Toward the Internet of Value: The Internet of Things and the Future of Payment Systems

Jessie Cheng
jcheng@ripple.com

I have adapted the following from a chapter of mine to be published in the American Bar Association’s forthcoming book, Electronic Payments in the 21st Century.

The discussion below is drafted for a broad audience of lawyers, policymakers, and others who are interested in learning more about the Internet of Value. It pairs discussion of the Internet of Value’s transformative potential with substantive analysis of concrete legal and policy issues — in simple, practical terms.

I. A World of Interconnected Objects

Nearly everywhere today, headlines proclaim that an Internet of Things is upon us. But what is this digital transformation, and where is it leading us?

The phrase broadly refers to a world where everyday objects are equipped with sensors and network connectivity, allowing these smart objects to collect, send, and receive information in a fully automated way. In practical terms, the Internet of Things transforms everyday physical items into smart objects able to react to the world around them, as well as communicate with individuals, in an efficient and frictionless way. Picture coffeemakers that kick in at the ring of an alarm clock, lighting and blinds that respond to changing conditions outside, and refrigerators that order milk when it runs out or goes bad. These smart objects make day-to-day chores more streamlined and remove the need for human decision-making.

Perhaps more likely around the corner than a consumer Internet of Things is an industrial form of it — an application of the interconnected ecosystem to the business-to-business context for tracking inventory, equipment functionality, and operating efficiency. GE, one of the world’s largest industrial companies, is opening a network of what it calls “digital foundries” around the world. Factory floors may soon see a transition toward sophisticated computer-controlled

---

1 Jessie Cheng is currently deputy general counsel at Ripple and vice chair of the Payments Subcommittee of the ABA Business Law Section’s Uniform Commercial Code Committee. Previously, she was counsel and officer in the legal group of the Federal Reserve Bank of New York and, prior to that, an associate at the law firm Wachtell, Lipton, Rosen & Katz.


production and automation, with smart machines communicating with each other and their industrial surroundings.

Taking the Internet of Things one step further, smart objects in the physical world can also have the ability to synthesize information and deliver analysis to individuals in real-time, transforming data into more easily distillable value. And ever more so as the costs to adding sensors, microchips, and internet connectivity to products decrease. The Internet of Things, as well as future innovations built on these new technologies, has the potential to fundamentally transform business operations and our day-to-day lives. But what do these technological strides mean for payments? How are these new technologies challenging existing payment systems, and what new transformations may be on the horizon?

II. The limitations of today’s payment networks

The Internet of Things has the transformative potential to drive a fundamental shift in the way payments are made. Already evident today is a movement away from the conventional payment mechanisms of cash and plastic cards, edged out by what would once have been considered the most unlikely objects. A smart watch, like the Apple Watch, can be used to initiate contactless payments through cell phone-stored financial information. A pair of smart glasses, like the Google Glass, could potentially also deliver a swift shopping experience.

Of course, the payment capabilities enabled by the Internet of Things can do more than ease the mundane burdens of the modern consumer. They can significantly expand access for people in the world’s poorest regions to formal financial services and empower the financially underserved to be more involved in the global financial system. Individuals without access to traditional bank accounts can instead use their smart objects, such as smart phones, to hold value and make payments.4

The transformative potential of the Internet of Things, however, is limited by today’s inefficient, fragmented, and costly payments infrastructure. The Internet of Things solves only for communication between objects—a seamless exchange of information. It does not come with a built-in streamlined exchange of value.

For example, imagine using a smart medicine cabinet. It might automatically detect when the medicine runs low and seamlessly initiate a payment for refill using stored financial information. This saves you time and effort: no need to drive to the pharmacy, no hassle trying to figure out how to pay with various spending accounts and health plans, and a lower risk of running out of medicine—everything can be done remotely, in real-time. However, the Internet of Things empowers you in this way only if you have a credit card or method of payment at hand that the smart medicine cabinet and the pharmacy accept. But what if you do not have access to a credit card or a bank account? Or, what if you are paying for an ailing family member located

---

abroad? Your payment method may not be interoperable with the local pharmacy there, or your U.S. bank may decline to process the transaction. And even if there happens to be compatibility, the risk of unpredictable time delays and opaque foreign exchange rates, service fees, and lifting fees remains.

