't discover others with similar views 100 years ago, but not so today.) This benefit to some individuals is perceived as intrusion to others. As we used to say to our kids when they complained about being in traffic: "We are part of their traffic." Similarly, we are other people's privacy problem, and are part of theirs. It is this co-dependency that is the basis for future governance systems. We should adopt a golden rule of data use: "do unto others as you would have them do unto you." More specifically, this raises the issue of co-management of databases for the purposes of social decisions about relative benefits and harms. To date, the discussion has taken place in developing markets, but the law is frequently out of touch with current reality due to the lag in awareness. Solutions exist, but for earlier problems. Terms of service and other Trust Frameworks are in need of continuous evolution in order to address new and emerging problems that were never conceived of at the time of their drafting.

3.5 Markets and Standards

Internet was built on open standards of technology which allows for remote building in conformity with design, affording interoperability among physical technological components. The Internet was a military technology deployed in civilian context, without consideration of the social implications. Now we get to deal with them.

Legal interoperability is now the challenge. What are open legal standards? What are open legal standard-setting processes? Candidate standards vie for adoption by stakeholders, each making an evaluation of worth and costs. As long as costs are known and accepted, then this process of deliberation is fair. The question of that fairness is broadly described as problem of privacy, but it is more than that. Channel integrity is a precursor to legal interoperability.

Legal systems consist of rules creation, operations and enforcement. There are many different rules in different jurisdictions, and there can be many different cultural and traditional legal approaches in these same jurisdictions. Ultimately standardization for reliability will make inroads into rulemaking processes and enforcement preferences, but the initial impact can be most effective in the middle operations elements, the boring parts of the process of rulemaking and enforcement.

Reliable, consistent service delivery is favored in times of rapid change. Large operations offer some stability as a scaffolding for innovation in rulemaking and enforcement/incentives. The large data providers are the candidates for initiating rulemaking. Once seen as passive presenters of whatever data can be imagined and put online, we now see them beginning to propose and implement rule changes [7].

Increasingly we depend on technologies and people in sociotechnical, social machines to deliver needed services. In the book, "Turning Troubles into Problems: Clientization in Human Services, a collection of essays explores how human service professionals, who must deal with a broad list of challenges including at-risk children, adults and the elderly need to construct the troubles of the groups as standard "problems" that can be dealt with by systems to which they are gatekeepers [8]. The essays consider the challenges of the interface between client "troubles" and administrable "problems" with attention to the multiple dynamic elements that require forms of "mass customization" to achieve scale with empathy and compassion in resource-constrained social services:

> Troubles are present across the life course; they are not the exclusive property of any stage of living. In contemporary society, troubles commonly are muddled and undefined until they are subjected to professional scrutiny. The "gaze" of experts transforms them into certifiable conditions, from specific diseases, disabilities, and dysfunctions, to particular crimes and transgressions [9].

Future IoT systems will need to convert troubles into problems to deal with problem resolution at scale. Insight can be gained from these socio-technical solutions that can be adapted to the problems outlined above.

4 New Paradigm Needed

We call for new architectures of mutual altruism in which participants can act selfishly, but benefit others. You and I rely on these systems to be reliable for our personal and business use. That reliability is dependent on the collective reliability of populations to produce useful and valuable information. You and I need to do our parts as data providers and data handlers.

4.1 Transparency is Mutual

If we want companies to be transparent, should we also be transparent with respect to those same issues. The No More campaign suggests that conversations about interpersonal harms should open up [10]. If 'sunlight is a disinfectant,' why doesn't that apply to people's practices online, including privacy issues with ubiquitous IoT data?

4.2 Be a Good Neighbor: Respect the Right to Be Remembered

'Turning Troubles into Problems' in networked systems, there is the right to not be overlooked. Much is made of the right to be forgotten [11], but at the edges of all bell curves of bureaucracy there are vast populations who suffer from having been long since forgotten. They are the human face of the externalization of costs in scaled systems. Their challenge is to be remembered by systems, not forgotten.

4.3 Responsibility: Empirically-Based Stewardship

Wasteful practices hurt everyone, particularly future generations. Nobody is perfect, but it's better to know behavior standards. What gets measured gets done, and, as an example, until we measure our energy consumption practices, we cannot get climate change mitigation "done." It is not the oil companies that are destroying the earth, it is you and me. We are the consumptive part of the energy production-consumption system. If we exclude ourselves from being counted in the global energy use spectrum, we are part of the problem, not part of the solution.

This doesn't mean that privacy is dead, but neither should social responsibility be dead. Plato declared that an engaged citizen is a public resource. In energy, we are citizens of the world, and we can do something about global problems like climate change from each of our living rooms. The inclusion of our thermostats and other IoT are each small contributions to our collective participation. What provides you with more efficacy– your vote in national elections once every couple of years or your daily "vote" by the consumptive decisions you make? That voice cannot be heard in isolation, it can be included in the conversation when you participate in data gathering.

