PRIVACY, SECURITY, AND LIABILITY ISSUES IN A CONNECTED WORLD

DR. IZHAR HAQ

SCHOOL OF PROFESSIONAL ACCOUNTANCY,
LONG ISLAND UNIVERSITY

- *ORCID: https://orcid.org/0009-0007-1141-6203*
- *Email: izhar.haq@liu.edu*

Izhar Haq is the director of the School of Professional Accountancy at Long Island University. He served as deputy controller at Florida International University for 10 years. He has over 20 years of accounting experience in senior positions in multinational corporations as well as governmental and not-for profit entities and is a consultant for the Oil and Gas Industry as well as start-up incubators in New York. His publications have appeared in *The CPA Journal, Journal of Finance* and *Accounting*, and *Tennessee CPA Journal.*

CO-AUTHORS

Michael Abatemarco
Long Island University
Michael Abatemarco is a professor of accounting, law, and taxation at the School of Professional Accountancy at Long Island University. He is also a practicing tax attorney whose firm is based in Garden City, New York. He articles have appeared in *The CPA Journal, Today's CPA,* and *The Bankruptcy Strategist Journal.*

Ed Weis
Long Island University
Ed Weis is a professor of management at the School of Business at Long Island University. He has a Ph.D. from University of Georgia and a J.D. and a Master of Accounting from University of Tennessee as well as a Graduate Certificate from Harvard University. He has decades of investment banking experience and served as Managing Director of Investment Banking at Merrill Lynch. He has also served as a Dean of Business at Molloy College and Vice President of Academic Affairs at Long Island University.

ABSTRACT

The proliferation of the Internet of Things (IoT) devices has resulted in the generation of enormous amounts of data in a connected world. The technical challenges of dealing with this enormous volume of data is dwarfed by significant privacy, security, and liability concerns. By extending standard models of information disclosure through integrating persuasion and legal aspects, we offer novel insights into the shape of future information technology systems. Specifically, we expect that artificially intelligent machines will allow organizations to decentralize parts of their information technology at the device level. However, such a new approach to a connected world requires careful investigation of these issues. Three case studies are used to analyze privacy and liability issues by employing an information disclosure model.

Keywords
big data, disclosure, information asymmetry, persuasion, privacy, security, liability, artificially intelligent machine, privacy preserving analytics, information system, internet of things, IoT, information technology, connected

INTRODUCTION

Estimates of the potential growth of the Internet of Things (IoT) over the next decade vary considerably in both size and economic impact. At the lower end, Gartner Group estimated that the IoT is expected to grow to more than 30 billion devices by 2020 (Gartner, 2013). Cisco Systems, a global provider of Internet technology, estimated that in 2012 there were 8.7 billion objects connected to the Internet and that by the year 2020 this number could reach 50 billion and would generate US$14 trillion in profits

for the world economy over the next ten years — more than the combined 2011 GDP of the seventeen member countries of the European Union (Rooney, 2013). The rapid emergence of the IoT poses not only technical but also societal and legal challenges. On the technical side, IoT-connected devices will contribute to the ongoing growth of data collected and transmitted (Gubbi et al. 2013). On the legal side, both privacy and liability issues are of concern. Without understanding the implications of deploying and using the IoT, companies and individuals might put themselves at risk of unforeseen exposure.

This study explores whether the emergence of IoT should change the design of information systems in organizations. What are the arguments in favor of or against a new approach to the information systems and what will it look like and what will its basic requirements be? Answers to these questions are important because artificially intelligent (AI) machines, such as smart devices and smart robots, use increasingly more artificial intelligence. Naturally, this leads to the question regarding what role management will play in future organizations and what impact this will have on information technology within and across organizations. We try to answer these questions by advancing a theoretical framework that is founded on information disclosure.

Our model shows that two key developments will likely affect the future of information technology. First, the interaction of humans and machines and the role information technology plays is expected to change as more data is processed and evaluated at the periphery of the organization. We expect information disclosure to become more selective, as too much information might overwhelm managers, and selective information is expected in facilitate decision making processes. A key aspect is how, for example, a smart device can persuade a manager to make an optimal decision by presenting only the most important and relevant information. Second, information technology is expected to serve not only humans but also machines. AI machines are expected to take over certain decision-making tasks from human managers. Third, decentralized information technology can be implemented at the machine level. Hence, in the context of the IoT, it will be possible to combine the roles of manager and information systems at the AI machine-level. Thus, the future direction of information technology offers a departure from traditional design.

There is no doubt that IoT will substantially change how we live and how our economies operate. The only question is how quickly the IoT is going to change how we do things. A standard view is that the IoT connects billions of devices. However, such a high level of connectivity is not sufficient to truly have a profound impact on society and business. Rather, it is the emergence of ever smarter AI machines that will have a profound impact on daily activities and interactions between humans and machines. This is a significant change only comparable to the great industrial revolution that changed how we produced and transported goods. This Internet revolution will affect every aspect of our daily lives, including how we monitor our health, how we drive, how we manage and operate buildings, just to state a few. At the heart of this revolution is not the Internet per se but the intelligent machine or smart device. This machine has built-in processing ability that allows the processing of data or information and, possibly, the execution of certain actions. The functional abilities of the device depend on the hard and soft components the device is built from.

Our work is related to several strands of the literature. Research about the Internet has focused on different aspects of improving electronic services and the underlying infrastructure. On the economic side, the focus has been on the pricing of Internet services (Hosanagar et al. 2008) and the economic benefits of the Internet by decreasing prices (Brown and Goolsbee, 2002), reducing search costs (Bakos, 1997; Sankaranarayanan and Sundararajan, 2010) and shared information goods (Bakos, 1999). Our extended theoretical model of information disclosure is founded on classic work in information economics, particularly that by Akerlof (1970), Spence (1973), and Stiglitz (1975).

The findings of this study suggest that the future information technology is deployed not only in a more decentralized fashion but also at the machine level. This is driven by the deployment of AI machines, such as smart devices and robots, that take over certain roles that have previously been the sole domain of management. Second, analyzing and interpreting data at the machine level has major implications for how we disclose information and how we apply and interpret privacy and liability law. Machines per se are not legal entities and, as such, cannot be liable for their decisions or actions. Hence, either owners or operators will have to assume responsibilities for bad decisions at the machine level. Third, advances in materials science and nanoscience as well as innovations in production processes will

merge human and machine. This will create real challenges for the application of current approval processes for equipment. Artificially intelligent machines in the human body raise not only serious privacy, security and liability issues but also considerable ethical issues.

This study makes three key contributions. First, we contribute to the information systems theory-building literature by developing a theoretical framework in the context of IoT. This framework combines standard arguments from information economics with privacy and liability aspects from legal theory to offer novel insights into the interaction of senders and receivers of information. Importantly, the model shows that when privacy and liability concerns are classified as costs, the value of information disclosure can be reduced. Second, we contribute to the literature on decision making by managers. Specifically, we highlight that AI machines are expected to assume decision-making tasks previously reserved exclusively to human managers. Like human managers, we argue that AI machines will require information systems to solve decision tasks. Third, we contribute to the information technology design literature by moving it to the periphery. We show how the placement at the AI machine-level can mitigate privacy and potential liability concerns of organizations operating within the domain of the IoT and how such information technology can serve both humans and AI machines.

The remainder of the paper is structured as follows. The next section defines the IoT and sets the boundaries for our model. The following section develops the theoretical framework, building on design and agency theories. This section also establishes the framework for the interaction of devices and humans and the role of information systems in it. In addition, it investigates the relationship between information disclosure, privacy issues and liability. This section is followed by three case studies that analyze the various aspects of the theoretical framework developed. This section also offers future directions of research as well as some limitations of the present investigation. The final section concludes the study.

METHODS

This study employs a **conceptual analytical approach** to examine the implications of the Internet of Things for information disclosure, privacy, and liability. Given the emergent and rapidly evolving nature of IoT technologies, the research does not rely on empirical data collection but instead focuses on theory development and analytical reasoning.

The analysis is based on the construction of a **theoretical framework** that models information disclosure between interacting entities, including humans and artificially intelligent machines. The framework abstracts from specific technologies and organizational settings in order to identify general mechanisms governing information granularity, selectivity, and associated costs. Privacy and liability considerations are incorporated as constraints that influence the value and desirability of information disclosure.

