GSR discussion paper

Interoperability in the digital ecosystem

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 25 June 2015.

The views expressed in this paper are those of the author and do not necessarily reflect the opinions of ITU or its Membership.

Table of Contents

Page

Interoperability in the digital ecosystem

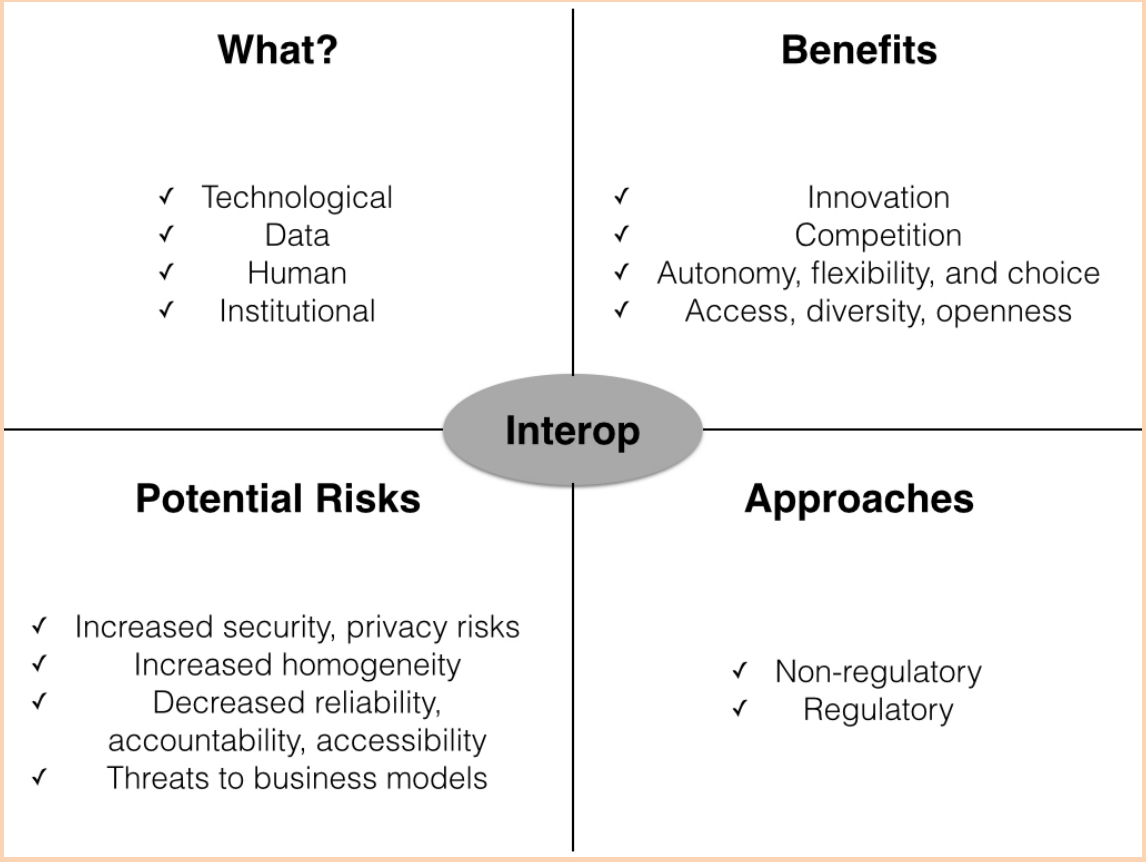
Author: Urs Gasser, Professor of Practice, Harvard Law School; Executive Director, Berkman Center for Internet & Society at Harvard University

Executive summary

At its most fundamental level in the context of the digital ecosystem, interoperability (or "interop") is the ability to transfer and render useful data and other information across systems, applications, or components. As a concept interop is central, and yet often invisible, to many parts of a highly interconnected modern society. The fact that someone can make a seamless international telephone call without thinking about things like "signaling standards" or transoceanic cables is a tribute to interop. So is the fact that someone can send and receive the same e-mail on a phone or in a browser, regardless of device manufacturer or ISP. And the development of the Internet of Things relies on interop. For that reason it is critical to develop a shared understanding how interop functions, the potential costs and benefits of increased levels of interop, and the variety of approaches for encouraging interop.

This paper begins by offering a framework for understanding interop as a concept. Figure 0 provides an overview of the concept of interop, its benefits, potential risks and approaches.

Figure 0 – Overview Diagram of interop:



Source: ITU

In theoretical terms, interoperability functions across four broad layers of complex systems: technological, data, human, institutional. For many people, it is the exchange of data through technological means that comes to mind when they think about interop. But it turns out that the human and institutional aspects of interoperability are often just as – and sometimes even more – important than the technological aspects.

This paper next offers examples of some of the many benefits and drawbacks of higher levels of interop. On the benefits side this includes: innovation, competition, choice and access. While, the potential drawbacks include: security and privacy risks, an increase in homogeneity, a decrease in reliability, accountability, accessibility, and a threat to certain existing business models.

The paper then offers a taxonomy for considering the various approaches that exist within the toolbox for managing and optimizing the level of interop. These approaches can either be deployed in a more unilateral fashion or they can be deployed in more collaborative ways. Moreover, there are approaches that can be deployed by the private sector and those that are utilized by regulators and other state actors. The paper also considers in more depth the unique role that governments and regulators can play in shaping the interop landscape.

Finally, the paper concludes by identifying some of the biggest questions and challenges that confront future interoperable technologies.

1 Introduction

Large segments of the world are now interconnected as never before: people stay in touch with far-away family and friends for low cost; they learn about news instantaneously, access knowledge remotely, collaborate more efficiently, and conduct every manner of business online. The most complex systems—government agencies, financial institutions, transportation infrastructures, health care and energy systems—are linked by these new, invisible information channels, which are essential components of today's global economy. But as interconnected as things currently are, they will grow dramatically more so thanks to the emergence of the "Internet of Things."

Generally speaking, the Internet of Things (or "IoT"), is the term for how anything that can be connected to the Internet will be. Interconnectedness through the Internet means not only new forms of interactions with end users, but also new forms of interactions with other devices. This is a world where the car of a driver who is running late will automatically send a text message to the driver's next appointment to let them know she's running late. Or where a jet engine can inform the ground crew that it needs maintenance before the plane even lands. Or where city parking meters can help drivers find open spots in order to reduce pollution and congestion. Or where a pill bottle can remind a patient to take their next dose. The possibilities for new forms of interconnectedness are staggering and endless.

Some experts believe that the market for IoT devices will grow exponentially over the coming years, resulting in over USD 1.7 trillion in value added to the global economy by 2019.[1] This explosion of new devices will require new infrastructure and technologies, with some analysts expecting that new infrastructure models will be deployed within two years and many existing networks will become overwhelmed with IoT traffic within just three years.[2]

This explosion of new IoT technologies, however, is built primarily on a single concept: interoperability. In order for a car, a jet engine, a parking meter, or a pill bottle to send and receive important data, it needs to be able to seamlessly connect to other systems and networks in ways that are meaningful and secure. That necessary interconnection of systems is interoperability (or "interop").

This capacity for connection has the ability to make daily life more convenient or efficient. But this growing level of interconnectedness comes at a potentially high price if designed or implemented poorly. Society must make trade-offs as it becomes digitally connected everywhere and anytime. Individuals struggle to keep up with news and information and also become more vulnerable, in ways that are less obvious and poorly understood. The same infrastructure that enables people to create, store, and share information can put their privacy and security at risk. Society's most advanced systems and infrastructures have become so complex that they are hard to manage effectively. And while many parts of daily life become more connected, some remain woefully underconnected.

For that reason, it is important to define the optimal level of interconnectedness and to understand how technology, markets, law, and regulation can shape the outcomes. As a first step, this paper looks at a framework for assessing how complex systems, components, and applications are connected—or sometimes, inexplicably, still separated. And then the paper evaluates some of the promises and the drawbacks that come with increased connectivity. Finally, the paper looks at approaches to enabling interop, and the role that governments, regulators, and organizations such as the ITU can play in that process.

---

[1] John Greenough, *The 'Internet of Things' will be the world's most massive device market and save companies billions of dollars*, Business Insider (Feb. 18, 2015), http://www.businessinsider.com/the-internet-of-things-market-growth-and-trends-2015-2#ixzz3WBO0CLrW.

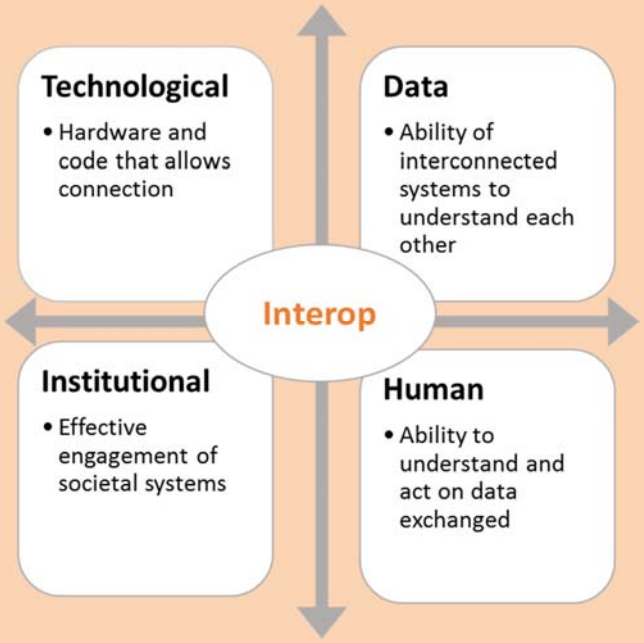
[2] IDC, *Press Release: IDC Reveals Worldwide Internet of Things Predictions for 2015*, Dec. 3, 2014, http://www.idc.com/getdoc.jsp?containerId=prUS25291514.

2 Interop framework and use cases

Defining interoperability is challenging because there is no one-size-fits-all definition. How one defines interop is based largely on context and perspective. For example, in the context of electronic health records, a patient may define interoperability as seamless access to his medical records. But the third-party operator of the hospital's e-health records database system may define interoperability as the ability to technically interconnect with the hospital's computer systems and integrate health records in a meaningful (and secure) way. In that regard, interop is not just one type of transaction or relationship; interop encompasses many forms of interaction, which often occur simultaneously. A transaction as simple as sharing electronic vaccination records with a new doctor might require numerous and concurrent forms of interoperability in order to succeed.

Although interop can mean many things, at its most fundamental level in the context of information technologies, it is the ability to transfer and render useful data and other information across systems, applications, or components. But this definition does not fully embrace the complex and varying layers of interop. In theoretical terms, interoperability functions across four broad layers of complex systems, as shown in Figure 1:

Figure 1 – Diagram of interop layers:



Source: ITU

For many people, it is the exchange of data through technological means that comes to mind when they think about interop. But case studies demonstrate that the human and institutional aspects of interoperability are often just as – and sometimes even more – important than the technological aspects.[3] How individuals work together as humans, often relying upon technological tools, can determine whether

[3] Berkman Center for Internet & Society, *Interoperability Case Studies*, https://cyber.law.harvard.edu/node/92249.

the most seamlessly interoperable technologies prove effective for their given task. For example recent research on online learning tools has shown that the students who have both human and online instruction get the most out of the experience.[4] The human instructors help to bridge the gap for the students where the software falls short of meeting their individual needs. In other words, it is not sufficient to simply connect students with knowledge without thinking about the other layers that affect their comprehension and how the students ultimately relate to the material.