Today’s payment networks are siloed, and the disjointed global system is riddled with inefficiencies and frictions. Payments flow relatively freely along domestic rails within a country, or if the payer and payee happen to have accounts with the same bank or network. Try making a payment across networks though, and you may be out of luck. Even where connections between payment networks do exist, they are likely slow and expensive. To open up the interconnectedness of the global economy to its full potential, the Internet of Things cannot be left to run on the fragmented rails of today’s existing payment systems. Rather, it must be underpinned by the Internet of Value.

III. Toward a world of interconnected payment networks

The Internet of Things requires interoperability across the world’s disparate payment networks — an Internet of Value — to realize its full transformative potential. Just as the Internet of Things enables interoperability across smart objects, the Internet of Value provides interoperability across the world’s payment systems and financial institutions, enabling payments to move seamlessly across systems, currencies, and banks.

In many ways, this evolution in payments toward global interconnectedness builds upon the technological advances that the industry has already made over the past two centuries. Technological advances are not unprecedented in payments, and new technologies have become important parts of fundamental, industry-wide changes. The railroads, steamships, and telegraphs of the 19th century linked together geographically remote commercial counterparties and created the foundation for international transactions. The second half of the 20th century introduced computers to automate complex and tedious procedures for payments processing. Electronic networks were also established to allow for faster and more secure communication. However, financial institutions and payment systems still operate in silos even today — streamlined, global interconnectivity has not yet been achieved and, as a result, some cross-border business processes still rely on manual or only semi-automated procedures. The Internet of Value has the potential to cure these inefficiencies and frictions, as well as serve as the platform for future innovations that may seem unimaginable today.

This future world is perhaps nearer than we think. Existing technologies today, such as the Interledger Protocol (“ILP”), represent the beginning of the Internet of Value, in which exchanging value will be as streamlined as exchanging information today on the internet. Remember, the internet itself is not one single network or system — it is a network of networks, enabled by open protocols like TCP/IP (Transmission Control Protocol/Internet Protocol) for sending information across independent telecommunications networks. The power of the Internet comes from this open connectivity — it is easy to communicate with anyone around the world in real-time, regardless of what provider they happen to use.
The same can be done for payments. In essence, ILP and technologies like it create connections between the many banks and payment systems around the world — from domestic payment systems and the books of correspondent banks, to digital wallets, blockchains, and beyond. And it does so through an open, universal protocol. Through this technology, any payer would be able to pay any payee in a simple, fast, and inexpensive way. The resulting global payments interconnectivity will transform the payments landscape, and this Internet of Value will serve as the foundation for the Internet of Things.

Financial institutions will likely continue to play a key role in the Internet of Value, but taking full advantage of its transformative potential will require an evolution on their part. Many are already pursuing key features of interoperability and real-time payments across currencies. As financial institutions embrace the potential of this fourth industrial revolution, they will create new services for customers — and avoid being left behind as other types of payment service providers adapt to and benefit from innovation-fueled changes.

More broadly, the participants in the Internet of Things will reshape the payments industry as a whole and drive forward a transformation in how the world transacts. As the number and diversity of smart objects increase, more and more quotidian objects will be converted into independent payment-initiation devices. These smart objects will automatically detect the need for a purchase — such as ordering replacement parts directly from foreign manufacturers — and seamlessly initiate payment on behalf of their consumer or institutional owners. Smart objects may also trigger a payment transaction in the other direction, to their owners — such as by submitting insurance claims directly from a remote factory floor. Within a global economy that is ever more integrated, this will mean an increase in transaction volumes for retail (that is, low-value) cross-border transfers. Even micropayments (one-off payments of tiny amounts) may quickly become a reality as individuals and companies enable objects to make automated payment decisions on their behalf.

IV. Legal and policy considerations for an interconnected world

The Internet of Things, underpinned by the Internet of Value, will drive an evolution in the global payments industry. However, it must grapple with the fundamental issues plaguing payment systems today. Ensuring security and privacy, as well as managing identity and financial information across multiple devices and locations, will be challenging. Nevertheless, innovation in smart objects is rapid, and the transformative potential of the Internet of Things will create new solutions. The real challenge may well be in future-proofing — no one knows where the technology and its myriad applications will lead.