To explore the applicability of the framework across different contexts, the study uses **illustrative case analyses** drawn from typical IoT application domains. These cases serve to demonstrate how decentralized, machine-level information systems can affect decision-making processes and mitigate or amplify privacy and liability risks. The cases are used analytically rather than empirically and are intended to highlight patterns and implications rather than to provide statistical generalization.

Overall, the methodological approach emphasizes abstraction, internal consistency, and analytical clarity, with the goal of generating insights that can inform future empirical research and the design of information systems in IoT environments.

IOT IN CONTEXT

The IoT is a newly emerging technology and, as such, is a concept that is still being defined. It has been described as "fuzzy" and "fragmented" with a "complexity that is not bounded by geographical, political, administrative or cultural borders" (Golling and Stelte, 2011). The first use of the term "Internet of Things" is generally attributed to Kevin Ashton, the Director of the MIT Auto-ID Center, who referenced it in a presentation he delivered to Procter & Gamble in 1999 (Ashton, 2009). The International Telecommunications Union (ITU) subsequently legitimized the term when they published the first report on the topic, entitled "The Internet of Things," in November 2005 (Santucci 2010). The phrase was recently adopted as a "new word" in the Oxford English Dictionary in August 2013, where it was defined as "noun — a proposed development of the Internet in which everyday

objects have network connectivity, allowing them to send and receive data (Oxford, 2013)."

The combination of IoT-enabled devices and telecommunications technologies is allowing the bridging of "objects" or "things" in the physical world, such as furniture and appliances, to the virtual world of databases and software applications. It can also facilitate the exchange of information between objects, including machine-to-machine (M2M), machine-to-human (M2H), machine-to-human-to-machine (M2H2M), and human-to-human (H2H) (Tan and Wang, 2010). Future MIS will see a shift in the interaction between these parties where machines transgress to AI machines or devices. While a "machine" can be a device in the form of sophisticated sensors (Kendall and Kendall, 1993), an AI machine is a device that in fact uses algorithms with artificial intelligence to analyze data. Unless otherwise specified, "machine" in this article refers to the latter — AI machine. Such a device is, as such, independently able to produce some type of information, and while it may presently be described as lacking sophistication in the information that a human can generate, it is only a matter of time before this can in fact be achieved. Language is illustrative of this point — raw data are akin to words. Stringing together a meaningful sentence and sending it to another party requires a degree of artificial intelligence. Using complex algorithms, AI machines have already managed to speak sentences (e.g., natural voice creation, such as AT&T Natural Voices™ and Acapela Voice Factory). It will be increasingly difficult to differentiate between human and machine. Increasingly, data that are being collected through these interactions are being analyzed using new "big data" analytic software (Chen, Chiang and Storey, 2012). In addition to aiding human planning and decision-making, it also raises major concerns about social issues including privacy, security, and liability issues precipitated by the use of the data.

Inherent in the concept of the IoT is the understanding that objects will need to be connected and able to communicate via the Internet. To do this, the objects will have to be uniquely identified using an assigned Internet Protocol (IP) address. By the introduction of the IPv6 standard, for example, the IoT can become enormous, and it is no longer limited by a lack of Internet addresses. Global standards need to be established to allow complete connectivity or "interoperability" among devices to completely achieve the "ubiquitous" or "pervasive" network envisioned under the concept of the Io T.

Like the current Internet, the future IoT will be self-configuring and ever evolving. This means that, like current personal computers, many worldwide users will purchase and deploy new IoT-enabled devices daily, and many of these devices will be mobile — popping up and disappearing from the network — similar to laptops and iPads at Starbucks around the world today. When IoT-enabled objects become connected to the Internet and can share their information with other Internet-connected objects, they become endowed with a certain level of intelligence and are subsequently often referred to as "smart" objects or devices. We discuss these and other smart devices as well as their potential societal benefits and costs in greater detail below.

In June 2013, The Economist Intelligence Unit surveyed 779 senior business leaders and established an IoT business index (The Economist, 2013). The results of the survey showed that over three-quarters of companies are either actively exploring or using the IoT and that three years from now, almost all respondents (96%) expect their businesses to be using the IoT in some respect. However, if business leaders see the IoT as such as an important development, should there be concern about what information technology looks like? Specifically, should information systems experts and scholars be concerned about this change?

There are some skeptics. For example, Robin Duke-Woolley, CEO of Beecham Research, noted in December 2012 that the "Growth rate projections are often far too high for what is essentially a solutions business, not a consumer products business…The forecast errors for these are potentially huge" (Cowan, 2012). Subsequently, in July 2013, Ben Rooney, a tech columnist for the Wall Street Journal, in an article entitled "Internet of Things Poses Big Questions," analyzed both IoT's short-term concerns and long-term potential. He quoted one source as saying "The hype that is going around about IoT at the moment feels incredibly similar to the hype approximately 2000" (referring to the first dot-com boom and collapse) but then goes on to note that the "IoT was most likely another example of Amara's Law: We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run" (Rooney, 2013).

Despite these concerns, many political leaders have embraced the IoT and view its potential for social development and economic growth in a positive light. At the same time, they express caution regarding the impact of big data and analytics through the excessive use of IoT-connected devices on national security. In June 2010, the European Parliament officially endorsed the development of the IoT and called on the European Commission (EC) to "secure co-financing for the implementation of these technologies" and "continue funding pilot projects" (EU Commission Task Force, 2010).

While encouraging IoT development, the resolution also directed the EC to perform an exhaustive survey of the effects of this technology on "health, privacy and data protection" to ensure that they collect EU citizen input on possible public policy concerns (EU Commission Task Force, 2010). One way to address these concerns is to investigate how AI machines could be used to mitigate these concerns and how this would affect the design of future MIS. Complex systems can sometimes also be highly connected, enabling the sharing of information and the distribution of power. In political decision-making environments, such phenomena can allow more people at lower levels of society to participate in the policy making process. This can be good because it can strengthen system resilience; however, it can also increase societal complexity and raise questionable legal consequences related to privacy, security and liability. Finally, complex systems are self-organizing, meaning that no entity designs or controls it, and the system can autonomously adapt to changing conditions (Geyer and Rihani, 2010).

In a public policy and regulatory context, complex systems have several positive attributes. Their connectivity and self-organizing characteristics that facilitate information sharing can help improve situational awareness and problem solving (Lier, 2013). Through emergence and coevolution, complex systems can also foster innovation by bringing together information and ideas and creating unexpected positive outputs. On the negative side, complex systems can disseminate false information and can result in leadership overload with too much unfiltered information complicating the policy making process. This can lead to policy ambiguity, feeding public uncertainty and anxiety about the future.

There are several tools and techniques that complexity scientists use to test their theories (Lewin, 2000). These tools include agent-based modeling, network analysis, data mining, scenario modeling, and sensitivity analysis. In many ways, the IoT is the perfect metaphor for complexity theory. As described, the IoT is a network system composed of many parts. It is an emerging technology that will self-organize, grow and evolve over the next few years, likely creating new innovations and leaving unexpected consequences in its wake. Furthermore, its evolution and growth will be closely tied to similarly complex political and economic systems, resulting in potential risks and complicated policy issues, which will be discussed in the next section. Anticipated societal rewards and possible unanticipated consequences will also be described below.

RESULTS AND DISCUSSION

Theory

In theory, the Internet can be defined as an artifact (Orlikowski and Iancono, 2001; Benbasat and Zmud, 2003), as it is at the intersection of "physical objects and human knowledge" (Gregor and Jones, 2007). The design of a new MIS requires a better understanding of the interaction of technological systems and social systems (Lee, 2001). The theoretical model is presented in Figure 1. The theoretical framework is prescriptive, and as such, it is a special predictive case (Gregor 2006). It consists of three building blocks: (1) the foundations of information disclosure; (2) persuasion and information disclosure; (3) and legal aspects of information disclosure.

