CHAPTER 1.3

Emerging Issues for our Hyperconnected World

PHILLIPPA BIGGS
with contributions by
TOBY JOHNSON
YOULIA LOZANOVA
NANCY SUNDBERG
ITU

The Internet is changing. From narrowband to broadband, from kilobits to gigabits, from talking people to talking things—our networked world is changing forever. In future, we shall no longer just be connected, we shall be hyperconnected: enjoying super-fast connectivity, always-on, on the move, roaming seamlessly from network to network, wherever we go—anywhere, anytime, via any device.

This vision of our future hyperconnected world builds on the connectivity and functionality made possible by converged next-generation networks (NGNs), but extends the concept of NGN in several ways—through embedded ambient intelligence, automated machine-to-machine (M2M) traffic, and the sheer size and scale of the "Internet of Things" (Figure 1). Today, connected humans are already in the minority of Internet users. According to industry forecasts, the number of networked devices overtook the global population in 2011 and will reach 15 billion connected devices as early as 2015 (Intel's projection in 2009),[1] or a milestone to be achieved as late as 2019 (Google's later forecast, made in 2011),[2] potentially exploding to 50 billion by 2020 (Ericsson's prediction, dating from 2010)[3]—by which time connected devices could outnumber connected people by a ratio of six to one, transforming our concept of the Internet forever. This chapter explores some of the technologies and standards necessary for realizing this vision of our hyperconnected world and its consequences for regulation.

REALIZING OUR HYPERCONNECTED WORLD

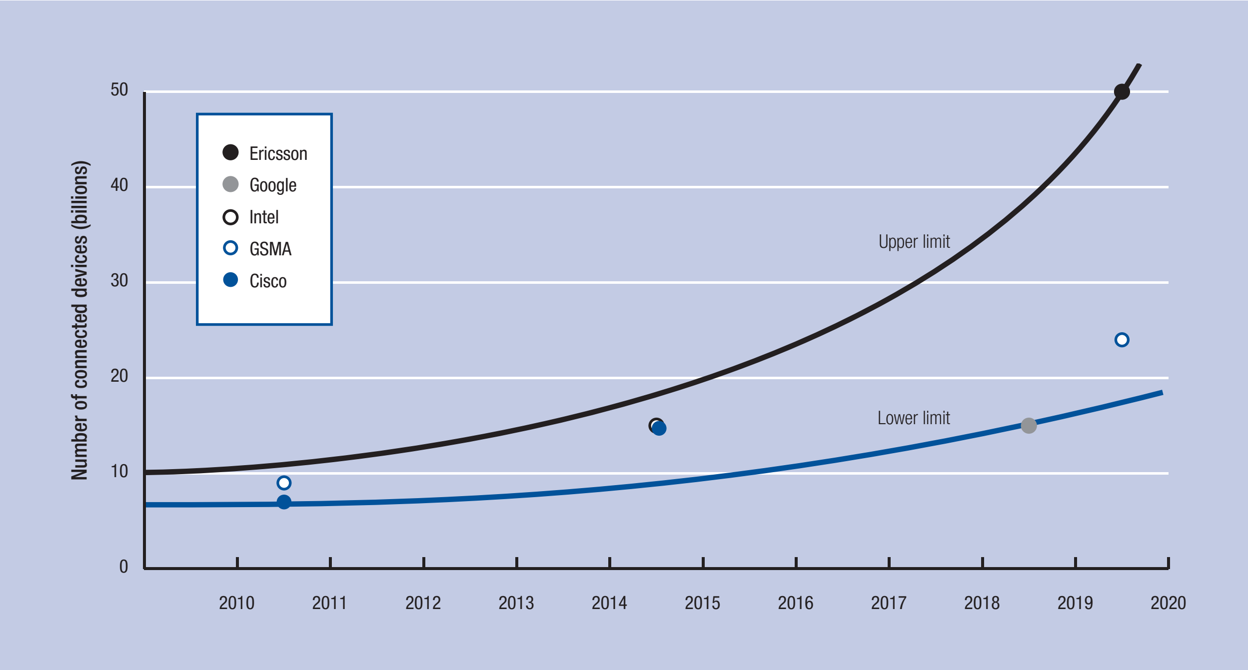
The concept of a hyperconnected world embraces elements of the Internet of Things,[4] M2M,[5] ambient intelligence, embedded computing, and mesh networks.[6] Cisco identifies four key enablers of multi-tasking and passive networking, which it asserts comprise "the two key pillars of hyperconnectivity": [7] (1) the growing penetration of high-speed broadband; (2) the expansion of digital screen surface area and resolution; (3) the proliferation of network-enabled devices; and (4) increases in the power and speed of computing devices.