---

5 For more information about the ILP, see the white paper, “A Protocol for Interledger Payments” by Stefan Thomas and Evan Schwartz, available at: https://interledger.org/interledger.pdf
a. Identity and access control

Identity and access controls enforce gatekeeping policies with respect to smart objects and the information they contain. They can also control the transfer of information over a network to which the smart object is connected. Together, these measures ensure information integrity and security at the time information enters a smart object or network, while it resides on the device and in the network, and while it is in transit within the network.

An ecosystem of connected smart objects capable of executing payment transactions raises new challenges for identity and access management. The number and type of smart objects in a particular individual’s or institution’s possession may be ever changing. Conversely, there may be multiple users, each with their own payment methods, allowed access to a given smart object, and who those users are at a given moment in time may also be in flux. Conventional controls and management systems that mainly focus on individuals — such as user IDs and passcodes — may be ineffective in capturing these complex relationships between smart objects and their users.

In this way, today’s identity and access management solutions are stuck in a pre-internet past. They depend on the same user ID and password gatekeeping used to secure static information stored on unconnected personal computers and isolated system folders. They were not, therefore, built with any interoperability in mind.

As a result, users are left to cope with a panoply of user IDs and corresponding passwords, ever growing in number and required complexity, simply to do business and stay in touch with the rest of the world. This can create security vulnerabilities to increasingly sophisticated fraudsters. And some users, overcome by password fatigue, may simply flout the advice of security experts — they may use essentially the same user ID and password for many similar smart objects, rely on easily crackable remembered words, or, worse yet, write them down on prominently placed Post-it notes.

Continuing to apply conventional identity and access management solutions to the multitude of smart objects that make up the Internet of Things would exacerbate these already existing security problems, as well as reinforce the fragmentation and inefficiencies of today’s payment systems. Without interoperability, users must redundantly establish separate identities for each smart object they use, and then keep track of them all. They may be called on to prove their identity by, say, submitting a copy of a passport or utility bill — which provides more data than may be necessary, creating yet more security problems.

However, the Internet of Things may well bring about a transformative shift in identity and access management. Interoperability can be achieved through common standards for how smart objects connect and communicate with each other. When smart objects can speak to each other in a common language, their identity and access controls can efficiently coordinate and seamlessly recognize a given user without a slew of cumbersome user IDs and passwords. Accommodating the great diversity of smart objects — varying in their manifold uses as well as sophistication — though, will be a challenge. Nevertheless, many unpredictable applications
may arise once smart objects speak the same language — we are, after all, still witnessing the solutions human ingenuity and creativity can discover once empowered by the internet.

b. Authentication and authorization

How does one establish one’s identity to a smart object and one’s intent to be legally bound in a smart object-initiated transaction? Perhaps one provides some piece of information that only the rightful user ought to know (such as a PIN or password). Or one uses some object that only the rightful user possesses (such as a debit card or token device). Or perhaps there is something that the rightful user simply is (a physical characteristic such as fingerprints and iris patterns). These approaches can be used individually or in some combination (called multi-factor authentication) to form a set of authentication and authorization procedures.

These various gate-keeping approaches solve the problem of authentication and authorization with varying degrees of robustness and convenience. The “something you know” approach is common and relatively inexpensive to implement, but it is subject to well-known weaknesses. Passwords can be cracked, particularly if they are jotted down on Post-it notes left lying around for all to see. The “something you are” approaches have been sprouting up fast and continue to capture the imagination. One day, we could sign on to a smart object using a fingerprint scanner and authorize a money transfer with a spy thriller-esque eye scan. However, such biometric hardware is expensive, systems generally lack compatibility, and the technology is still maturing. Moreover, biometrics are not secret and cannot be changed, destroyed, or invalidated once compromised or intercepted — and the risk of interception may be particularly high where arrays of smart objects are relaying biometrics over an open network.