What then do each of these interop layers mean?

- *Technological:* The technological layer is the hardware and code that allow one system to physically connect to another. Much like train tracks and roads allow cities to connect and share commerce, the technological layer allows systems to connect to one another and share data, often through an explicit, agreed-upon interface.
- *Data:* Without the ability to understand and process what is being transmitted, it is insufficient for technological systems to have the capacity to pass bits from one system to another. The data layer is the ability of interconnected systems to understand each other. Technological interoperability is often worthless without the data layer and the ability of interconnected systems to make use of the transmitted bits. The data and technological layers are often considered together because they are inextricably linked in many ways. However, anyone who has ever received an e-mail attachment that their computer could not open understands that simply having the technological capacity to receive data is not the same as interoperability at the data layer.
- *Human:* This layer is the ability for humans to understand and act on the data that is exchanged. Although it is more abstract than the technological and data layers, it can be just as crucial for interoperability. Language is one form of human interoperability—in order to communicate, people need to use a common language. Another form of human interop is a willingness to work together. Interop often succeeds or fails based on the individuals and personalities at the end points of the data exchange, and the level of effort and the good will they are willing to expend in order to work together successfully.
- *Institutional:* The institutional layer is the ability of societal systems to engage effectively. The legal system is one example of an institutional layer of interoperability. For instance, in order for two companies in different countries to collaborate, they need to reach a shared understanding of applicable law, and be comfortable that their rights can be vindicated. Interop at the institutional layer does not require homogeneity of legal systems; it instead requires only *enough* commonality to protect the interest of both parties.

Although they are related concepts, it is important to clarify the relationship between interoperability and compatibility. Compatibility is a specific form of interoperability that represents certain design choices in the development of a system. For example, in 2014, the EU approved a directive that called for the use of a common standard for cellphone chargers.[5] This legislation addressed a narrow design choice: the compatibility of the cables that provide power to mobile devices. The interoperability of mobile devices is a far bigger and more complicated issue than a single element of compatibility, but one element of the overall interoperability is the compatibility of cables. Throughout this paper, it is important to bear in mind that compatibility is an important part of interop and can play an important role in how well and easily systems work together.

---

[4] Justin Reich, *The Role of Humans in Blended Learning*, May 26, 2014, http://www.edtechresearcher.com/2014/05/the_role_of_humans_in_blended_learning/.

[5] Directive 2014/53/EU of The European Parliament And of The Council, 2014 O.J. (L. 153/62), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0053&from=EN.

2.1 Mobile payments: Interop layers applied

In any complex interoperable system, all of four layers will play a role. In some examples one layer may be more important than others, but successful interoperability relies upon interconnections at every layer. The recent growth of mobile payment platforms is a useful illustration of how the layers interact to ultimately shape the success of the platform as a whole. In particular, the example highlights the important role that the institutional and human layers have played.

Mobile payments are like traditional credit card transactions, but mobile payments use a mobile device (typically a smartphone) in lieu of a plastic card. As smartphones have become more common, a variety of wallet-less electronic payment systems have proliferated, with mixed results. Beginning in 2011, Starbucks made it possible for customers to pay for their drinks using Starbucks' mobile app. Today, over 16% of US transactions at Starbucks are made through their app, representing over 7 million payments per week.[6] Around the same time, Google announced Google Wallet, and although Google does not share detailed figures, there is evidence suggesting it has had limited use.[7]

The divergent results of Starbucks and Google have not discouraged other market entrants from around the world. Recently, a federation of US retailers, including discount department store Walmart, announced CurrentC, a mobile payment platform designed to reduce the influence of traditional credit card companies and banks on retail transactions.[8] In October 2014, The Republic of Korea's Line messaging platform announced plans for a mobile payment service called Line Pay.[9] In March 2015, South Korean electronics giant Samsung purchased LoopPay, a system that allows greater backwards compatibility with older credit card retail terminals.

One of the most significant new entrants is Apple Pay, which was announced in September 2014. Within three days of becoming available, Apple processed 1 million card activations,[10] the number of card-issuing banks has grown from six in September 2014 to 2,500 in March 2015, and the number of retailers accepting Apple Pay has tripled to nearly 700,000.[11]

What unites all of these mobile payment systems is their reliance on interoperability. The need for interoperability becomes apparent when you consider the variety of actors involved in a single transaction, as documented in Figure 2, below. Interconnecting all of these actors across a variety of merchants and devices, requires numerous forms of interop at each layer. Although interop is necessary and present in every mobile payment platform, this example highlights a point that will be addressed later in this paper: interop is not a binary value – it can occur to greater and lesser degrees. The mobile payment competitors have taken different approaches, each trying to find the optimum level of interop, and Apple's and Starbucks' relative success in the mobile payment space demonstrates the importance of not neglecting the human and institutional layers.

---

[6] Marcus Wohlsen, *Forget Apple Pay. The Master of Mobile Payments is Starbucks*, Wired, Nov. 3, 2014, http://www.wired.com/2014/11/forget-apple-pay-master-mobile-payments-starbucks/.

[7] Charles Arthur, *How Many Google Wallet Users Are There? Google won't say - but we can*, The Guardian, Sept. 25, 2014, http://www.theguardian.com/technology/2014/sep/25/google-wallet-apple-pay-nfc.

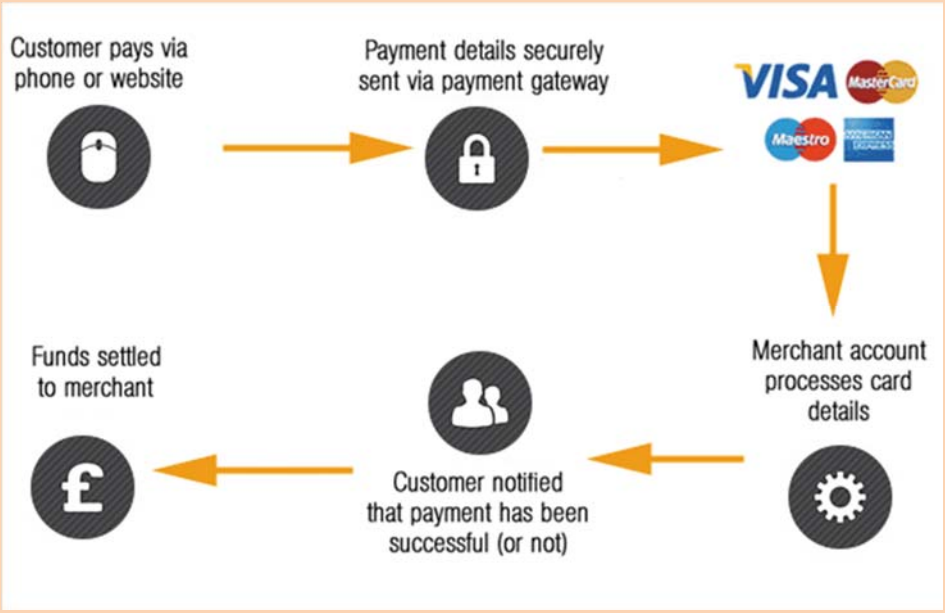
[8] Josh Constine, *CurrentC is the Big Retailers' Clunky Attempt to Kill Apple Pay and Credit Card Fees*, Tech Crunch, Oct. 25, 2014, http://techcrunch.com/2014/10/25/currentc/.

[9] Catherin Shu, *Line Pay, the Messaging App's Mobile Payments Service Will Make Its Global Debut Soon*, Tech Crunch, Dec. 4, 2014, http://techcrunch.com/2014/12/04/line-pay-the-messaging-apps-mobile-payments-service-makes-its-debut/.

[10] Daisuke Wakabayashi, *Apple CEO Tim Cook Happy With New Apple Pay Service*, WSJ, Oct. 28, 2014, http://www.wsj.com/articles/apple-ceo-tim-cook-happy-with-new-apple-pay-service-1414474181

[11] Anthony Ha, *Apple Pay Now Accepted In Nearly 700k Locations*, Tech Crunch, Mar. 9, 2015, http://techcrunch.com/2015/03/09/apple-pay-stats/#rU8Np5:AqOz

Figure 2 – Diagram of mobile payment processing and various actors:



Source: Web-Merchant.com, New to Online payments? http://www.web-merchant.co.uk/onlinepayments.asp

Consider some of the approaches the various payment platforms have taken to each layer:

Technologic: Successful implementation of a mobile payment system requires multiple kinds of technologic interoperability. One type of technologic interop is interconnections between banks and devices. For example, in order to initially set up a credit card to work with Apple Pay, Apple must have backend compatibility with the processing banks, in order to transmit securely to the banks user and card information.

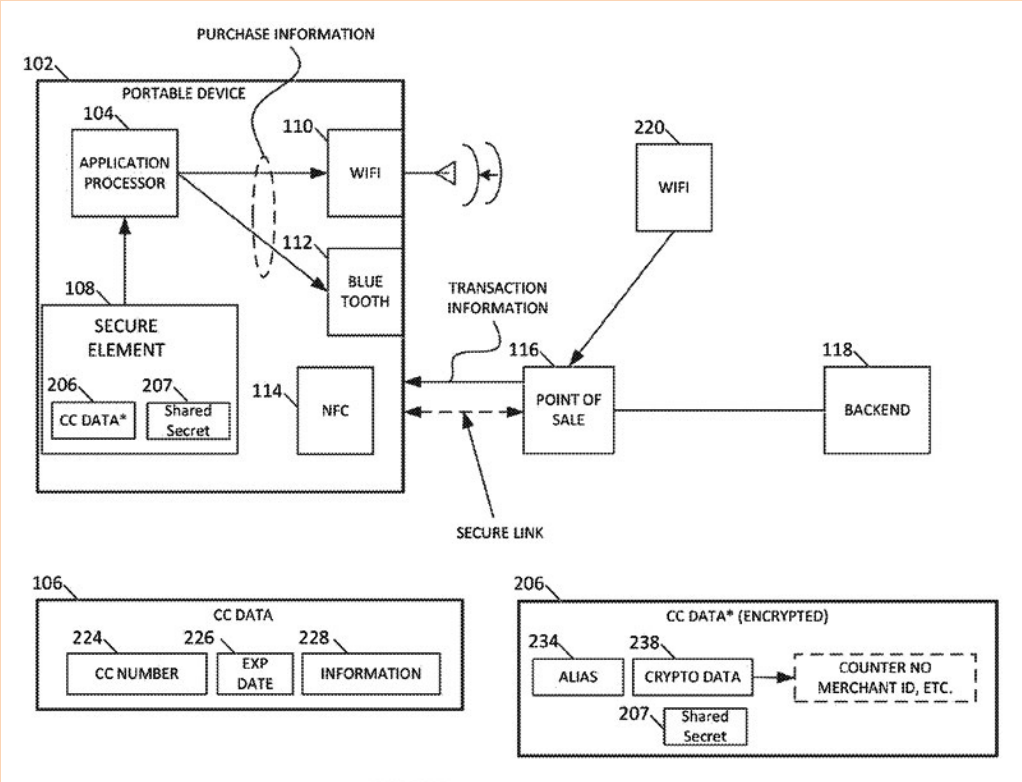
Another type of technologic interop is the ability of a mobile device to interconnect to the payment platform. Google Wallet, for instance, can run on a wide range of Android devices that contain a Near Field Communication (NFC) chip, which is necessary for communication with the retailer payment terminal.[12] Apple Pay also requires an NFC chip for exchanging data with payment terminals, however, Apple Pay also requires that the device is an Apple iPhone, and that the iPhone includes several security features including a special encrypted chip and Touch ID for biometric identification. Because only the newest iPhone 6 and iPhone 6 Plus have all of these technical components, those are the only devices that currently support Apple Pay, limiting Apple Pay's technologic interop across devices.