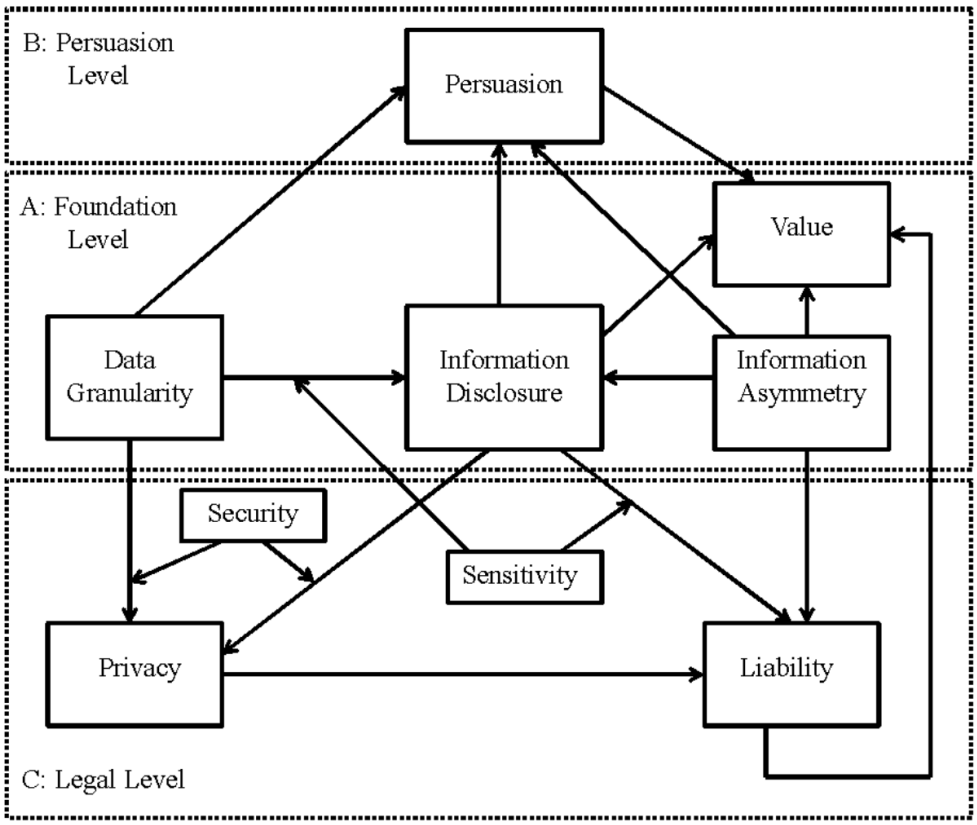

Figure 1: Theoretical Framework of Information Disclosure

Foundations of Information Disclosure

At the center of our model lies information disclosure (see Figure 1, region A). In the IoT, data are collected via sensors or devices operated by humans. Information disclosure can occur in two ways: (1) as raw data or (2) as processed data that have been transformed into information. This information is organized and structured and helps the manager in the decision-making process. The information-economic perspective helps in understanding the value of the information disclosed that has been transmitted from the sender to the receiver. For decision making, the fineness theorem by Blackwell states that more information, i.e., information with greater granularity, is at least worth as much as the subset of this set of information (Marschak and Radner, 1972). In economics, the theorem plays an important role in agency problems and situations with asymmetric information (Akerlof, 1970; Spence, 1973; Stiglitz, 1975). In our model, greater information asymmetry between the sender and the receiver reduces value. The sender can deliberately send a wrong signal, which reduces the value of the information for the receiver.

Persuasion and Information Disclosure

The sender can overwhelm the receiver by disclosing too much information. Although this information is more valuable than less information, it might be difficult to find the relevant information to effectively solve a problem. One way to possibly overcome this issue is by persuasion (see Figure 1, region B) (Rayo and Segal, 2010). Until now, this strand of research has only investigated situations where there is symmetric information between sender and receiver. Under certain conditions, a sender can persuade a receiver in a fashion that solely benefits the sender (Kamenica and Gentzkow, 2011). Interestingly, this work also shows that full information disclosure is optimal in some situations, whereas no disclosure is optimal in other situations. In the context of the IoT, interactions between machines, i.e., M2M, are likely symmetric, as machines cannot be dishonest per se. Interactions involving humans are likely

asymmetric. At the heart of persuasion lies the idea of selective information disclosure.

Legal Aspects of Information Disclosure

It is important to recognize that Blackwell's fineness theorem is only valid provided a set of assumptions are fulfilled. An obvious restriction is costs. Collecting data with a finer granularity is a costly exercise and, thus, must be subtracted as a cost from the value of such information. Note that we do not specify who ultimately benefits from the value of such information. The reason for this is that who shares in the value is context dependent. Often, this is the receiver, but it is also possible that the sender or a third-party will benefit from the disclosure of information. Similarly, privacy will indirectly affect the value of disclosed information, whereas liability will directly affect it (see Figure 1, region C). Both can be interpreted as a cost and, as such, will reduce the benefit of information disclosure. Privacy concerns are mitigated by the level of sensitivity of the information disclosed. The accidental release of less-sensitive information is unproblematic. However, the unintended disclosure of sensitive information can result in serious liability exposure.

Implications for the Future Shape of Information Systems

The greater number of human and machine interactions is expected to have profound implications for the design of future information systems. Traditionally, one question was whether the information technology departments should be organized in a more centralized or decentralized fashion. The interaction between humans and machines, and particularly the interaction between managers and machines, opens future possibilities. Is it still meaningful to design information systems to serve the management? Or should the future design be shaped in a way that it also better serves ever more AI machines? We believe that substantial technological advances will create a need for future information systems that serve both human managers and AI machines.

What role does information systems play at the machine level? Just as the information technology department supports the decision-making process of the manager, it is similarly expected to support AI machines. Consider a situation of a network of smart sensors. Each smart sensor, though tiny, can boast powerful processing for analyzing data and creating information. Based on the outcome of the analysis performed by the localized information system, the smart sensor can then decide what to do with the information. For example, the information can be sent to other machines, be it sensors or robots or, alternatively, humans. Why do we advocate such a localized information system? In practice, large sensor networks have frequently failed to fully meet the objectives as set out before deployment. For example, smoke detectors often trigger false alarms. A smart sensor system with localized information system can communicate effectively between devices and reach certain conclusions and decisions without requiring interaction with a human. Again, using above example, one reason for a false alarm could be a malfunctioning sensor. Naturally, a sensor network of "dumb" devices cannot self-heal. A smart sensor network could instead analyze the data and then solve the problem by ordering a replacement device. Although intelligent machines will be able to compete with human managers in many aspects, for the foreseeable future, certain areas will remain the domain of the manager. Most importantly, managers should continue to have an edge in asking good questions (Dewhurst and Willmott, 2014). In the following section, we discuss aspects of the third level of our theoretical framework of information disclosure within the future of information technology.

EMERGENCE OF LEGAL ISSUES IN SMART DEVICES

The IoT is an emerging complex system with the potential to produce many innovations but that also has unforeseen policy consequences. Politicians, academics, and business leaders around the world — particularly in Europe and the United States — are now debating the potential policy impacts, with most of the initial discussion focusing on three contentious and competing issues: privacy, security and liability.

Privacy Risks and the IoT

Privacy is already a public policy issue with the existing Internet, and much of the current IoT privacy debate looks at the possibility (or probability) that the sheer size and ubiquitous nature of the IoT will transmogrify the problems, heightening the issue by orders of magnitude (Chen, Chiang and Storey, 2012). The IoT offers the prospect that an enormous amount of personal data can be

collected and processed (Fleisch and Mattern, 2005). However, most of the data collected by the IoT will not be of a personal nature. Currently, most sensors operate in remote locations with little or no interaction with people. Furthermore, people often freely provide their personal information in exchange for perceived benefits or information and with the belief that their personal data are protected from unwanted viewing through privacy screen settings.

Two key issues at the core of the privacy debate include the following: 1) the desire of an individual to conceal or keep secret private information and 2) the use of private information after it is collected (Weber, 2009; Weber, 2010). As will be explained, this (the misuse — either accidental or intentional) is closely connected with liability issues.

When considering the desire to keep private data secret, a key consideration is the *context* in which data may be collected. For example, most people expect privacy in their homes, and there are special privacy expectations regarding information about our health, finances, and our families, especially children. Societal expectations are guided by judicial rulings, which are supposedly guided by societal expectations, which in turn are guided by judicial rulings, and so on (Harper, 2008; Rosen, 2001). In the United States, there are current laws protecting the privacy of health data (Health Insurance Portability and Accountability Act of 1996 or HIPAA), financial data (The Right to Financial Privacy Act of 1978), and children (Child Online Privacy Protection Act of 1998 or COPPA). However, there are some instances where people are unaware that they are being scanned, for example, through hidden surveillance equipment or by RFID tags attached to store purchases (Mayer, 2009).