4.4 Markets and Registries as Risk and Rights Mapping Tools

Markets are the place where Terms of Service are subject to critique and adoption. Positive value propositions are embraced, and those that are not favored are not. When Trust Frameworks of multiple entities change over time to accommodate the needs of broad groups of stakeholders, it is comparable to an open, community development process. Consider that safety equipment in vehicles was in response to market and regulatory pressures. There is a chicken and egg argument about which came first, the market innovation or the consumer need, but ultimately it is a feedback process that moves the market forward.

In order to make this happen, the consumer must be provided with information about choices. For products, it is obvious – purple carrots look different than orange carrots; or this new mobile device is larger, therefore better, etc. As more value is developed in information markets, differences are less obvious without an interface. Registries are the place where we can discern difference. Like securities markets, the differences of value in 100 shares of class A common stock of two companies cannot be found in the Delaware corporate law or even the stock instrument issued by the company, but in information about the company's respective earnings potential and other data about its interactions and performance. Trust Frameworks are at the early stages of standardization. Now there are great differences among these frameworks, but they are standardized by some external laws that sculpt things like DMCA provisions, bankruptcy provisions, etc., and some industry practices, for example similar IP licensing language, etc., mostly developed due to the attorney "herd mentality:" when preparing new documents legal advisors look at examples online for models even though a practice still may not yet be broadly standardized.

Standards emerge in markets. Initiatives like NSTIC and a similar EU initiative are directed at seeking to identify candidate best practices in policy and law to inform

future potential standards for deployment in domestic national and global markets [12]. This is a standardization process, but is taking place on the broad scale of global data and identity infrastructures. It is a distributed process that is (frustratingly for countries and companies) not centralized in one place.

Markets are the mechanism and the process for this standardization, and registries and Trust Framework construction tools are important functions to provide for those processes. Registries are where solution discovery, collaboration opportunities and other collaboration and coordination processes take place in loosely coupled system of standard setting. This is the means for addressing the development of practices that will begin to define IoT privacy and security mitigations.

5 Declaration of Interdependence

When our nation was founded, it enshrined its independent coherence through a declaration of independence from the United Kingdom. Our current task is to cohere individuals into responsible communities of interest around issues, such as energy consumption through a declaration of interdependence. Networked information systems are a source of modern problems, and modern solutions. The paradox is resolved when individuals self organize to solve problems, and to help one another. The neighborhood watch has become a model for global citizens to pursue their interests in common with others. Everyone will benefit from greater reliability and less accidental and intentional harm attack which can be the outcome of understanding how interconnected we are and how each of us is responsible for enacting privacy constraints in this new world of IoT. There is no 'other' who can do this for us. It is up to each of us to define ourselves as participants in this new interconnected world and to recognize that we are both demanding consumers and unwitting victims of too much information about us as individuals.

This is not your usual academic paper. It is, instead, a Declaration of Interdependence, which is meant to provide a narrative for the coming Internet of Things. Not everyone is equally enthusiastic about interdependence, but in reality, critics of networks and dependency often ignore the benefits while focusing on the downsides. This narrative seeks to identify paradoxes, which we should knead together until they constitute a balanced approach; that doesn't resolve the paradoxes, but rather accommodates them and taps their risk potential for mutual benefit. While the Internet was designed in the absence of social considerations, the Internet of Things does not have to suffer the same fate. As appetite for more and more information grows, and as more and more personal information is collected, we can get ahead of the consequences by engaging in insightful dialogue about how to define the new rules and tools that we need to exist in this new networked, interdependent world that is being created.

References

1. Cringely, R.X.: Breaking Moore's Law (2014). http://betanews.com/2013/10/15/breaking-moores-law/ (retrieved)
2. Podmolik, M.E.: Know thy neighbor: Zillow adds public data on homes in foreclosure but not yet for sale. Chicago Tribune, 26 October, 2012. http://articles.chicagotribune.com/2012-10-26/business/ct-biz-1026-zillow-20121026_1_zillow-distressed-homes-premarket-inventory (retrieved)
3. Picard, R.: Affective Computing. In: Tatnall, A. (ed.) HC 2013. LNCS, IFIP AICT, vol. 416 (2013)
4. Hilbert, M.: The worlds technological capacity to store, communicate and compute information. Science **332**, 60 (2011)
5. Privacy Rights Clearinghouse. Chronology of Data Breaches Security Breaches 2005-Present. http://www.privacyrights.org/data-breach (retrieved)
6. Nissenbaum, H.: Director Information Law Institute. New York University. http://www.nyu.edu/projects/nissenbaum (retrieved)
7. Debt Advice Foundation. Google to impose Strict New Rules on Short-term Lenders, 13 December, 2012. http://www.debtadvicefoundation.org/news/2012/12/13/google-impose-strict-new-rules-short-term-lenders (retrieved)
8. Gubrium, J., Javinem, M. (eds.): Turning Troubles into Problems: Clientization in Human Services. Routledge Press, New York (2014)
9. Ibid. p.3
10. No More: Together we can end domestic violence & sexual assault. Retrieved at: http://nomore.org/
11. Rosen, J.: The Right to Be Forgotten, Stanford Law Review. Online 88, 13 February, 2012. http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten (retrieved)
12. National Strategy for Trusted Identities in Cyberspace (NSTIC). http://www.nist.gov/nstic/ (retrieved)