Another type of technologic interop is the ability of the device to interact with retailers' payment systems. Because Apple Pay and Google Wallet use NFC communication, only retailers that have NFC-capable payment terminals can accept those services. Only a small (but growing) number of payment terminals accept NFC, making this is a fairly significant limit on technical interop. Figure 3 is a drawing from an Apple patent that shows the way in which it interconnects with a retailer "point of sale." Although the patent does not necessarily describe the current iteration of Apple Pay, it highlights the complexity of the technological interop on the platform. CurrentC and Starbucks use bar codes instead of NFC, but this requires that the retailer payment system have an optical scanning device to read the bar code. Samsung's

[12] For more information on NFC, please see Daniel Howley, *What is NFC, and Why Does It Matter For The iPhone 6?*, Yahoo! Tech, Sept. 3, 2014, https://www.yahoo.com/tech/what-is-nfc-and-why-does-it-matter-for-the-iphone-6-96456683964.html.

Loop Pay is designed to work with both NFC and existing magnetic card swipe terminals, dramatically increasing the technical interoperability.

Figure 3: Apple patent diagram showing various components of Apple Pay system



Source: NFC World, http://www.nfcworld.com/2014/01/16/327536/apple-patent-combines-nfc-bluetooth-wifi-mobile-payments/

Data: For a retailer, simply having an optical reader or an NFC payment terminal is not sufficient for processing payments through CurrentC or Apple Pay, because in addition to technologic interop, retailers need interop at the data layer in order to work with any given mobile payment system. For example, at the technical layer, Apple Pay and Google Wallet could work with any retailer payment reader that uses NFC. However, not all NFC readers can process Apple Pay or Google Wallet data. In fact, retailers associated with the CurrentC standard, including some of the largest retailers in the United States, disabled the use of their NFC terminals in order to stymie NFC-based competitors.[13]

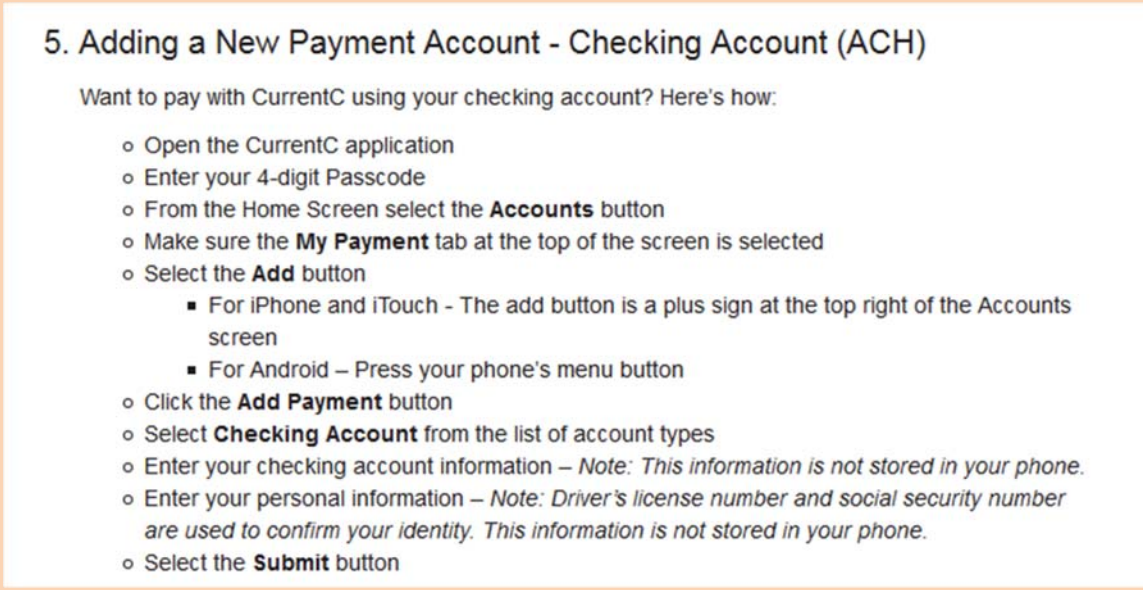
Similarly, in order for a bank to interoperate with a mobile payment platform, it needs more than technical connections to the device. For example, in order to increase the security of the transactions, Apple Pay creates one-time-use secure tokens that are transmitted to the bank instead of credit card numbers. The use of these tokens ensures that if a retailer is hacked, any captured numbers are unusable for future transactions.[14] However, using these one-time tokens requires that the issuing banks be able to interpret these tokens and match them back to a specific user account.

[13] Jason Del Rey, *Why You Can't Use Apple Pay at CVS, Walmart and Other Retail Stores*, Re/Code, Oct. 28, 2014, http://recode.net/2014/10/28/why-you-cant-use-apple-pay-at-cvs-walmart-and-other-retail-stores/.

[14] Bob Sullivan, *How Tokenization May Change The Way You Pay*, CNBC, Dec. 14, 2014, http://www.cnbc.com/id/102264704.

Human: One of the biggest reasons why Apple Pay and Starbucks have been successful with mobile payments has been their respective approach to the human layer. While other mobile payment systems are fairly complicated for the end users, setting up and using Apple Pay and the Starbucks app were engineered to be simple. For example, setting up a card in Apple Pay requires only that the user photograph an image of their card. And to use Apple Pay, the user simply holds the device near an NFC terminal and activates the biometric fingerprint reader for verification. By contrast, as Figure 4 shows, setting up CurrentC requires multiple steps including entering a passcode, entering checking account data, and entering other identifying information.

Figure 4: Screen capture of instructions for adding payment information to CurrentC account



5. Adding a New Payment Account - Checking Account (ACH)

Want to pay with CurrentC using your checking account? Here's how:

- Open the CurrentC application
- Enter your 4-digit Passcode
- From the Home Screen select the **Accounts** button
- Make sure the **My Payment** tab at the top of the screen is selected
- Select the **Add** button
  - For iPhone and iTouch - The add button is a plus sign at the top right of the Accounts screen
  - For Android – Press your phone's menu button
- Click the **Add Payment** button
- Select **Checking Account** from the list of account types
- Enter your checking account information – *Note: This information is not stored in your phone.*
- Enter your personal information – *Note: Driver's license number and social security number are used to confirm your identity. This information is not stored in your phone.*
- Select the **Submit** button

Source: CincoTec, http://www.cincotec.com/blog/apple-pay-vs-currentc

Institutional: Many mobile payment systems operate over the existing institutional credit card network that comprises the global payment processing system. This system has already established the norms and rules that help ensure that retailers and banks are fairly compensated. One aspect of this system is the fee that retailers must pay to the credit card companies to cover the cost of the complex institutional network. These so-called "swipe fees" average to about 2 per cent of each transaction, which retailers dislike.[15] For that reason, the CurrentC mobile platform, which is run by major US retailers, is trying to circumvent the existing institutional structure. By withdrawing against end-user checking accounts instead of using credit cards, CurrentC aims to take advantage of a different institutional structure relating to bank withdrawals, and thereby avoid the fees associated with credit card processing.

As the example of mobile payment systems demonstrates, all layers of interop are important. It is for that reason that no short definition of interop fully captures its scale and complexity. The example also highlights how technology, market, and law can either support or inhibit interoperability in a multitude of ways.

From a technical perspective, the mobile payments example shows that there is no single technical architecture that is necessary for interoperability. Some market actors use NFC, others use optical bar codes, and still others use hybrid technologies. A company's choice of technological platform can have a

[15] National Retail Federation, *Swipe Fees*, https://nrf.com/advocacy/policy-agenda/swipe-fees.

big impact on its ultimate interoperability; the more widespread and available the technology is, the greater the opportunities for interoperability.

From a market perspective, the mobile payments example shows the influence of network effects on actor behavior. The basic incentive structure on markets with network effects does not necessarily or automatically lead towards higher levels of interoperability among organizations, systems, or components. Instead, companies set interop strategy depending on firm-specific factors such as current market position, technological capabilities, and IP portfolio, among others. Apple, for example, seeks to use its mobile payment platform as a competitive differentiator. Thus, it has chosen not to interoperate with other mobile devices, limiting the platform to its newest iPhones.

And from a legal perspective the mobile payments shows the influence of general laws such as competition law, consumer protection law, contract law, or tort law, as well as self-regulatory enforcement. In particular, the self-regulation of the payment industry shows a bi-directional influence that simultaneously supports greater levels of interoperability and less. In the United States, new rules set by the industry will hold retailers liable for fraud unless they switch to new interoperable payment terminals by October 2015.[16] This self-regulation is increasing interoperability in several ways. First, the new payment terminals will support NFC payments, dramatically increasing interoperability between retailers and services like Apple Pay and Google Wallet. Second, it increases institutional interop by bringing the US into line with European standards for more secure credit card processing. However, the industry self-regulation (and specifically the fees associated with them) has arguably also decreased interoperability in some ways, as those fees pushed CurrentC to adopt its less interoperable approach to payment processing.[17]

The mobile payments example also highlights how interop is not a binary concept. There are degrees and types of interop, which fall along a multidimensional spectrum, explored in greater detail in Part 5 of this paper. Although all of the mobile payment systems involve various levels of interop, some take a more unilateral approach, while others rely upon collaboration. Because Google does not build smartphone hardware, they rely on cooperation from partners in order to deploy Google Wallet on compatible handsets. By contrast, because Apple controls its device ecosystem, creating and selling both the software and the hardware, it can deploy Apple Pay with less reliance on others.

The same diversity in kinds of interop can be observed in the approaches of regulators. As part of the US Government's Cloud Computing Strategy, for instance, the state and its regulators variously and simultaneously mandate interop standards, influence interop through procurement strategies, and help support the development of multistakeholder processes to develop additional standards and approaches.

The benefits and costs of interoperability are most apparent when technologies work together so that the data they exchange prove useful at the other end of the transaction. Consumers respond favorably to highly interoperable systems at the technology layer. Consumers consistently prefer systems that work together without asking them to and that make their lives simpler in the process. The data layer, a close cousin of the technology layer, turns out to be just as important: it is critical for data to be interoperable across systems as well. It is not enough merely to pass zeros and ones from one system to another. The data must in fact be readable and understandable. Without interoperability at the technology and data layers, interoperability at the higher layers in the model—the human and institutional layers—is often impossible. But the challenge of getting the basics of interoperability right, even at the fundamental technology and data layers, can be deceptively hard.

---

[16] Tom Gara, *October 2015: The End of the Swipe-and-Sign Credit Card*, Wall Street Journal, Feb. 6, 2014, http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/.