There are also privacy concerns about the amount of collected data, its relevance, and where and how long it is stored. With the existing Internet, there are many instances where databases are hacked, identities are stolen, and personal data are sold to third parties and reused without consumer knowledge. Most privacy advocates believe that only the minimum relevant amount of data should be collected for legitimate purposes to serve a specific need (data proportionality) and that data should be erased after a reasonable amount of time (data minimization). Privacy advocates also believe that most data should be anonymized so that it cannot be tied directly to an individual (Pattison, 2013). There is special concern that if data are not anonymized, then they could potentially be used to track specific individuals while being linked to information in other databases and possibly used to predict future behavior. This could lead to social profiling (CDD, 2013), such as barring a person with a low credit score from entering a store; social sorting (Miller and Kearns, 2012), where different individuals or groups receive access to unequal opportunities; and changes in relative power between retailers and consumers. Despite these privacy aspirations, the sheer volume of data and the way it is stored make it unclear whether the data can ever truly be erased or made completely unidentifiable.

In addition to data minimization and anonymization, there are other proposed recommendations regarding privacy controls. This includes requiring consumer consent before data collection and having companies implement "privacy by design" (PbD), which would build privacy controls into IoT-enabled devices so that they can be shut off or disabled by consumers who do not want to be scanned. The suggestion has also been made that companies be subjected to data privacy audits to ensure that consumer data is being properly handled. There is also a general feeling that consumers have a right data transparency — knowledge of what personal information is collected and how it is used (Kingsley, 2013).

In response to these concerns, companies involved in the design and future production of IoT hardware and software are currently lobbying for the ability to self-regulate product privacy. The concern is that privacy regulation could stifle IoT innovation. They have organized cooperative industry efforts such as the Future Privacy Forum (FPF) and have proposed the implementation of a privacy seal program based upon a fundamental set of privacy principles. However, regulation of privacy is still a major concern in both Europe and the U. S. Under the concept of data sovereignty, information that is stored in digital format is subject to the laws of the country in which it is located.

The issue of privacy was further exacerbated during the summer 2013 with the release of National Security Agency (NSA) documents by Edward Snowden on PRISM, a clandestine mass electronic surveillance data mining operation begun by the NSA in 2007. The electronic surveillance, which included monitoring the phone, email, and other communications of both U.S. citizens and foreign nationals, highlights the complex policy relationship between the desire for individual privacy and the need for public security.

Security Risks and the IoT

Security is another serious IoT policy issue that transcends the individual to include small companies and corporations, municipalities, critical infrastructure, and national security threats. Such threats exist with the current Internet but are expected to be exacerbated by the IoT convergence of the physical and cyber worlds and the exponential increase in the number of objects potentially vulnerable to attack (Ning, Liu and Yang, 2013).

This problem, it is posited, stems from a disconnect related to security and privacy between electronic and mechanical engineers who design the machines or devices, on the one hand, and the communication engineers who connect and integrate those devices to the IoT, on the other hand. Figure 2 illustrates this diagrammatically.

This lack of communication is also often an issue between software and hardware engineers. This can be managed well, but it requires that rules of consistency be followed to ensure internal integrity of the processes. Windows XP is illustrative of this point. Microsoft is obsoleting XP, and upgrading the operating system software on an existing computer is usually not an option. It is necessary to purchase new hardware. Potentially, all devices belonging to the IoT will have the same issue. A smart vehicle, for example, in perfect mechanical condition will become unusable because it is an older model, and a software patch will not load.

Therefore, security must be engineered early in the development of Internet-connected devices; "bolt-on" security after the fact does not work. Consider our network-connected medical devices. Many of these have never undergone a serious security evaluation. Stemming from this is the issue of privacy. For a transit system to work, for example, traffic routers must track the starting location, route, and destination of every vehicle on the road. Alarming implications for privacy result if the data are not properly protected.

As with today's Internet, there are many ways to compromise IoT systems, components and services. First, as noted in the introduction, the IoT can be hacked. One journalist attending the 2013 Black Hat Conference forecast that IoT

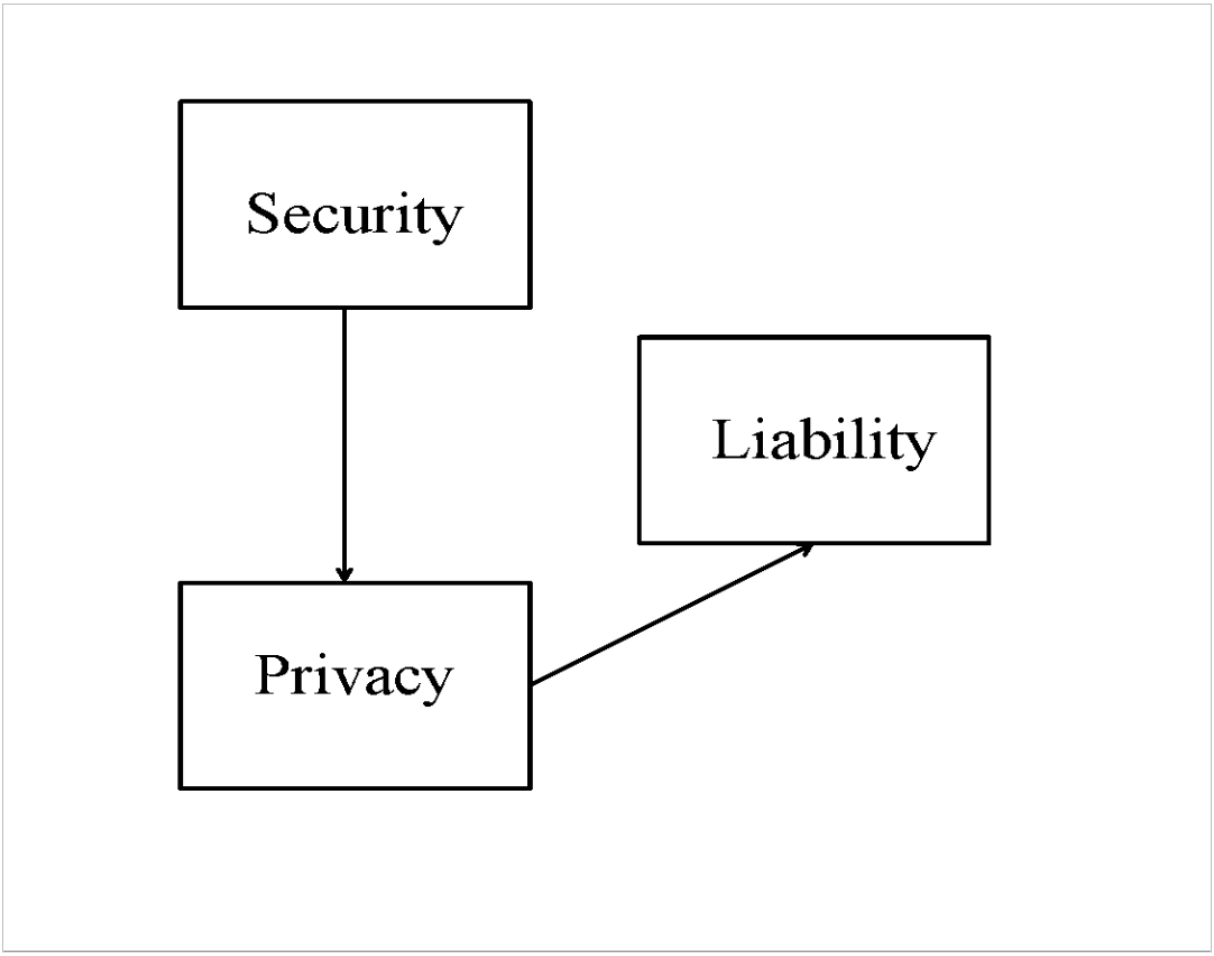

Figure 2: Interrelationship between Legal Issues in the IoT and MIS

and "thing hacking" would produce its own conference in the coming years (Lundquist, 2013). One revelation that has come to light is that vulnerable "things" on the Internet are very easy to find. There is a search engine called "Shodan" (www.shodanhq.com) that can be used to expose over 500 million things that are "carelessly" connected to the web, including (as quoted on their homepage) "webcams, routers, power plants, iPhones, wind turbines, refrigerators, and VoIP phones." Once hacked, data can be compromised, or software can be infected with malware or viruses. Furthermore, hacking can give an intruder access to other components of the system, creating local service disruptions or system-wide outages.