There is great variation, too, within these categories of authentication processes. The “something you have” approach, for example, can use static or dynamic data authentication. Credit and debit cards with magnetic stripes, for example, use static data authentication: they store sensitive payment data that is unchanging. Whoever knows your card number, expiry date, and so forth can use that information over and over again to make fraudulent purchases. Credit and debit cards with an EMV chip, on the other hand, use dynamic data authentication. This means every time you use an EMV card for payment, the microchip generates a code that is unique to that transaction, and that code is used to authenticate and authorize that particular transaction. Even if a fraudster were to steal card information from one of your transactions, the stolen transaction code created in that instance would not be usable again, and the fraudster’s transaction would just be denied. In short, dynamic data authorization makes it harder for fraudsters to profit from what they steal.

Dynamic data authentication is not limited to credit and debit cards. Consumers today can load their financial information onto smartphone-based payment systems that use this more secure method to authenticate transactions. However, even these systems are not iron clad. One weak spot is at the point of enrollment, when financial information is first loaded onto the smartphone. That is, clever fraudsters can take stolen financial information and load it onto their own device. In case any red flags are raised and the bank phones up to request more information from the enrollee (a “something you know” approach), the fraudster may be
equipped with just enough information about the victim to pass the test. It is only after financial information is loaded on to a smartphone that the risk of misuse is vastly reduced.

The problems of fraudulent or unauthorized charges are further compounded for consumers if the Internet of Things is left to run on the fragmented and disparate rails of today’s existing payment systems. Different payment methods come with different statutory consumer protections. For example, the strongest level of statutory protection for unauthorized charges generally applies to credit card transactions, capping consumer liability at $50. A $50 ceiling also applies to debit card transactions, but unauthorized charges must be reported within two business days; the ceiling can increase to a $500 cap or unlimited liability if the consumer fails to timely report the unauthorized charge. Other payment methods may not even have these consumer protections. Because smart objects can be linked to a wide variety of payment rails — various types of cards, bank accounts, and even virtual currency wallets — consumers are left with a complicated patchwork of consumer protections, in some places robust but in others threadbare. Yet the average user may be largely unaware of this variation: a smart object-initiated transaction is just that. The particular payment method used by the smart object, and the statutory protection that applies, are nuances that may escape average consumers.

Until the Internet of Value arrives, the smart objects of the Internet of Things must be cobbled together with today’s traditional payment rails, and the chain will only be as strong as the weakest link. As financial transactions have moved from cash to checks to the electronic transfers of today, sophisticated fraudsters have followed. And as more consumers use payments-enabled smart objects, more points are open to attack. Even worse, an attack on one interconnected smart object could potentially provide a gateway for a fraudster to gain access to a trove of other payment capabilities and stored financial information.

c. Privacy and security

One of the paradoxes of modern life is that we cherish our privacy, our right to be left alone, yet we obligingly hand off our personal data and financial information in day-to-day interactions. We may take cybersecurity seriously and diligently observe online precautions, but we gladly surrender our credit card information and personal details to retail websites, for example. However inwardly conflicted we may be, our expectations around privacy are evolving. It is harder these days to shut out an increasingly connected and ubiquitous online world. Already, many aspects of our lives today — shopping, fitness, banking, gaming, entertainment, and social connections — are captured on our internet-connected smartphones. As the amount of information collected and transmitted by smart objects continues to increase at an unprecedented rate, the Internet of Things will likely raise novel privacy and security concerns.

---


Of course, the technology-neutral privacy and security concerns familiar to us today remain front and center. Take, for example, the FTC’s complaint against TRENDnet, Inc., settled in September 2013. According to the complaint, TRENDnet, an electronics company, sold video-monitoring cameras that provide live video feeds over the internet. It had marketed these cameras to consumers as home security and baby monitoring devices, allegedly claiming in its product descriptions that these cameras were “secure.” However, the cameras’ faulty software apparently allowed hackers to access the live video feeds of hundreds of consumers unbeknownst to them and view their private lives and the interiors of their homes. Concluding that TRENDnet had “failed to provide reasonable security to prevent unauthorized access to the live feeds” from its cameras, the FTC brought its enforcement action using its general consumer protection enforcement powers under Section 5 of the FTC Act (regarding “unfair or deceptive acts or practices”). As the TRENDnet action illustrates, the FTC views unfair and deceptive trade practices in the context of information security as falling within the ambit of its authority, and it will likely play a key role in the interconnected ecosystem of the Internet of Things.