[17] Tony Bradley, *Blocking Apple Pay is a Terrible Strategy For CurrentC Merchants*, Forbes, Oct. 29, 2014, http://www.forbes.com/sites/tonybradley/2014/10/29/blocking-apple-pay-is-a-terrible-strategy-for-currentc-merchants/.

3 Benefits of higher levels of interop

Interoperability is not an end in itself. Instead, optimizing the level of interop has societal value as a means to others ends. Innovation is one policy goal that often benefits from increased interop, but it is not the only one. For example, interop can also have a positive impact on consumer choice, ease of use, access to content, and diversity, among other things. Below the paper highlights some of the key ways that higher levels of interop might be beneficial.

3.1 Innovation

Perhaps the strongest example of how interop can foster innovation is *the Internet* itself. The Internet has the ultimate interoperable design in which more and more non-interoperable networks and systems have converged. It is on this open, interoperable infrastructure that the Internet of Things (IoT) is being built. Every IoT device from a jet engine requesting service with a ground crew to a thermostat checking the weather relies on the fact that the protocols that enable devices to connect across the network are agnostic to the data that is transmitted using those protocols. In other words, high degrees of interoperability enable and foster innovation over the Internet, including deploying networked devices.

Companies with a strong interest in the IoT are currently hoping to replicate the success of the Internet by spurring innovation at the IoT layer, which itself runs on top of the Internet. For example, one consortium of tech companies has created Thread, an open protocol to help connect low-power devices. And yet another consortium of tech companies is creating a protocol to enable faster and easier device discovery and interconnection.[18] Outside of the commercial context, the ITU has also been a leader in advancing standardization in the IoT space.[19] In all cases, the hope is that building protocols to enable interconnections will support increased innovation on top of an IoT platform.

It is worth bearing in mind that although innovation is generally positive, it can include some risks. Innovation can be bi-directional. Just as interop can help support the development of innovative devices and software that has positive social value, it can also support innovative devices and software with negative social value. On the Internet, worms, viruses, spam, and other unwanted activity are in many ways just as "innovative" and just as dependent on interoperability as more positive developments. A recent example of this peril was in the Heartbleed vulnerability in the SSL protocol that enables secure, encrypted communication across the Internet.[20] Because the SSL protocol is interoperable, anyone with enough technical knowledge can write a version of the protocol that can be used interchangeably with other implementations. One version, called OpenSSL, became so popular that it was running on an estimated 66% of the Internet. Unfortunately, OpenSSL had a critical flaw—Heartbleed—that allowed attackers to potentially see encrypted communications. Thus, interop enabled this vulnerability to become widespread.

Additionally, high degrees of interop can sometimes threaten innovation. For instance, a successfully interoperable system—by unleashing network effects – can lead to very high switching costs for consumers, thereby potentially diminishing developers' incentives to invest in an entirely new technology, i.e., a *radical* innovation that would seek to replace the old one. Under such a scenario, innovators might only focus on incremental change of existing interoperable systems and foreclose opportunities for radical innovations–even if the alternative system would be superior.

---

[18] Tina Amirtha, *Google's Secret Weapon in the Battle for the Internet of Things: Academia*, Fast Company, Feb. 10, 2015, http://www.fastcompany.com/3041698/googles-secret-weapon-in-the-battle-for-the-internet-of-things-academia.

[19] ITU, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

[20] The Heartbleed Bug, http://heartbleed.com.

3.2 Competition

Standard economic analysis suggests that increased interoperability is likely to foster innovation by reducing lock-in effects and lowering barriers to entry. This pattern is observable in the subscription streaming video market. HBO, a movie network and content creator, recently began selling its "HBO Now" service directly to consumers over the Internet, breaking with its traditional business model of selling only through cable and satellite providers.[21] Under its old model, HBO's content distribution system needed to interoperate only with the systems for cable and satellite providers. Under the new model, however, HBO enabled interoperability with web browsers and devices such as Apple TV, Roku, Chromecast, and others. This change toward increased interoperability has increased competition in two ways. First, it has increased competition for subscription TV services. By decoupling HBO content from subscription TV, cable and satellite operators can no longer rely on content monopolies to ensure customer lock-in. In fact, several cable companies have begun offering "skinny" packages consisting of high-speed broadband, HBO, and few other channels, in order to compete with online-only content like HBO Now and Netflix.[22] Second, by increasing its interoperability, HBO is competing with an entirely different market: online movie streaming services. This shift has not gone unnoticed by Reed Hastings, CEO of Netflix, who recently remarked "I predict HBO will do the best creative work of their lives in the next 10 years because they are on war footing. They haven't really had a challenge for a long time, and now they do. It's going to spur us both on to incredible work."[23] This kind of competition benefits users by reducing prices and by providing incentives for product and service innovation.

Although interop generally supports competition, in some circumstances it could, counter-intuitively, lead to anticompetitive situations. For instance, certain unilateral or bilateral arrangements by firms that lead to interoperability and to greater innovation may promote a single firm or a few firms in a manner that is, over time, anticompetitive. For example, standards consortiums may sometimes create closed standards that enable interoperability across only the products of their stakeholders.[24] In this way, interoperability can be deployed as a tool for building closed ecosystems. The value to the consumer of being in the ecosystem (and benefitting from the interoperability the ecosystem provides) can in turn raise switching costs and reduce competition.[25]

Even in the general case where more interoperability leads to competition in the market, this does not mean that the net effect is maximum innovation. According to one strand of economic theory, firms may have an even stronger incentive to be innovative in circumstances where low levels of interoperability would promise higher or even monopoly profits to successful competitors. This sort of (Schumpetrian) competition for the market sets incentives to come up with entirely new generations of technologies or ways of doing business (so-called "leapfrog competition") in order to replace incumbent players and achieve temporary dominance. Amazon's strategy in the e-book market might be seen as a case-in-point for this

---

[21] Miriam Gottfried, *HBO Now Spells Trouble for Pay TV's Tomorrow*, Wall Street Journal, Apr. 9, 2015, http://www.wsj.com/articles/hbo-now-spells-trouble-for-pay-tvs-tomorrow-heard-on-the-street-1428615881.

[22] *Id.*

[23] Emily Steel, *Netflix Is Betting Its Future on Exclusive Programming*, NY Times, Apr. 19, 2015, http://www.nytimes.com/2015/04/20/business/media/netflix-is-betting-its-future-on-exclusive-programming.html.

[24] Sam Paltridge, Michael Donohue, Brigitte Acoca, *2015 OECD Digital Economy Outlook: Chapter 5: Emerging Issues: The Internet of Things*, OECD, DSTA/ICCP(2014)15/CHAP5/REV1 (Mar. 20, 2015), at ¶ 38.

[25] Eric Jackson, *Apple Isn't a Hardware or Software Company – It's an Ecosystem Company*, Forbes, June 30, 2014, http://www.forbes.com/sites/ericjackson/2014/06/03/apple-isnt-a-hardware-or-software-company-its-an-ecosystem-company/ (describing how the value of being in Apple's ecosystem increases as their devices gain greater interoperability *within* Apple's own platform).

sort of competition. Initially, Amazon's e-books could not be used on most non-Kindle devices, and thus evidenced low levels of interoperability as the company searched for monopoly profits. Although Amazon e-books can now be read using Amazon's free reader software on Android, iOS, Windows, and OS X devices, it remains true that Amazon e-books can only be read on either Amazon devices or through Amazon's software.

3.3 Autonomy, flexibility, and choice

In almost all circumstances, increased levels of interoperability tend to enhance user choice and autonomy. In interoperable ecosystems, users are more likely to choose among competitive and efficient options with regard to systems, applications, components, etc., which may be tested, mixed, and matched for specific purposes. One way that interoperable systems offer choice is through application programming interfaces (APIs), which are instructions for how one application or system can talk to another.[26] Twitter had an open API, which allowed anyone to write a Twitter client that could access Twitter's underlying data. The Twitter API supported a vibrant Twitter client ecosystem and users could switch easily between the Twitter clients of their choice. Twitter's decision to change their API in order to capture all of the client traffic, and ultimately capture the ad revenue, has reduced user choice and nearly eliminated the availability of third-party clients.[27]

Users are not the only ones who may have greater freedom to make choices when the level of interoperability increases. Consider, for instance, publishers in the e-book business that may run the risk of being locked into a gatekeeper-like distribution channel. If Amazon builds up a dominant market position based on a non-interoperable system, publishers will have no choice but to sell to Amazon at nearly any price it demands. By contrast, an interoperable system would lower the barriers to entry, making it difficult for Amazon to lock publishers into bad deals. In fact, it was this fear that led to the recent high-profile dispute between Amazon and publishers.[28]

3.4 Access, diversity, and openness

Increased levels of interoperability can make it easier for users to access content. Creating an account can be a hurdle for users, and if they do create an account, users are likely to reuse a simple password they can remember. Single-sign on digital ID infrastructure seeks to address both of these concerns. First, single-sign on infrastructure allows users to log into new services using existing credentials, such as their Facebook account. This lowers the barrier to joining new services and speeds up the process. Second, because the user can log in without creating a new account, it means that user needs to remember only their single-sign on password, instead of creating a new password. "Login with Facebook" is one example of this approach, intended to make it easier for users to log into a variety of online services, not just Facebook.com. As more sites interoperate with a single-sign on platform, the value to the user increases, as it reduces access barriers to online services of various sorts, including e-commerce platforms.

Similarly, there appears to be positive relation between interoperability and "diversity." As noted above, Twitter's open API supported a variety of clients. Moreover, when that API was restricted, it quickly led to a decrease in diversity of Twitter clients, with several unable to sustain their business following Twitter's changes.

---

[26] Brian Proffitt, *What APIs Are and Why They're Important*, Read Write, Sep. 19, 2013, http://readwrite.com/2013/09/19/api-defined.

[27] Mike Beasley, *Twitterrific 5 for Mac may become the first casualty in Twitter's war on developers, but it won't be the last*, Nov. 25, 2014, http://9to5mac.com/2014/11/25/twitterrific-5-twitters-war-on-developers/.

[28] David Streitfeld, *Amazon and Hachette Resolve Dispute*, NY Times, Nov. 13, 2014, http://www.nytimes.com/2014/11/14/technology/amazon-hachette-ebook-dispute.html?_r=0.

4 Potential risks and drawbacks

Interoperability is not an unalloyed good. In certain instances, greater interoperability brings with it possible drawbacks. These problems tend to be highly fact-specific and are often not problems related to interoperability *per se*, but rather are related to what people do with the systems once they are made to interoperate.