In April 2008, the National Intelligence Council (NIC), part of the Office of the Director of National Intelligence, released a report entitled "Disruptive Civil Technologies: Six Technologies with Potential Impacts on US Interests out to 2025." The report, prepared by SRI, stated that "Popular demand combined with technology advances could drive widespread diffusion of an IoT that could, similar to the present Internet, contribute invaluably to our economy." However, it then goes on to note that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date" (SRI Consulting, 2008).

Therefore, the more sensitive the information transmitted through the IoT, the more problematic it becomes. To address this problem, more critical processing can be done at the AI level to only send the relevant information that can be in a desensitized format. The key objective is that the right message be sent to the receiver while simultaneously utilizing the function of AI machines to undertake a large part of the process.

There are many ways to protect IoT data security. Like some privacy situations, not all data and IoT systems will be sensitive, requiring elaborate security protection. For data and systems that do require security, technical solutions are being developed to protect the confidentiality, integrity and access to sensitive systems and data. Additionally, like privacy, it is posited that there is a need for global security standards and government regulation. Some groups and government officials (including in the United States, the United Kingdom and Germany) are now, in fact, advocating for security-by-design (SbD), where manufacturers are required to build prescribed security features into their IoT devices. Such prescribed security requirements would, no doubt, be very costly to implement. The IoT is still in its infancy, with many innovative applications still on the virtual drawing board. Thus, any attempts at regulation today could have repercussions concerning the way IoT devices, particularly AI machines, and applications evolve in the future.

Granularity, Security, Privacy and Liability

As outlined in Figure 2, understanding this nexus between Privacy and Security and Privacy and Liability provides an added understanding of the *cost* and respective *value* of information disclosed between users (sender and direct receivers) and third parties (indirect receivers). As mentioned above, **collecting data with a finer granularity is a costly exercise and needs to be subtracted as a cost from the value of such information. The beneficiary of the value of such information is dependent on the context or reason it is obtained.**

Existing scholarship has mostly assumed away the cost of generating more granular information — the cost of fineness of information. For example, if we have greater segmentation of data and information and face the same decision, then this information is worth at least as much as if we had less-detailed information. However, such a statement ignores costs. If we want finer information, we must accept greater costs. These costs may be physical, for example, the need for a greater sensor network, but they may also be legal. Along with this comes other issues regarding privacy of individuals, organizations, and considerations about the implications of liability, especially regarding who (i.e., which entity would be responsible), what, and how.

The issue of privacy will indirectly affect the value of disclosed information, whereas liability will directly affect this value. While both can be interpreted as a cost and, as such, will reduce the benefit of information disclosure, privacy concerns are offset by the level of sensitivity of the information disclosed. Thus, while the accidental release of less-sensitive information is unproblematic, the unintended disclosure of sensitive information can result in serious liability exposure. These observations and relationships are represented below.

It is posited that the assessment of "value" to a *user* (who is the provider of the information) is directly connected with liability issues. An assessment of "high" value to a user would mean there are higher liability issues linked to the information and, therefore, potentially greater costs

associated with security. Meanwhile, an assessment of the value to a third party would stem directly from the benefit derived from information disclosure and, therefore, information availability. If we have more information (or less information asymmetry), then there is greater value for the receiving party. However, this is a simplified version of the argument because it does not account for costs — particularly indirect costs through unforeseen adverse legal outcomes.

What, then, is the nexus between Granularity and Privacy to Liability? The IoT is not a question of *if,* but of *when*. It is likely to result in a fundamental change of the function and role of information systems in that the future will serve not only humans but also machines. This is no doubt a fundamental matter that informs decision-making in a business context. Presently, there exists a multitude of technologies, yet the full extent of capabilities in a networking sense has not yet been utilized, which leads to process inefficiency. Consider the replacement of a defective smoke detector in an office, which is delayed by a human manager due to time constraints. Machines can assume an important role. A smart device could instead be utilized to determine that a device next to it does not work properly and to order a replacement device. The new information system expands from human to machine by placing it close to the machine such that the machine, in part, becomes a manager. This precipitates consideration about the liability of a non-human manager (i.e., an AI machine), as discussed below.

Liability and the IoT

Liability issues are related to physical items and to the underlying data (or information). Three questions must be asked: First, who owns the data, and can ownership be assumed by something other than a "human" entity? The question concerns product liability in the context of the IoT and whether the law of torts is sufficient to address future issues in the new information systems. The third question concerns the degree to which the law of contracts can mitigate the liability of operators or receivers of data (or information), whether the interaction (of sender and receiver) be human to machine (H2M), machine to machine (M2M), AI machine to AI machine ($M_{AI}2M_{AI}$), or machine to human (M2H). As previously mentioned, the new information system requires the use of AI machines. Problematic areas from a privacy and liability perspective are essentially any connections that involve M_{AI}.

Traditionally, the roles of managers and information management have been assumed by two separate entities. However, under the new information systems, although it is not necessary, it is possible to merge the role of manager and information technology at the machine level. The reason is that we expect the machine itself to be increasingly more involved in the actual decision-making process by using ever more sophisticated AI algorithms. As such, it also makes it possible to place these "mini" information systems directly on the AI machine. Naturally, at this point, an understanding of managerial and information technology roles is not very clear, and we believe this is going to be a key area of research in the future. One of the things we see as a potential benefit is that the merging of roles could potentially help contribute to privacy preserving analytics because it will no longer make it necessary to disclose highly personal or private data (or information) to unintended receivers. One can also see that data at the local level is stored in an encrypted fashion, which would also help mitigate privacy and security concerns.

Data Ownership: The issue of data ownership is of central importance in the Io T. Information ownership, as opposed to data ownership, has been explored in the context of cloud computing and cloud storage (Gasser 2014). Specifically, the liability for data misuse is traced back to a legal entity (i.e., human or corporate entity). However, because data is increasingly created and processed by machines, the issue of liability of data — including its misuse *by* a device and *because* of a device — becomes somewhat murky.

Vehicle self-navigation systems are a case in point. For self-navigation to work, cars need to be connected in various ways so that safe navigation of vehicles on streets is achieved. Such connected cars are fitted with complex self-navigation systems. Such a system boasts several sensors that generate data and that can send basic data about the performance of a car and potential defects to the original equipment manufacturers (OEMs) before they materialize (White, 2013; NHTSA, 2013). However, this raises the question of whether the car owner can always preclude third parties such as OEMs, car shops and others from accessing the data generated by those sensors, as the data belongs to the owner of connected cars once the sale of that vehicle has been completed.

An alternative view may be that OEMs can find arguments for having obtained database rights in the data because of the investment they have made or that they have retained ownership in data-generating devices in the car that they might have specifically excluded from the sale at the time. Further restrictions certainly arise concerning personal data. OEMs are keen to obtain such data, but a lack of clarity on data ownership creates legal risk for the companies, which may stifle innovation. There are also a range of issues around liability that arise in a connected car setting should data not flow as intended across a network (or within the vehicle) or should security safeguards against external tampering or even cyber-attacks prove insufficient.

The Physical Device and Negligence: Product manufacturers have a duty to exercise a reasonable degree of care in designing their products so that those products will be safe when used in reasonably foreseeable ways. As a (very unlikely!) thought experiment, consider a manufacturer of fully automated (i.e., specifically designed so no driver intervention is needed) braking systems that, against all common sense, conducts testing using only vehicles driven on dry road surfaces. If the braking systems then prove unable to reliably avoid frontal collisions on wet roads, a person injured in a frontal collision on a rainy day could file a negligence claim. He or she could argue that his or her injuries were directly attributable to the manufacturer's negligent failure to anticipate driving in wet conditions as a reasonably foreseeable use of a car equipped with the fully automated braking system.