The result is that manufacturers of traditional household devices, now made smart and internet-connected, must become experts in consumer privacy and security matters to which they may previously never have given a second thought. In addition to the FTC Act, state-level prohibitions against unfair, deceptive, or abusive acts and practices (UDAAP) may also be important — state attorneys general may interpret the scope of these UDAAP laws as the FTC has interpreted its Section 5 authority. Beyond these general consumer protection laws, other sectoral laws may also come into play. In particular, the Gramm Leach Bliley Act, the California Financial Information Privacy Act, and similar laws that protect the privacy of personal financial information will raise important legal considerations for smart objects capable of initiating payments through stored financial information.

Missing from this bevy of legislation, however, are any privacy and information security laws dedicated specifically to the smart objects that make up the Internet of Things. Any targeted regulation of this nascent space must strike a balance between fostering innovation and growth that enrich our lives, on the one hand, with protecting consumer privacy and the use of sensitive personal information, on the other. Indeed, a number of panelists speaking before the U.S. Senate Committee on Commerce, Science and Transportation at a February 11, 2015 hearing on this issue urged Congress not to rush to regulate the Internet of Things. In its January 2015 report, “Internet of Things: Privacy & Security in a Connected World,” the FTC concluded that there is “great potential for innovation” in this uncharted space, and any Internet of Things-specific legislation would be “premature” at this early stage. However, recognizing the increasing need to manage ongoing data security threats — as well as the potential for smart objects to amplify those threats — the FTC reiterated its previous recommendation to enact broad-based federal privacy legislation that is “strong, flexible, and technology-neutral.” Its

8 In the Matter of TRENDnet, Inc., FTC File No. 1223090.
10 The U.S. Senate Committee on Commerce, Science and Transportation Hearing, “The Connected World: Examining the Internet of Things” (February 11, 2015).
report also offers concrete steps that smart object developers can take to enhance and protect consumer privacy and security, applying to smart objects the core principles and recommendations the FTC has featured in other reports (reasonable security, data minimization, privacy notices, and consumer choice as to collection of personal data).

These privacy and security concerns have gained traction in the European Union as well. An independent EU advisory body called the Article 29 Working Party on Data Protection released a 2014 opinion stressing that the existing EU data protection legal framework is fully applicable to the Internet of Things. In particular, the opinion highlighted individual autonomy and consent, with users remaining “in complete control of their personal data throughout the product lifecycle,” and with consent being “fully informed, freely given, and specific.”

The contrasts that exist between the FTC’s 2015 guidance and the Article 29 Working Party’s 2014 opinion perhaps reflect the cultural and political differences between the United States and the European Union regarding online privacy. The United States has generally viewed personal data protection largely through the lens of consumer protection, whereas the European Union sees it as a fundamental right of EU citizens. Although the Article 29 Working Party’s opinion contributes to unifying the application of the EU data protection framework to the Internet of Things across the European continent, still lacking today is any formal and coordinated global effort toward harmonization. The resulting fragmentation of the internet along national lines may become more apparent and problematic as the interconnected ecosystem of the Internet of Things draws ever more personal data into the internet’s borderless space.

V. The next transformation

Already today, one’s connection to the internet is no longer limited to a box that sits on a basement desk. An increasing number and diversity of objects are being equipped with sensors, internet connectivity, and data analytics capabilities. These smart objects have the potential to fundamentally transform business operations and our day-to-day lives, and they are already beginning to form the backbone of the Internet of Things.

However, to open up the interconnectedness of the global economy to its full potential, the Internet of Things cannot be left to run on the fragmented rails of today’s existing payment systems. A lack of global interoperability results in inefficiencies and frictions, further compounded as more smart objects initiate transactions over the internet’s borderless space. Cobbling the Internet of Things with today’s fragmented payments infrastructure may introduce new risks and vulnerabilities. Rather, the Internet of Things must be underpinned by the Internet of Value — interoperability across the world’s disparate payment networks. The resulting global payments interconnectivity will transform the way businesses operate and the way people relate to the world around them, as well as serve as the platform for future innovations that may seem like a pipe dream today.

12 Opinion 8/2014 on Recent Developments on the Internet of Things (Sept. 16, 2014).