4.1 Increased security risks

As described above, systems can increase interoperability by providing greater opportunities for technical interconnection, being more open about the types of systems and services that can interconnect, supporting a greater variety of data, making it easier for humans to leverage the interconnections, and more. Unfortunately, each of these forms of interop can also increase the opportunities to exploit the system. A system that has more points of access, allows more types of systems to connect, and processes data with fewer limitations, increases potential attack vectors and creates more opportunity for nefarious actors to exploit data or to inject bad code. For example, single sign-on systems like Facebook's "Login With Facebook" can provide great convenience for end users, but it can also mean that a single stolen credential gives an attacker carte blanche access to numerous online systems, instead of just Facebook itself.[29]

This security concern is not precisely a problem with interoperability, nor is it insurmountable. The fact that the systems can interoperate does not *per se* mean that more people have access to underlying data in a given system. It is theoretically possible that increased interoperability as between systems could lead to further vulnerability of the different components or systems if sound security measures are not taken. For example, it was recently discovered that the mobile payment system Apple Pay was being used for credit card fraud.[30] The problem, as it turned out, was not one of interoperability *per se*, but rather that banks were not properly verifying account credentials when users set up Apple Pay accounts. Criminals were able to take advantage of banks' lax verification protocols by registering stolen credit card numbers in Apple Pay. Interoperability may increase the number of opportunities for security breaches, or the potential fall out from such breaches, but it is not the cause of the security vulnerabilities themselves. By the same token, systems that are not interoperable at all are just as likely to have damaging security breaches if proper precautions are not taken.

4.2 Decreased privacy

The possibility, in certain situations, that interoperability might reduce individual privacy is among the most commonly voiced concerns about interoperability. It is true that increased levels of interoperability may increase the number of players who could plausibly have access to personal information exchanged via an interoperable system. Single sign-on systems are the most obvious setting in which interoperability might lead to less user privacy: if technical and user controls are not well-established, the fact that multiple service providers have access to a user's online identity increases the risk of one of them misusing that data. In the electronic health records context, where privacy is of the utmost importance, it has been argued that an interoperable standard may allow highly sensitive personal data to be captured or stolen. In both cases, the higher risk of technical failure is a consequence of the fact that interoperability encourages more complex ecosystems, with more participants, and thus creates more risk vectors. Against that backdrop, it becomes clear that it is not interoperability *per se* that gives rise to increased privacy risks, but rather the specificities of its implementation. Even if one assumes that a technically waterproof interoperable solution cannot be achieved—a highly debated assertion—one can

---

[29] Amit Chowdhry, *How Facebook Finds Out If Your Passwords Were Stolen*, Forbes, Oct. 22, 2014, http://www.forbes.com/sites/amitchowdhry/2014/10/22/how-facebook-finds-out-if-your-passwords-were-stolen/.

[30] Robin Sidel, *Apple Pay Sign-Ups Get Tougher as Banks Respond to Fraud*, Wall Street Journal, Mar. 6, 2015, http://blogs.wsj.com/totalreturn/2015/03/06/apple-pay-sign-ups-get-tougher-as-banks-respond-to-fraud/.

imagine organizational or legal tools, such as privacy regulation, successfully addressing the respective privacy concerns.

4.3 Increased homogeneity

Interoperability might lead to less diversity in a market. A single platform, with which many systems interact, might become a *de facto* standard in such a way as to constrain innovation to what is possible on or within that platform. As with possible concerns related to security and privacy, it is not interoperability *per se* that would lead to this homogeneity, but rather the conditions that might flow from the extent to which parties avail themselves of the interoperability.

Although the Internet is a wonderfully interoperable system that has led to tremendous innovation, the protocols that underlie it represent a form of homogeneity. Most of the interconnected systems that people use today rely on TCP/IP at some level to connect systems to each other, networks, or the Internet itself. The protocols themselves do not include security components or end-to-end data reliability, which requires things like encryption to be built on top of the protocol.[31] In that way, the prevalence of the Internet protocols constrains innovation; security and other necessary components must be built on top of the protocol, because it would be too hard to innovate new protocols and get widespread adoption, even if those new protocols were arguably better. In the same way, e-mail protocols have become a *de facto* standard, meaning that innovations in security for e-mail must be built upon an existing set of protocols. This homogeneity constrains what is possible, ultimately providing an upper bound on the security that can be achieved in standard e-mail.[32]

4.4 Decreased reliability

The increased complexity of interoperable systems may lead to decreased reliability. This possible drawback depends heavily on the approach taken towards interoperability. As more systems rely on interop to interconnect, the overall network grows in complexity, and flaws in these systems might be difficult to fix quickly or even identify. In some instances, flaws in one system, on which other systems have come to rely, may not be fixable at all by the relying party. This problem might affect consumers, too, who find that they cannot identify a single point of contact in order to get a problem fixed, but rather need to call upon more than one entity. Consider a customer at a store who is having trouble using their mobile payment system. Is the problem with the retailer's payment terminal? The customer's mobile device? The payment system they are using? The underlying credit card infrastructure? It may be challenging for the customer to properly diagnose the issue. In fact, nearly two thirds of Apple Pay users have reported problems using the service, which has led many to simply give up on the system, particularly if the problems are outside of the customer's control.[33] As systems that interoperate scale, the level of complexity will continue to rise.

Reliability also has variation, as well: reliance. As interoperability increases, downstream systems may become increasing reliant on upstream systems. This problem was observed when Twitter's decision to change its open API threatened the business of the downstream systems that were built on top of that API. Although there was no promise between downstream and upstream entities to maintain the status

---

[31] Ian Peter, *Can TCP/IP Survive?* Circle ID, Sep. 7, 2004, http://www.circleid.com/posts/can_tcp_ip_survive (Article describing several of the weaknesses in the TCP/IP protocol).

[32] David Talbot, *Why E-mail Can't Be Completely Private*, MIT Technology Review, Aug. 14, 2013, http://www.technologyreview.com/news/518056/why-e-mail-cant-be-completely-private/.

[33] Tim Higgins, Elizabeth Dexheimer, *Apple Pay Running Into Hurdles at Checkout Counter, Survey Finds*, Bloomberg Business, Mar. 31, 2015, http://www.bloomberg.com/news/articles/2015-03-31/apple-pay-running-into-hurdles-at-checkout-counter-survey-finds-i7x95shl.

quo, such examples threaten interoperability more generally by reducing the incentive of downstream entities to invest in interoperability.

Reliability is one area where an open standards approach to interoperability holds out significant promise to both the reliability and reliance challenges. In complex, interoperable systems, it would be most helpful if problems could be solved by firms and for consumers as seamlessly as possible, without always having to come back to a single firm to fix an underlying problem. Open standards could mitigate, though not outright solve, this issue, insofar as problems could be solved collaboratively, with multiple stakeholders represented in the process of solution identification and implementation.

4.5 Decreased accountability

Interoperability is often accompanied by an increase of complexity in the relations among private actors, especially in the context of industry-driven interoperability initiatives. Against this backdrop, the question of responsibilities and liabilities calls for increased scrutiny. In context of single sign-on for digital IDs, for example, one can imagine a scenario in which a user's identification is misused by a third party, such as an advertiser, with whom the user has no contractual relationship. The lack of a contractual relationship may hinder the user's ability to be properly compensated for the harm. However, the example reveals that these concerns, again, are less a consequence of interoperability *per se* than of a concrete implementation, and that one might assume that a careful drafting of contracts (in this example: between the user and the identity provider) should avoid unintended and unnecessary liability exposure. As an alternative, the digital identity provider could take a more active role in policing the third parties with which they do business. Facebook recently took this step, demanding that companies using Facebook credentials submit to "an audit process that requires them to explain why they've chosen to collect certain pieces of customer information in their data payload," and based on those explanations Facebook can choose to deny access to data.[34]

4.6 Decreased accessibility

Looking at the aforementioned risks of decreased reliability and security as a result of interoperability, concerns have been voiced that such developments could induce different players to withdraw from the online environment as such. In the electronic health care record industry, for instance, there were concerns that interoperability would pose higher security risks than non-interoperable solutions and would prompt either doctors or patients to opt-out of the system. Although that has not been observed to date, if it were to occur, accessibility would decrease and the efficiency and health gains of online distribution could not be realized.

4.7 Threats to business models

Similar to the other downsides of increased levels of interop, the threats that interop poses to existing business models is not a downside of interop *per se* but is instead a factor of both the concrete implementation of interop and the extent to which incumbents have relied upon lower levels of interop in the design of their business models. As described above, higher levels of interop can have many benefits, but those benefits may be unequally distributed across a market. Indeed, some businesses may have a vested interest in maintaining *lower* levels of interop where they benefit and rely upon models that are built upon the lock-in of customers. For example, as of 2012, Amazon's Kindle e-reader devices were sold

[34] Alexandra Larralde, *Social Login Trends Across the Web: Q4 2014*, Janrain, Jan. 8, 2015, http://janrain.com/blog/social-login-trends-across-the-web-q4-2014/.

at cost, with the company profiting solely from the fact that customers are locked into the Amazon ecosystem for purchasing content for their devices.[35] Amazon achieves this customer lock-in by limiting both technological and other forms of interop. At the technologic layer of interop, although Amazon enables the Kindle to interoperate in limited ways with the services of other firms, such as a daily download of the *New York Times* or reading e-books on a Kindle iPhone, iPad, or Android app, the company does not allow its e-books to be read through non-Amazon software or e-readers. Similarly, the Kindle does not support common open formats such as EPUB. This lack of technical interop helps ensure that customers will rely upon Amazon's marketplace for content.

Amazon has also tried to reduce interop at the data and human layers, by limiting publishers' alternatives to Amazon. As part of its business strategy, Amazon has priced e-books at lower prices than competitors (sometimes at a loss) in order to encourage lock-in. Several book publishers began to fear that this customer lock-in would kill competitors and enable Amazon to demand monopolist pricing from publishers. Some of these publishers recently challenged Amazon's strategy, asserting that they wanted to set prices equally across e-book stores—in other words, the publishers wanted to increase the interoperability of their content across platforms. This conflict between publishers and Amazon became a public dispute when Amazon pulled most Hachette books from its store in retaliation. After a protracted battle, the publishers won temporary control over the prices for their books.[36]

The fact that higher levels of interop may pose a threat to certain business models is not a downside of interop *per se*, nor is it a reason to avoid policies and stratagem that promise higher levels of interop. In some circumstances, disrupting these kinds of business models may itself be a benefit of higher levels of interop.[37] That said, it is important to acknowledge that higher levels of interop may not be viewed positively by all affected parties, and those whose business models are threatened by higher levels of interop may take fight actively against those policies.

Taken together, these risks and drawbacks to interop can paint a challenging picture. But the potential negative aspects of a highly interoperable future do not need to come to pass. To be certain, the risks are very real, and those risks are connected to the degree and type of interoperability that is established between and among technologies. That said, the risks are largely ones of implementation and not endemic to interop itself. For that reason, as individuals, business, and regulators build an increasingly interconnected world at the technology and data layers, care must be taken to ensure that the system does not come with costs in other areas—such as privacy and security—that are higher than society is willing to pay. A theory of interoperability by design that builds in privacy and security protections from the start can help enormously in this respect.