The Physical Device and Strict Liability: Even when a manufacturer exercises all possible care in attempting to build safe products, sometimes a product will nonetheless be shipped containing an unsafe defect — for example, an "Eye System" such as Google Lens causing cataracts in users. If that defect then causes injury to a user of the product, the manufacturer could be "strictly" liable for the resulting damages (Restatement (Second) of Torts). The term "strict" is used because it removes the issue of manufacturer negligence from consideration; instead, it is based on consumer expectations that products should not be unreasonably dangerous (Dobbs and Keeton, 1984; Greenman v. Yuba Power, 1963). Historically, and to a significant extent today, strict liability has been invoked with respect to manufacturing defects, design defects, and "failure to warn" (Restatement (Second) of Torts).

Under the Second Restatement — and, thus, under an enormous body of products liability case laws — a manufacturer can be liable for the sale of a product containing an "unreasonably dangerous" defect even if it has "exercised

all possible care in the preparation and sale" of the product (Restatement (Second) of Torts). In addition, the liability can apply even if the user of the product "has not bought the product from or entered into any contractual relation with the seller." As a result, any entity in the product distribution chain upstream from the user can be held strictly liable, and the user does not need to have purchased the product at all. If a manufacturing defect injures a passenger riding in a car owned by a friend, the injured passenger could file a strict liability claim against the manufacturer (or other entities in the distribution chain).

In 1998, the American Law Institute published the "Restatement (Third) of Torts: Product Liability." The Third Restatement specifically addresses manufacturing defects, design defects, and failure to warn, but it notably ties liability for design defects and failure to warn to "foreseeable risks." Under this framework, which will likely be used by an increasing number of courts in the future, the failure of a manufacturer to identify and mitigate a dangerous "foreseeable" risk is more akin to negligence than to strict liability. While the landscape is somewhat in transition with respect to the specific theories of liability that can be invoked to pursue claims regarding manufacturing defects, design defects, and failure to warn, all three remain central to products liability law.

Manufacturing and Design defects: Consider a manufacturer of fully autonomous and self-navigating vehicles (such as an unmanned aerial vehicle or "UAVs") that usually ships its vehicles with well-tested, market-ready automatic braking software. However, suppose that in one instance it accidentally ships one vehicle with a prototype version of an AI algorithm containing a flaw does not present in the market-ready version. If the vehicle with the faulty device becomes involved in an accident attributable to the flaw, a person injured in the accident could file a claim for damages arising from this

manufacturing defect. A manufacturer can be found strictly liable for dangerous manufacturing defects, even if it has exercised "all possible care" in preparing the product. It could be argued that if liability issues affecting M2M (or $M_{AI}2M_{AI}$) or M2H (or $M_{AI}2H$) data exchange as a result of such a manufacturing defect, the manufacturer would be held liable. This would avert consideration of attributing legal entity status to entities such as machines (nor AI machines) otherwise not presently classified as "legal entities" for the purposes of legal liability.

More importantly, the built-in sensor system and AI equipment assists the vehicle in performing crucial driving tasks such as keeping the vehicle on the road, in the right lane, at the appropriate speed, and at a safe distance from other vehicles and road obstacles. There are several considerations to account for because a human operator may seldom drive a vehicle in the future. When then, should the human passenger (the owner of the vehicle) overrule an incorrect decision by an AI machine?

For example, sometimes a device may contain a design defect that causes harm. In the context of Vehicle Self-Navigation Systems, liability complaints alleging design defects are likely to arise in connection with the shared responsibilities between the vehicle and the human driver. Suppose that a manufacturer markets a system that it claims has a specific level of automation (e.g., NHTSA level two automation, which "involves automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions"). The NHTSA definition of automation level two also states that the "driver is still responsible for monitoring the roadway and safe operation and is expected to be available for control at all times and on short notice" (NHTSA, 2013). The meaning of "short notice" is, however, unclear.

Consider an accident that occurs because a human driver does not take over control of the autonomous vehicle quickly enough. In a products liability lawsuit, an injured party would likely argue that the system had a design defect because it should have been designed to provide the driver with more advanced warning. The manufacturer of the system might counter by arguing 1) that the system *did* provide sufficient advanced warning and 2) that providing even more warning would necessitate adding very costly new sensors to the system that would only increase the warning time so marginally as to make no practical difference in the time available to a driver (or user) to react. Due to the United States Constitution guarantee that each American citizen has certain civil rights of personal liberty, the manufacturer or operator cannot wholly mitigate their liability under Torts Law through private contractual arrangement. Liability for an alleged design defect is often determined using a risk-utility test, the standards of which vary in different states. Risk-utility tests generally examine whether the risks posed by an alleged design defect could have been avoided or reduced using an alternative solution that would not have impaired the utility of the product or unnecessarily increased its cost.

Privacy: The issue of liability for breach of privacy has a direct nexus to information disclosure and data granularity. Smart machines — Eye Systems, for example — process data and come up with conclusions. Specifically, it can collect data about your health condition. A breach of privacy may ensue where a mistake is encountered in the artificial intelligence process. Because of this, the information that is now sent from this machine (i.e., smart device) to others (or to a human) ($M_{AI}2M_{AI}$ or $M_{AI}2H$) results in some sort of damage. Consider, for example, if this information somehow ends up with an insurance company that is very private to you and, as a result, refuses to insure you or increase your premium because it is a pre-existing medical condition. This damage or cost could be to society at large (because incorrect information is provided) or to an individual entity (because specific data or sensitive information concerning that person are leaked). Who, then, is liable for this harm? As discussed, the issue of liability is met with two hurdles. First, only a "legal entity" has standing to sue or be sued (County of Riverside v. McLaughlin). A legal entity, at least under present law, does not extend to a machine or to artificial intelligence. Second, liability may be directly related to the way in which data are transferred via the Internet, or the data are affected *because* of the device.

Similarly, information leakage within the IoT raises issues concerning ISP liability for third party content, which has previously been explored in scholarship (Schruers, 2002). However, what happens when a subscriber to an ISP behaves badly and causes an injury to an unsuspecting third party — say, by copying someone's data without authorization or making a libelous statement? Is the ISP responsible for the behavior or actions of its subscribers? Can the victim

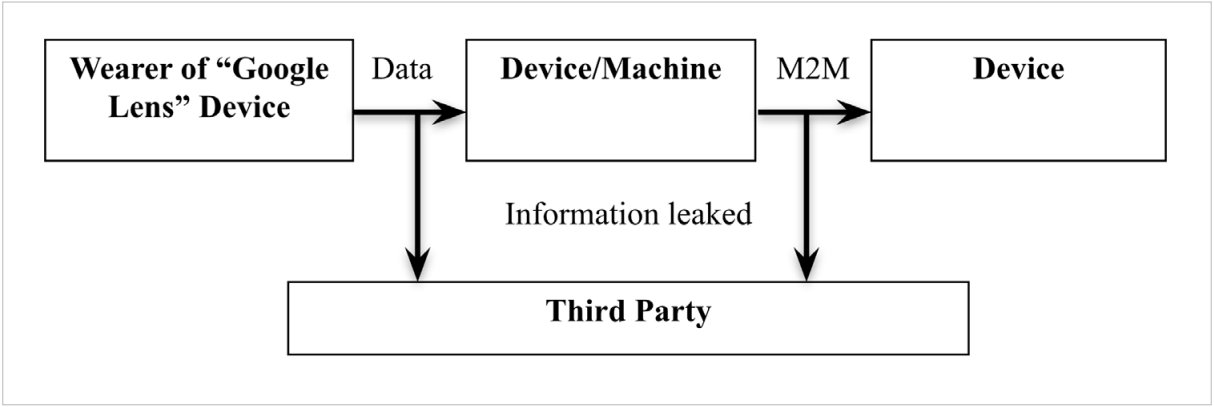

Figure 3: Eye System, Defamation and Privacy

of an online injury argue that even though the ISP is not the direct cause it can be sued because it knew of the activity, encouraged it, profited from it, or had control over it?