---

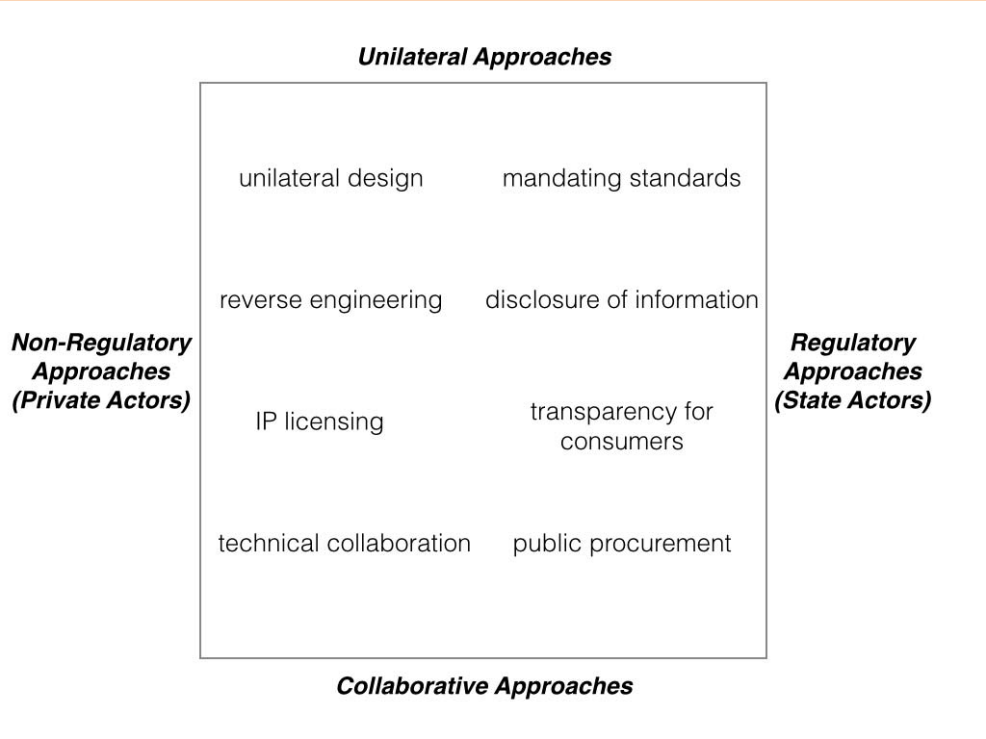
[35] Reuters, *Amazon Kindle Sold 'At Cost,' CEO Jeff Bezos Confirms*, Huffington Post, Oct. 11, 2012, http://www.huffingtonpost.com/2012/10/11/amazon-kindle-lost-leader-bezos_n_1959919.html.

[36] David Streitfeld, *Amazon and Hachette Resolve Dispute*, NY Times, Nov. 13, 2014, http://www.nytimes.com/2014/11/14/technology/amazon-hachette-ebook-dispute.html?_r=0.

[37] *See* Part 3.2, *supra*.

5 Approaches

Figure 5: Approaches to interop



Source: John Palfrey & Urs Gasser, Interop (2012)

As described through several examples above (and others below) there are a variety of approaches to interop. It is useful to think about these approaches along a spectrum from unilateral to collaborative. In other words, there are a variety of ways that entities can incorporate various levels of interop, and those can range from providing an open API (a more unilateral approach) to working with competitors and other stakeholders to create open standards (a more collaborative approach). Moreover, this same spectrum from unilateral to collaborative can be observed across both private actors and state and government actors, including national and transnational regulatory bodies. This spectrum of approaches is laid out in Figure 5 and described in greater detail below. Although the approaches have similarities across both private and public actors, this section compares and contrasts those approaches.

5.1 Non-regulatory approaches (private actors)

Many approaches towards interoperability are based on access to technology or technical specifications, and involve the licensing of IP rights or other contractual agreements. However, the degree of cooperation among different players and the corresponding licensing terms may vary considerably from case to case. The following paragraphs sketch three clusters of approaches to interoperability that range from unilateral to highly collaborative.

5.1.1 Unilateral design and IP licensing

This first cluster of approaches includes those that are marked by a comparatively low degree of collaboration between the systems that are interconnecting. Unilateral design occurs when a market participant designs its products or services in a way that allows other players to offer interoperable products or services. The range of possibilities in this cluster of more "unilateral" approaches is considerably broad.

For example, companies often use APIs as a unilateral invitation for others to interconnect with their systems. In the case of single sign-on digital ID offerings, companies like Facebook offer an open API that any app or online store can utilize, providing they comply with Facebook's rules for accessing the API. Twitter's revocation of its open API is a cautionary tale of how reliance upon unilateral forms of interop may be risky because such forms of interop may be unilaterally withdrawn as easily as they are offered.

Another important and related way to achieve interop with minimal collaboration is through IP licensing, where one party grants to others access to technology, specifications, and/or rights associated with the technology's use. The effectiveness of a licensing approach to interoperability not only depends on the company's willingness to grant a license in the first place, but also on the terms of such a licensing agreement. The scope of and compensation for the license play a particularly important role. Generally speaking, IP licensing tends to be a cost-efficient path toward higher degrees of interoperability, especially in cases where transaction costs are minimized by way of sophisticated and "streamlined" licensing procedures. As to its flexibility, the context-sensitivity of the licensing approach is high, as both parties to an agreement will carefully evaluate the characteristics of the ecosystem. Because of that flexibility, IP licensing tends to be responsive to future technologies. That flexibility, however, may decrease with the widespread adoption of a particular technology. This was precisely the pattern observed in the publishing dispute between Hachette and Amazon. When the market was relatively immature, the licensing agreements between the publishers and e-book makers were fairly simple, largely following existing licensing models. However, as the market matured and Amazon's Kindle became the dominant technical platform, the book publishers feared a loss of flexibility in the licensing terms. It was for that reason that licensing process became far more fraught, and the publishers sought more control over the pricing of their products.

5.1.2 Technical collaboration

Technical collaboration is a more collaborative form of interop. It usually involves some form of IP licensing at its foundation, but technical collaboration is often characterized by a degree of cooperation that goes beyond the mere granting of IP licenses. Often, technical collaboration is an approach to interoperability used by companies at different levels of the value chain in order to improve the user's experience. A significant example of this is the level of cooperation required for many mobile payment systems. As described above, and documented in Figure 2, mobile payment systems require technical cooperation between retailers, device manufacturers, payment processors, and banks.

Technical collaboration shares many of the advantages of IP licensing. It generally appears to be a rather effective, efficient, and flexible approach towards increased levels of interoperability. However, there exist scenarios under which the approach's advantages are smaller. One scenario where this might occur is where the market participants and collaborators grow so large as to make coordination and monitoring costs too difficult or expensive. This challenge has been observed with respect to mobile money markets in some countries. As a recent ITU report described, "In a country with just a few mobile payment operators, it might be possible to do this bilaterally or multilaterally. However, as the number of operators increases, the relationships between them, and the costs of the solution, grow exponentially."[38] Like other approaches, technical collaboration can also be misused to achieve anti-competitive ends that might not be aligned with the goal of an increased overall level of interoperability.

5.1.3 Standards and open standards

Standards are generally characterized as a collaborative approach towards higher levels of interoperability. In some cases, standards are open—an approach to interoperability that has gained much attention in recent times, while its exact definition remains a subject of controversy. In one interpretation,

[38] Venkatesen Mauree, *The Mobile Money Revolution: Part 2: Financial Inclusion Enabler*, ITU-T Technology Watch Report (May 2013), http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200002PDFE.pdf, at p. 15.

open standards require that (a) they are approved by formalized committees that are open to participation by all parties and operate on continuous bases, and (b) are made accessible to the public free of charge. In other cases—where participation is not open or the standards are not made public free of charge—the standards are less open. In the health space, both open and less open standards are apparent, sometimes within the same organization or institution. For example, the ITU-T Focus Group on machine-to-machine interoperability, focused largely on e-health applications such as remote patient monitoring, has released an open API and several free reports in order to support the ITU's standardization work.[39] In contrast, the ITU has used a more hybrid approach in the development of ITU-T H.810, standards for the interoperability of personal health systems. In that case, the ITU partnered with Continua Alliance, a non-profit organization that charges for access to its standards.[40]

Standards have a great potential for achieving high degrees of interoperability and are key instruments in the toolbox. However, this approach also can, at times, have limited overall effectiveness. Open standards initiatives are a purely voluntary effort, and anecdotal evidence suggests that companies with patent portfolios might easily interfere or even block such initiatives. Furthermore, standard-setting processes are in many cases complex, time-consuming, and relatively expensive when compared to unilateral or bilateral approaches; arguably, their cost efficiency is therefore comparatively low. With regard to flexibility, standards—particularly open standards that involve more stakeholders in the formation—regularly take into account the characteristics of the specific environment in which they are intended to operate. This means that a standard may represent a snapshot of the state of the art at a particular point in time. Depending on the speed at which technology develops, a standard based on outdated assumptions might restrictively peg future developments to historical limitations.

5.2 Regulatory approaches (state actors)

As Figure 5 notes, Governments and other regulators can also pursue interoperability through a variety of approaches, spanning more unilateral to more collaborative approaches. These approaches also vary significantly with regard to the degree of specificity in which they address the interoperability challenge. On one side are approaches such as mandating standards or requiring the disclosure of interoperability information that are, obviously, very specific in nature. On the other side are more generic interventions like general laws aimed at increasing transparency or competition, but do not address interop specifically. Particularly careful consideration is needed when it comes to interop-specific interventions, while the application of general laws and doctrines is much less problematic.

It is important to note that regulatory approaches can be carried out through a variety of entities that exercise legitimate governance authority over their defined domain. At the country level this could be a legislative body, an executive, or a designated regulator like a telecommunications regulatory authority. At the regional or international levels this could be a multinational body or a coordinating agency like the ITU. The remainder of this paper interchangeably refers to these various entities as "governments" or "regulators." In either case, it is simply referring to any regulatory body that exercises some form of legitimate governmental authority. Across any of these entities, the regulation-based approaches are consistent, and they include:

5.2.1 Mandating standards

Regulators may decide to mandate the adoption of an interoperable standard that ultimately determines how and under what terms entities can interoperate. The role of the regulator in the standard process can itself span a spectrum, from more unilateral to more collaborative. On one end, the regulator

[39] *See, e.g.*, ITU-T Focus Group on M2M Service Layer, *M2M service layer: Requirements and architectural framework*, Apr. 2014, https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-M2M-2014-D2.1-PDF-E.pdf.

[40] ITU-T, *HSTP-H810: Introduction to the ITU-T H.810 Continua Design Guidelines*, July 11, 2014, https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-EHT-2014-H810-PDF-E.pdf.

might unilaterally determine the standard. On the other end of the spectrum, the regulator might set a timetable for industry players and require them to establish and implement a common standard. Between the two extremes, all manner of hybrid approaches are possible. The impact of the European Union Data Protection Directive on the development of cloud computing standards, demonstrates the interplay between regulation and interoperable standards. The European Union's Data Protection Directive places strict limits on how personal data can be collected, stored, and processed. However, because the Directive and the national laws that implement it do not specifically address cloud computing, it has left open the question of how cloud-computing companies could fulfill their obligations under the Directive. This set up, even without further intervention from the regulator, has prompted standard setting as entities look for ways to interoperate with each while complying with the law. Recently, the International Organization for Standardization and the International Electrotechnical Commission, two non-governmental standard setting organizations, released a joint cloud computing standard that contributes to the already existing "jungle of standards."[41]

The effectiveness of this type of approach to interoperability is usually very high. A government-mandated standard can even establish an interoperable system in cases where industry players are unwilling to do so, whatever their motives might be. However, a government-mandated approach may be limited in its ability to be efficient and flexible. Administering, monitoring, and eventually enforcing a standard tends to incur considerable costs. Further, a traditional government-mandated approach often leaves very little flexibility. Not only are governments sometimes ill-equipped to choose the most suitable standard, but they also sometimes operate under conditions that make it difficult to respond in due time to market developments or changes in technology.

5.2.2 Disclosure of interoperability information (compulsory licensing)

Another regulatory approach towards interoperability consists of the government mandating the disclosure of information that is essential to build interoperable systems, components, and applications. The terms of such a regime may differ along several dimensions, for instance with regard to the group of people entitled to ask for such information, the possible consideration for the disclosing party, compensation, or the sanctions for non-disclosure. In some cases, however, the regulator can simply require industry participants to make interoperability information available, and leave it to the participants to resolve the details such as consideration or compensation. That is what occurred with mobile banking in Ghana, where the mobile carriers were offering banking services in partnership with banks. In order to ensure interoperability across banks and mobile carriers, the Bank of Ghana (the regulator) prohibited exclusive partnerships. In other words, the regulator required that any mobile operator that partners with one bank, must allow interoperability with another bank. The result of this regulation is that every mobile operator with banking services has at least three partner banks.[42]

The merits of this approach depend largely on its concrete implementation, *i.e.*, the particular design of the relevant disclosure rules. As to the effectiveness, for example, a direct relationship is likely to exist between the amount (and characteristics) of information to be disclosed, the number of parties granted access to the disclosure, and the level of interoperability that may be achieved. Similarly, the efficiency of such rules depends on their specificities. The degree of flexibility also depends on the concrete design, but as a general matter disclosure rules can arguably be implemented in a way that takes factual circumstances into account (*e.g.*, if the obligation to disclose is dependent on market, product and service maturity). Finally, disclosure of interoperability information is very unlikely to create any kind of technological lock-in.

---

[41] Paul de Hert, Vagelis Papkonstantinou, Irene Kamara, *The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection*, Brussels Privacy Hub, Working Paper v. 1, N°2, Nov. 2014, http://ssrn.com/abstract=2542125, at p. 7.

[42] Venkatesen Mauree, *The Mobile Money Revolution: Part 2: Financial Inclusion Enabler*, ITU-T Technology Watch Report (May 2013), http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200002PDFE.pdf, at p. 16.

5.2.3 Transparency rules (labeling requirements)

In order to reduce potential information asymmetries, the government can use a rather traditional approach aimed at fostering transparency and mandate the disclosure of information about the interop characteristics of a certain product or service. Again, such regulation may vary in several regards, including the characteristics and optical appearance of the information to be disclosed. If the government does not establish transparency rules by way of "specific" legislation addressing interoperability in a certain area, such regulation could be -- and partially already is -- implemented via consumer protection or (unfair) competition law. Although often not mandatory, certification programs often serve this role of bringing transparency to interoperability. For example, after the ITU standardized the home networking standard G.9954 for enabling existing-wire multimedia home networking, the HomePNA association began certifying devices for compliance with the standard.[43] Similarly, the IEEE created a program to certify products that conform to ITU-T Recommendation G.8265.1, relating to synchronization of mobile backhaul networks.[44] In neither case was transparency explicitly mandated, but increasing transparency about interoperability was necessary for those in compliance with the standards to maximize the benefits of their compliance.

Because labeling requirements contribute to interoperability in indirect ways, their effectiveness is difficult to assess. Much depends on the actual design of the labeling provisions and how well they manage to avoid information insufficiency on the one hand and overload on the other. Recent research further suggests that information needs to be embedded in consumer decision-making processes in order to be effective. While there are monitoring and enforcement costs associated with labeling requirements, it is likely that overall efficiency performs better than in the regulatory approaches outlined previously. Finally, the flexibility of labeling requirements is high, given the indirect nature of the approach and, therefore, the limited conflict with future technological developments.

5.2.4 Market power in procurement decisions

The government may favor interoperable products or services when undertaking procurement decisions and thereby provoke or support the market's tipping towards interoperable solutions. Such an approach requires that the government possess substantial purchasing power in the relevant market. This is apparent in the move toward government use of cloud services, where governments are investing significant resources in moving services and data to third-party cloud-based systems. Cloud computing service providers, however, have an interest in making their services as “sticky” as possible to minimize loss of customers to competitors. Ultimately, for the government, this can have the effect of locking itself into a particular cloud service provider. For that reason, governments can try to influence the market by hiring only companies that support data interoperability.[45]

The effectiveness of this approach is high only in instances where a government's procurement decisions have a considerable and lasting market impact. The approach may turn out to be relatively inefficient in cases where the government has to choose between an offer with lower upfront fiscal costs and an offer with higher levels of interoperability. The flexibility of the procurement approach is comparatively low because the exercise of procurement power may create a technological lock-in on the

---

[43] *HomePNA Certifies 9 More Products, 1 Reference Design, Increases Number of Reliable, Interoperable Products to 26*, Business Wire, Apr. 16, 2008.

[44] *IEEE Conformity Assessment Program (ICAP) Announces the Official Launch of the IEEE 1588(TM) Telecommunications Certification Program*, Marketwired, Oct. 9, 2013.

[45] *See generally* Urs Gasser, David O’Brien, *Governments and Cloud Computing: Roles, Approaches, and Policy Considerations*, Berkman Center Research Publication No. 2014-6 (Mar. 7 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410270.

part of the government (or else cause significant costs if the exercise of procurement power is to be repeated).

5.2.5 Competition law

Interoperability may further be achieved based on an ex post-intervention grounded in competition law. Such an intervention is possible in many countries—although particular conditions may vary considerably—when the refusal of a certain powerful player to disclose interoperability information is considered to constitute an abuse of a dominant position. Even when a company discloses interoperability information at the technical layer, competition law may prevent a powerful player from engaging in anticompetitive practices at the data layer. Whether competition law extends that far is currently the question being tested at the European Commission, which has recently filed a formal antitrust complaint against Google.[46] At issue in the case is how Google interoperates with sites that offer competing shopping services. Although Google will display data from comparison shopping tools that compete with Google's own services, the competitors claim that Google works to drive visitors to its own services. If the European Commission prevails in its case against Google, it will highlight the importance of paying attention to all of the interop layers, and not just the technologic layer.

Antitrust interventions operate with some effectiveness when establishing interoperability in specific areas. However, these interventions run the risk—in view of the duration of the respective enforcement procedures—that they continuously lag behind market development. Further, antitrust measures generally cause significant costs on part of the government that is charged with monitoring and enforcing the law. On the positive side of the balance, however, it has to be noted that the fact-specific and narrowly tailored character of antitrust interventions generally ensures the flexibility of the approach with regard to the market, technological, and legal environment in which it is applied.

5.2.6 Supplementing strategies

In addition to the approaches outlined in this section, governments and regulators also have at their disposal "supplementing strategies." These strategies include things such as the funding of research initiatives aimed at establishing higher levels of interoperability, facilitating standards setting processes, and establishing public-private partnerships that foster interoperability. Although governments and regulators roles may be most naturally oriented toward top-down action, it is important for them to bear in mind the variety of bottom-up approaches in which they can participate, either in more active or passive roles.[47]

5.3 Benchmarks for Interop

Each of the approaches identified above (both private sector and regulatory approaches) has its own features, including strengths and weaknesses or, in more economic terms, associated costs and benefits. One of the particularly tricky tasks is to evaluate them from a policy-oriented perspective and in an unbiased and balanced manner. On an abstract level, the following three benchmarks may be helpful starting place for evaluation. That said, approaches to interop need to be evaluated within their context, which may require developing additional, context-specific evaluation criteria.

5.3.1 Effectiveness

Each approach described above is likely to result in different levels of interoperability and can be expected to play a distinct role in maintaining an interoperable ecosystem. The suggested effectiveness

[46] Tom Fairless, Rolfe Winkler, Alistair Barr, *EU Files Formal Antitrust Charges Against Google*, Wall Street Journal, Apr. 15, 2015, http://www.wsj.com/articles/eu-files-formal-charges-against-google-1429092584.

[47] Rolf H. Weber, *Legal Interoperability as a Tool for Combatting Fragmentation*, CIGI (Paper Series No. 4, Dec. 2014).

criterion evaluates the respective contributions and compares the available approaches that are considered in a given situation. Understanding interoperability as a means and not an end in itself, the evaluation of an approach's effectiveness should also consider to what degree the respective strategy tends to enhance competition in the market, foster innovation, or contribute to other policy goals such as consumer autonomy and choice. To be effective, a solution must also provide interoperability over time, not just in the first instance.

5.3.2 Efficiency

In several instances, achieving and maintaining a certain level of interoperability comes with costs. The efficiency criterion seeks to measure the level of costs imposed on an affected player—companies, but also users and governments, among other stakeholders—for a given degree of interoperability and compare it with other available means of achieving interoperability. The costs of unintended consequences (some of them addressed in this paper under the heading "potential risks and drawbacks") also need to be taken into account.

5.3.3 Flexibility

In order to be successful, a given approach to interoperability needs to be able to take into account important factual circumstances that characterize the environment in which it operates. Examples are the market's maturity, product and service maturity, the features of current and future business models, the needs of users, etc. Looking forward, it is particularly important that the approach is responsive to technological development in order to avoid technological lock-in.

Depending on the context, the three benchmarks of effectiveness, efficiency, and flexibility might have different relevance or weight. One might imagine scenarios, for example, where interoperability serves such an important goal (*e.g.*, emergency number compatibility) that flexibility – at least in the short run – is considered to be less important than a high degree of effectiveness in the immediate term. In other instances a government might not want to impose standards given their relatively high costs and poor flexibility, despite the approach's potential effectiveness.

6 Role of governments and regulators

6.1 Role of governments *qua* governments

As noted above, governments and regulators have many possible approaches to fostering interoperability. Given the array of approaches, as well as the necessity of properly matching the approach with the circumstances and context of the situation, it is important to consider how best government can deploy their array of tools in the "interop toolbox."

Of course government can act as a regulator, but it can actually implement interop policy through several other roles. Consider, for example, the following roles that governments have played while pursuing interoperable cloud strategies:[48]

- *Governments as users* – governments are adopting cloud computing services to take advantage of its costs savings and innovative features and in turn using their market power to shape interoperability.

[48] *See generally* Urs Gasser, David O'Brien, *Governments and Cloud Computing: Roles, Approaches, and Policy Considerations*, Berkman Center Research Publication No. 2014-6 (Mar. 7 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410270.

- *Governments as regulators* – governments acting through their legislative, judicial, regulatory branches to implement policy through the rule of law.
- *Governments as coordinators* – governments coordinating public and private initiatives, through standard setting processes, and by facilitating the sharing of information between private and public stakeholders.
- *Governments as promoters* – governments actively promoting the industry as a whole by endorsement, funding, and incubation programs.
- *Governments as researchers* – governments conducting or funding research on technical or societal issues important for interop.
- *Governments as service providers* – governments providing cloud services for use by other government agencies or the public.

The timing and type of any intervention is a critical consideration for how and when government should take steps to promote interoperability. In its role as a regulator, for instance, governments need to carefully determine the appropriate time at which to intervene, for instance by adjusting consumer protection or privacy laws, in order to strike the right balance between enabling an environment that facilitates technological innovation on the one hand and providing regulatory safeguards for users and other stakeholders on the other hand. Ideally, the government responds to public pressures in making these determinations and engages in a multifactor analysis to determine the right point at which to intervene with the right intervention. Such an analysis would include an assessment of the maturity of the technology, industry organization, and markets.