Such an issue may arise where information is mistakenly "leaked" between an M2M or M_{AI}-$2M_{AI}$ exchange in a People Flow System or an Eye System. For example, incorrect information concerning a person's health obtained from a device (as described above) could be mistakenly leaked and published on the Internet (see Figure 3), resulting in damage to their reputation. Such a person (the "wearer" and related affected parties) may bring an action for defamation of character, also known as libel, if the publication of an untrue statement that causes injury to the reputation of a person or business occurs. Notably, the Google Lens is licensed by the pharmaceutical giant Novartis. This raises multiple issues, including the following: Who is liable — the licensor or the licensee? What is the applicable jurisdiction to bring an action for breach of privacy or negligence? And does such a smart device require approval by health authorities?

Determination of liability can be relatively straightforward and is generally specified in the contractual arrangement between the licensor and the licensee. The applicable jurisdiction is similarly clear-cut, other than where the jurisdiction in question is in an online environment. Such an issue may be increasingly prevalent in the context of the Io T. Presently, however, there is no statutory reference in any jurisdiction around the world that explicitly outlines how online jurisdiction is determined. Rather, this may be outlined in case law. The leading case in the United States is Zippo Manufacturing Co. v Zippo Dot Com, which states that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of the commercial activity that an entity conducts over the internet."

Under present law, ISP accountability is similarly challenging. Section 230 of the Communications Decency Act (CDA) states that no ISP "shall be treated as the publisher or speaker of any information provided by another information content provider." In other words, the CDA shields ISPs from liability for statements or content from its users. This is true even where the ISP paid the writer for use of the statements (Zeran v. America Online Inc.; Blumenthal v. Drudge; Jane Doe v. America Online). An action for unauthorized copying (i.e., copyright infringement) may also be brought under the Digital Millennium Copyright Act (DCMA). A discussion of this is beyond the scope of the present paper.

The issue of liability and privacy could, however, be addressed at the device level. With respect to the former, a device could have built-in capabilities to connect to the licensor or the licensee. In such a case, a determination of liability and governing jurisdiction may be easily identified. The latter could be addressed using selective information disclosure. This would overcome some of the privacy problems because some of the privacy issues would be kept away from the human domain. At one end of the spectrum, having access to everyone's data raises the possibility of jeopardizing everyone's privacy. The other extreme is that humans are guarded from accessing any information at all. If a buffer is built with machines, these machines try to perform intelligent task with available data and send humans information that is relevant as opposed to superfluous. Thus, the feasibility of this approach has been demonstrated by the People Flow System, in which a smart sensor monitors the movement of individuals but only

discloses this information to the receiver as anonymized dots (or circles). The advantage of this approach is that the AI machine can still know whether the circle is the same person, whereas the receiver will be shielded from this private information.

Granularity, Privacy and Regulation

Closely tied to privacy is information disclosure and granularity. For example, Watson et al. (2010) define "granularity" as "the level and frequency of information collection." Interestingly, in one of their examples, they observe that extra data that were collected added little value. As identified in Figure 1, granularity has a direct impact on information disclosure, the sensitivity of which informs the "value" of that information to both the sender and the receiver. An example is when a sender volunteers information by way of release in hopes of gaining a benefit in exchange or being compensated for the information release. This becomes increasingly valuable the fewer people there are who receive this information. This is where the sensitivity comes in. If information generated is truly valuable, then the property value holds monopolistic property rights. When a person keeps information to themselves, it is a monopolistic market. However, if information is good enough, then the sensitivity of the information is at issue. In our current market, there is an enormous amount of information disclosure, possibly because of ignorance or compensation to a person (e.g., providing something for free), but which hides that there is some benefit to the third party as a result of that information. The aim of information technology should be to bring things back in order so that TPs benefit less and the information is guarded more closely. We can collect data with great granularity, store them locally (even at the machine level) and process it there. By doing so, we can reduce privacy issues and concerns, possibly making regulation easier.

When there is a mistake *with* or *in* the Artificial Intelligence process and harm is suffered, an assessment of liability depends on the type of harm suffered, the classification of the parties involved, and an assessment of the chain of events (i.e., causation). Consider a situation where an AI machine makes a decision and for some reason it makes a mistake in the DM process. Because the machine cannot be held responsible for its own actions, who is responsible for the harm that is caused?

One possible solution to minimizing the potential negative effects of using a device could rest in the new information system and the shape that it takes. Perhaps an open data approach could be adopted for big data and the IoT, which could help alleviate some legal issues that could arise around access and proprietary rights to data. It could be argued that moving toward an open data approach for data generated by IoT technology could avoid issues around unfair competition. The People Flow case study is illustrative of this. The traditional approach has centered around the use of CCTV, which streams much data, but where it is difficult to create and find relevant information. Often, a person needs to watch hours of streams to identify unusual behavior. In contrast, a smart sensor would make decisions about how to monitor. For example, a smart sensor can detect unusual patterns and then use CCTV to collect data with greater granularity. In addition, privacy can be better maintained because the smart sensor can reorganize

the collected data. The machine, for instance, can identify the person but then only inform the receiver that *a* person behaves in a suspicious fashion.

We observe that making data available to those who intend to use it in the interests of fostering new ideas and services would help avoid monopolies emerging around access rights to data. With data likely to become an increasingly important asset, having monopoly rights to data and restricting rivals' access to that data under certain circumstances could be interpreted as a breach of competition rules.

From a broader perspective, do we have a decentralized MIS (many little MIS interacting), or do we give more intelligent machines a greater role or responsibility than less important machines? An analogy can be drawn for a manager — for example, a line or division manager — who will ultimately be responsible. The "new" MIS will no doubt introduce an increasing number of situations where a "machine" should be liable — particularly if it operates in place of a manager. Under the present legal system, however, an assessment of liability may otherwise shift to an owner of a device — a legal entity. Such considerations are very complex, and we are providing an initial attempt to organize these factors in a meaningful fashion.

For now, there appears to be an urgent need for implementing an updated data protection law framework in the United States as well as introducing new rules on network and information security. Businesses should receive sufficient guidance on anonymizing and pseudonymizing data sets that include personal information as well as minimizing the amount of data they collect following the adoption of new data protection laws that would complement technical solutions that are privacy-enhancing by design. Guidelines outlining how security risks associated with the increasing volume of data being created can be managed and reduced would be complementary to this. At the same time, incentives to share datasets between partners and mechanisms to facilitate knowledge and technology transfers should also be developed. We predict that one area on the horizon spurring from this could also be how cloud computing solutions can be best configured and used for data analytics and advanced infrastructures and services. We envisage that such measures would promote the industry-led development of more open standards to encourage data to be exchanged within the new information system.

Adapting the Law to Fit the New Information Technology

Products liability law has proven to be remarkably adaptive to new technologies. The same will hold true for smart devices within the new information system. Products liability has been one of the most dynamic fields of law since the middle of the 20th century. In part, this is because the new technologies that emerged over this period have led courts to consider a continuing series of initially novel products liability questions. Overall, the courts have generally proven quite capable of addressing these questions and in so doing have been the primary drivers of a positive feedback cycle involving case law, the American Law Institute's Second (in 1965) and Third (in 1998) Restatements, revisions to the Uniform Commercial Code (UCC), and changes to state statutory law. Through this process, products liability law has evolved to its current state. Given this strong record of adaptation to new technologies, there is no reason to expect that the legal system will be unable to address the products liability issues that arise with respect to smart devices that operate within the Io T. As the IoT matures in the coming years, it will be important to establish a nationally consistent set of regulations. Those standards, once they are established, would indirectly impact liability. The process of setting standards at the federal level would provide a set of metrics that state courts would likely choose to adopt in liability cases.

SMART DEVICE CONNECTIVITY

The IoT is not a question of *if,* but of *when*. It is likely to result in a fundamental change of the function and role of MIS. As discussed, future information systems will serve not only humans but also machines. This, no doubt, is the fundamental departure that will affect decision-making in the business context. Under current management practices, the roles of managers and MIS are separated. This, by design, makes privacy-preserving analytics challenging.

In the future, however, through the use of AI, machines and devices will be able to do far more incredible things than they can currently do. Therefore, our theoretical model (which is designed under a prediction perspective) can be utilized to provide specific answers using case study examples as to what can be done. We predict that this will not only affect the IoT itself

but that it can also be implemented in areas outside IoT where it is possible to merge AI and information systems. One of the potential benefits we see is that the merging of roles could potentially help contribute to privacy-preserving analytics because it will no longer be necessary to disclose highly personal or private data (or information) to unintended receivers.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

REFERENCES

Akerlof, G. A. (1970). The market for 'lemons': Quality uncertainty and the market mechanism. *Quarterly Journal of Economics* (84:3), pp. 488–500.

Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*. http://www.rfidjournal.com/articles/view?4986

Bakos, J. Y. (1997). Reducing Buyer Search Costs: Implications for Dlectronic Marketplaces. *Management Science* (43:12), pp. 1676–1692.

Bakos, Y., Brynjolfsson, E., and Lichtman, D. (1999). Shared Information Goods. *Journal of Law and Economics* (42), pp. 117–155.

Benbasat, I., and Zmud R. W. (2003). The Identity Crisis Within the IS Discipline: Defining and Communicating the Discipline's Core Properties. *MIS Quarterly* (27:2), pp. 183–194.

Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

Brown, J. R., and Goolsbee, A. (2002). Does the Internet Make Markets More Competitive? Evidence from the Life Insurance Industry. *Journal of Political Economy* (110:3), pp. 481–507.

Chen, H., Chiang, R., and Storey, V. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, (36: 4), pp. 1165–1188.

County of Riverside v. McLaughlin, 500 U.S. 44 (1991).

Cowan, J. (2012). The $$ Cost of M2M Hype and False Hopes. http://www.m2mnow.biz/2012/12/14/9173-the-cost-of-m2m-hype-and-false-hopes/

Dewhurst, M., Willmott, P. (2014). Manager and Machine: The New Leadership Equation. *McKinsey Quarterly*, Issue 3, pp. 76–83.

Dobbs, D., and Keeton, R. (1984). Prosser and Keeton on the Law of Torts. 5th ed. Minneapolis, MN: West Group.

EU Commission Task Force for Smart Grids, Expert Group 1 (December 2010). Functionalities of Smart Grids and Smart Meters. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf

Fleisch, E., and Mattern, F. (2005). Das Internet der Dinge. Berlin, Heidelberg: Springer.

Gartner Press Release. (2013). Gartner Says Personal Worlds and the Internet of Everything are Colliding to Create New Markets. http://www.gartner.com/newsroom/id/2621015

Gasser, U. (2014). Cloud Innovation and the Law: Issues, Approaches, and Interplay. *Berkman Center Research Publication* No. 2014–7.

Geyer, R., and Rihani, S. (2010). Complexity and Public Policy: A New Approach. New York, NY: Routledge.

Golling, M., and Stelte, B. (2011). Requirements for a Future EWS — Cyber Defence in the Internet of the Future. 3rd International Conference on Cyber Conflict Proceedings 7–10, Tallin, Estonia, pp. 135–150.

Greenman v. Yuba Power Products, Inc., 59 Cal. 2d 57 (Cal. 1963).

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly* (30:3), pp. 611–642.

Gregor, S., and Jones D. (2007). The Anatomy of a Design Theory. *The Journal of the Association for Information Systems*, (8:5), pp. 312–335.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* 29(7), pp. 1645–1660.

Harper, J. (2008). Reforming Fourth Amendment Privacy Doctrines. *American University Law Review* (57:5), pp. 1381–1403.

Hosanagar, K., Chuang, J., Krishnan, R., and Smith, M. D. (2008). Service Adoption and Pricing of Content Delivery Network (CDN) Services. *Management Science* (54:9), pp. 1579–1593.

Jane Doe v. America Online, Inc., 718 So.2d 385 (1998)

Kamenica, E., and Gentzkow, M. (2011). Bayesian Persuasion. *American Economic Review* (101:6), pp. 2590–2615.

Kendall J. E., and Kendall, K. E. (1993). Metaphors and Methodologies: Living Beyond the Systems Machine. *MIS Quarterly* (17:2), pp. 149–151.

Kingsley, T. (2013). AT&T comments to the Federal Trade Commission on the Privacy and Security Implications of the Internet of Things; FTC Project No. P135405.

http://ftc.gov/os/comments/internetthingscomments/00004–86142.pdf
Lee, A. S. (2001). Editorial. *MIS Quarterly* (25:1), pp. iii-vii.
Lewin, R. (2000). Complexity, "Life at the Edge of Chaos" 2nd ed. Chicago, IL: University of Chicago Press, pp. 130–132.
Lier, B. (2013). Luhmann Meets Weick: Information Interoperability and Situational Awareness. E: CO (15:1), pp. 71–95.
Lundquist, E. (2013). Black Hat 2013: Five Security Trends That Will Draw Most Attention. www.eweek.com/security/black-hat-2013-five-security-trends-that-will-draw-most-attention/
Marschak, J., and Radner, R. (1972). Economic Theory of Teams. New Haven and London: Yale University Press.
Mayer, C. (2009). Security and Privacy Challenges in the Internet of Things. published in Workshops der Wissenschaftlichen Konferenz Kommunikation in Verteilten Systemen 2009 (WowKiVS 2009) Proc. WowKiVS 2009 Volume 17.
Miller. G., and Kearns, M. (2012). Nanotechnology, Ubiquitous Computing and The Internet of Things: Challenges to Rights to Privacy and Data Protection. Draft Report to the Council of Europe.
National Highway Traffic Safety Administration (2013). Preliminary Statement of Policy Concerning Automated Vehicles. http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf
Ning, H, Liu, H., and Yang, L. (2013). Cyberentity Security in the Internet of Things. http://www.cybermatics.org/lab/paper_pdf/2013/Cyberentity%20security%20in%20the%20internet%20of%20things.pdf
Orlikowski, W. J., and Iacono, C. S. (2001). Research Commentary: Desperately Seeking the "IT" in IT research — A Call to Theorizing the IT Artifact. *Information Systems Research* (12:2), pp. 121–134.
Oxford Dictionaries. (2013). Internet of things. at: http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things
Pattison, S. (2013). ARM Holdings PLC comments to the Federal Trade Commission on the Privacy and Security Implications of the Internet of Things; FTC Project No. P135405. http://ftc.gov/os/comments/internetthingscomments/00011–86154.pdf
Rayo, L., and Segal, I. (2010). Optimal Information Disclosure. *Journal of Political Economy* (118:5), pp. 949–987.
Restatement (Second) of Torts § 402A (1965).
Restatement (Third) of Torts § 7 (1998).
Rooney, B. (2013). Internet of Things Poses Big Questions. Wall Street Journal Online. http://online.wsj.com/article/SB10001424127887323899704578583372300514886.html
Rosen, J. (2001). The Unwanted Gaze: The Destruction of Privacy in America. Vintage, p. 60.
Sankaranarayanan, R., and Sundararajan, A. (2010). Electronic Markets, Search Costs, and Firm Boundaries. *Information Systems Research (21:1), pp. 154–169.*
Santucci, G. (2010). 1.1 The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects. https://www.google.com/#q=Vision%20and%20Challenges%20for%20Realising%20the%20Internet%20of%20Things&safe=active
Schruers, M. (2002). The History and Economics of ISP Liability for Third Party Content. *Virginia Law Review* (88:1) 205.
Spence, M. (1973). Job Market Sigaling. *Quarterly Journal of Economics* (87:3), 355–374.
SRI Consulting. (2008). Disruptive Civil Technologies Six Technologies with Potential Impacts on US Interests out to 2025. http://fas.org/irp/nic/disruptive.pdf
Stiglitz, J. E. (1975). The Theory of 'Screening', Education, and the Distribution of Income. *American Economic Review* (65:3), pp. 283–300.
Tan, L., and Wang, N. (2010). Future Internet: The Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE).
The Economist Intelligence Unit. (2013). The Internet of Things Business Index: A Quiet Revolution Gathers Pace. http://www.arm.com/files/pdf/EIU_Internet_Business_Index_WEB.PDF
Watson, R. T., Boudreau M. C. and Chen A. J. (2010). Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. *MIS Quarterly* (34:1)
Weber, R. (2009). Internet of Things — Need for a New Legal Environment. *Computer Law & Security Review* (25), pp. 522–527.
Weber, R. (2010). Internet of Things — New Security and Privacy Challenges. *Computer Law & Security Review* (26), pp. 23–30.
White, C. (2013). Car Tech Outlook: Self-Driving Cars Are Just around the Corner. *Mashable*. http://mashable.com/2013/06/23/self-driving-cars-3
Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).
Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F.Supp. 1119, 1124 (W. D. Pa. 1997).