Even government use of procurement power requires careful consideration. By acting early to influence the market, governments can have the biggest impact on the development of a market and its use of interoperability. As soon as certain industry practices and standards are set, they are much harder to influence. For that reason, some countries have found better results through anticipating needs early and entering the market at the moment where their influence can be most effective.

In addition to the importance of timing interventions in ways that they can be most effective, it is also critical to recognize that technology, markets, strategies, rationales for adoption and promotion *change over time*. The dynamic nature of technologies, such as cloud computing, requires that governments (no matter the role) engage proactively over time with the changing landscape, incorporate a systematic learning process, and adjust their strategies, approaches, and instruments accordingly. The National Institute of Standards and Technology (NIST) at the United States Department of Commerce has been effective at adapting to changing circumstances in its work relating to the development of an interoperable smart grid. One example of this is how the NIST managed the Smart Grid Interoperability Panel (SGIP), a multistakeholder body the NIST convened in 2009 order to help develop necessary standards. Initially, NIST staff held key leadership and technical roles on the SGIP. However, in response to a changing environment and the increased maturity of the smart grid industry, in 2013 NIST transitioned SGIP into an industry-led non-profit organization. By October 2013, SGIP had over 200 members and had finalized 56 standards.[49]

6.2 Role of governments as legal stewards

Governments can also shape an important part of the institutional layer of interop in their role as caretakers of a robust and stable legal environment. The future success of emerging complex systems, such as cloud computing, will depend not just on market forces but also on a well-developed legal framework. This legal framework must establish trust and legal certainty for both users and providers of future interoperable systems.

[49] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*, NIST Special Publication 1108R3 (Sept. 2014), http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf.

The relationships between interop and the law are many, complex, and tangled. As described above, the law can help establish, adjust, or maintain interop. At the same time, interoperability is also a feature of the legal system itself, termed *legal interoperability*. Legal interoperability, broadly defined, is the process of making legal norms work together across jurisdictions. This interoperability may occur either within the legal system of a single nation-state—consider federal and state legislation—or across national lines. Like technical interoperability, legal interoperability is not a goal in itself but, rather, a means to one or more ends.

The relationship between law and interoperability is multidirectional. Higher levels of interop are often the product of carefully designed legal interventions—or, at least, are fashioned in the shadow of the law. An example in this category is the enforcement of competition law against powerful technology companies trying to leverage their market power by excluding competitors. The forced disclosure of interoperability information as a matter of consumer protection is another. Conversely, interoperability itself can prompt calls for new laws to address its effects; it may also lead to the adjustment or reinterpretation of existing legal norms. As an example, consider the relation between interoperability and privacy: interoperability in the technology world is giving rise to fresh concerns about data privacy for individuals. In turn, the European Court of Justice expanded existing privacy directives to include a "right to be delisted" that spans across jurisdictions. The changes wrought by higher levels of interoperability in the technology sector are prompting calls for new forms of legal interoperability.

Governments have several options for increasing levels of legal interoperability. As in the case of technical interoperability, the point is not to make the systems all the same but rather to make them work together in particular ways. It is not necessary for countries to turn over all legislative authority to the United Nations or to create a raft of new international laws that govern all jurisdictions. There is no chance that every cultural difference can be smoothed out through harmonization of the law. Nor should it be the goal to create one uniform "world law." Jurisdictions compete productively against one another, and learn from each other, through the creation of heterogeneous legal and policy regimes. Governments need to aim for interoperability among legal systems at an optimal, rather than maximum, level, just as in other interop challenges.

It is important to find the optimal level of legal interop, because evidence suggests that legal interoperability, especially in the information economy, drives innovation, competition, trade, and economic growth. For instance, when China entered into the World Trade Organization in 2001, it had to change a great many laws and enact a number of new ones to satisfy the demands of its trading partners. China has made large-scale changes, for instance, in its system of intellectual property law. Though Chinese law is not the same as intellectual property law in the United States or Europe, it is dramatically closer today than it was a few decades ago.

This level of legal interop, however, comes with challenges. As legal interop increases, companies find it feasible to enter markets that were previously off limits. However, those companies frequently face challenging legal questions that require them to reconcile competing law and interests. For example, as Twitter expanded into more countries, it found itself the recipient of an increasingly large number of demands to remove content. Initially, Twitter responded to these requests by removing Tweets worldwide; if a single country demanded that Twitter remove a Tweet, Twitter would do that for all users, in all markets. However, Twitter eventually decided that one way to address this legal interop challenge would be to use geolocation to remove Tweets only for users visiting from the country that made the legal demand.

Sometimes friction in the form of low levels of legal interoperability may be desirable from a public policy viewpoint. For example, one of the most important considerations for states is cybersecurity. Leaders are extremely concerned about the public security implications of highly interconnected systems. Interoperability of digital systems means that viruses and targeted cyber attacks can have damaging consequences. Viruses and malware frequently take advantage of common, interoperable systems.

Although government-created friction at the *technical* and *data layers* may be controversial,[50] government-created friction in terms of low levels of *legal* interoperability across countries may be both less controversial and beneficial at encouraging a greater diversity of non-interoperable systems that may serve certain defensive purposes.

Legal interoperability is a complex and critical issue, in part because it has the ability to either enable upward mobility in the global economy or to reinforce existing power structures, depending on the choices made. [51]

7 Important issues for the future

Interoperability is not an end in itself. Nor must interoperability always be maximized. Instead, both private actors and regulators must work carefully to optimize the level of interop necessary to meet their objectives. This process of optimization, however, is neither easy nor simple. This paper has described an interop framework, the potential costs and benefits of increased levels of interop, and a variety of approaches for encouraging interop. Thus, when determining the optimum level of interop, all of these factors must be carefully weighed and balanced.

That weighing and balancing is of course necessary from a tactical, outcome oriented perspective, but that perspective can at times obscure the forest for the trees. With emergent and profound new systems and technologies, such as the Internet of Things, quickly becoming more prevalent, it is important to bear in mind some of the big questions and challenges that confront the IoT and other future interoperable technologies. Although these big questions do not yet have good answers, anticipating and considering them now, may help the regulators and others who will struggle with them going forward.

Some of these big questions are:

- **How does society address a proliferation of standards?** In several areas, notably e-health, there is now a ceaseless release of new standards. Some of those standards are no doubt valuable contributions. Many others, however, are conflicting efforts. If standards are generally used to try to bring interoperability to otherwise incompatible approaches, what happens when the sheer number of conflicting standards fragments the market so as to undermine the original goal of interoperability? In the consumer goods market, the solution to this problem is generally to let the standards compete and let the invisible hand of the market choose among the competing standards. But that approach can be expensive, both in terms of time and money. It may also have costs in innovation, as potential market participants wait to invest in the winning standard. For these emerging new technologies and systems, are those costs acceptable? Or is there a way to accelerate the process of choosing the optimal standards from the jungle that is developing?
- **How can interop better manage complexity and scale?** As described above, higher levels of interop can lead to highly complex systems. This complexity and scale, however, has many costs. It can make it hard to identify and correct failures. It can create security risks and magnify the impact of vulnerabilities. At certain scales, it can even represent a form of lock-in, as network effects become predominant. In many ways, successful interop can be its own worst enemy. How can interop better mitigate these problems so as to fully capitalize on the societal gains of large-scale interop?
- **How can highly interoperable systems better communicate to end-users?** As described above, end-users often do not know where to turn when something goes wrong in a highly interoperable

[50] Cory Doctrow, *Crypto wars redux: why the FBI's desire to unlock your private life must be resisted*, The Guardian, Oct. 9, 2014, http://www.theguardian.com/technology/2014/oct/09/crypto-wars-redux-why-the-fbis-desire-to-unlock-your-private-life-must-be-resisted.

[51] Rolf H. Weber, *Legal Interoperability as a Tool for Combatting Fragmentation*, CIGI (Paper Series No. 4, Dec. 2014).

system. If a system behaves like a single, cohesive unit, that is both a success for interop and an obfuscation to the end user. This presents a challenge for interop even under the best of circumstances, where the end-user might have access to greater parts of the system and interact with the system through highly complex interfaces. However, in the Internet of Things or the wearables market, end users are less likely to have access to large parts of the system and the interface may be as small as a watch face. In those challenging circumstances, how can interoperable systems better communicate to end-users?

- **How do issues of surveillance and national security factor into the interop calculus?** When regulators and governments are weighing whether and how to intervene in order to encourage higher levels of interop, to what extent should surveillance and national security factor into that decision? Just as the Internet is value neutral and can be deployed in ways that benefit society and are detrimental to it, so too is interop. Higher levels of interop do not inexorably lead to more surveillance or less, for example. Greater levels of interop can create both a higher risk of surveillance and greater threats to national security, in ways that can be beneficial offensively and threatening defensively. How then do regulators and governments approach issues of interop when considered through the lens of their broader roles and responsibilities?
- **How do regulators optimize interop while operating within the constraints of their complex political environments?** Although regulators and governments have many traditional means of increasing levels of interop (*e.g.*, mandating standards, passing legislation), this paper has highlighted many of the other approaches that exist with the regulatory toolbox. Indeed, in many cases, the alternative means approaches may be the most effective at optimizing interop. Regulators and governments, however, have many constituencies with competing interests. The balancing described in this paper is challenging enough in a vacuum, but is more so in the real world. For example, an agency may feel political pressure to demonstrate big, decisive action, when a more light-handed approach would actually better optimize interop. How then can regulators and governments best take into account their constraints while still optimizing interop?

The answers to these questions are not simple, but wrestling with them will be critical for designing the next generation of interoperable technologies.

Appendix 1: Suggested additional readings

In the text in order to keep the reading experience streamlined, this paper cites a relatively small number of works. A glance through those few notes hints at the wider range of work of academics, practitioners, and regulators that has already gone into seeking to understand this phenomenon. In addition to the notes cited above, below are a selection of other readings that offer a starting point for readers who want to dig deeper into the topic of interop.

Stacy A. Baird "Government Role and the Interoperability Ecosystem" (*I/S: A Journal of Law and Policy* 5, no. 2 [2009]: 219–290).

Yochai Benkler, *Wealth of Networks* (2006).

Yochai Benkler, *The Penguin and the Leviathan: The Triumph of Cooperation over Self-Interest* (2011).

Laura DeNardis, *Opening Standards: The Global Politics of Interoperability* (2011).

"Network Effects," in David Easley and Jon Kleinberg, *Networks, Crowds, and Markets: Reasoning About a Highly Connected World* (2010).

Urs Gasser and John Palfrey, *Interop* (2012).

Marc Levinson, *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger* (2006).

Viktor Mayer-Schoenberger, "Emergency Communications: The Quest for Interoperability in the United States and Europe" (Kennedy School of Government Faculty Research Working Papers Series RWP02–024, March 2002).

John Palfrey, *Intellectual Property Strategy* (2011).

Hal Varian, Joseph Farrell, and Carl Shapiro, *The Economics of Information Technology* (2004).

Rolf H. Weber, "Legal Interoperability as a Tool for Combatting Fragmentation," CIGI (Paper Series No. 4, Dec. 2014).

Jonathan Zittrain, *The Future of the Internet and How to Stop It* (2008).