In the *ITU Internet Report* on the Internet of Things, ITU notes that the development of the Internet of Things and the hyperconnected world encompasses a set of technological developments in different fields—wireless and mobile connectivity, miniaturization, nanotechnology, radio-frequency identification (RFID), and smart technologies.[8] Although the Global System for Mobile Communications (GSM) is currently the most widely used technology for M2M, the World Bank suggests that Wi-Fi is likely to play an important role in the future Internet of Things,[9] with Wi-Fi chips embedded in portable computers and smartphones able to operate on a

---

This chapter reflects the views of its authors only and in no way reflects the views of ITU or its membership.

Figure 1: Projected estimates of the number of Internet-connected devices



Sources: Compiled by ITU, for Intel: Higgenbotham, 2009; for Ericsson: Higgenbotham, 2010; for Google: Malas, 2011; for Cisco: Cisco, 2010; for GSMA: Mobile World Live, 2011.

license-exempt (unlicensed) basis,[10] and with the majority of upgrade costs lying with consumers rather than with the operators. Reportedly one in ten people around the world now use Wi-Fi.[11] Advances in these technologies, taken together, will help realize a miniaturized, embedded, automated Internet of connected devices communicating constantly and effortlessly (Figure 2).

Applications of the Internet of Things are far-reaching, especially when combined with other technologies such as sensor technologies, nanotechnology, or payment systems in the retail sector. Traditional appliances and devices—such as home appliances, vehicles, energy meters, and vending machines—are now entering the network. Perhaps future directions for our hyperconnected future are most readily illustrated with some practical examples.

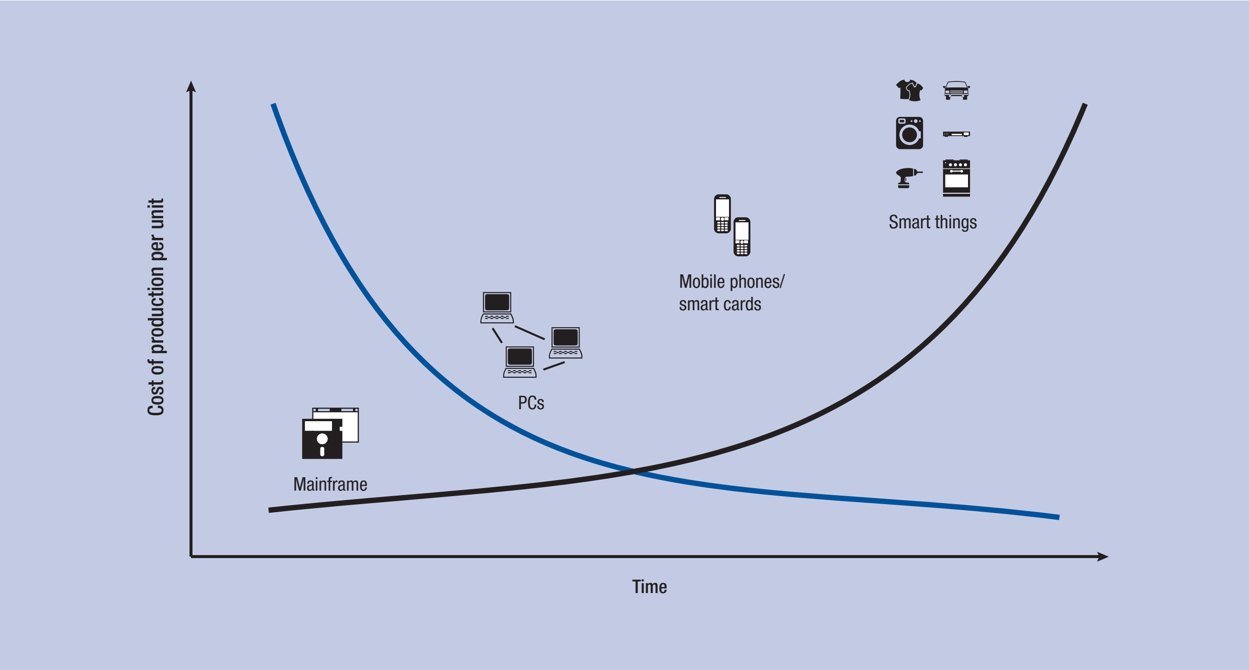
In security and surveillance, commercial security cameras, nannycams, and petcams could transform the way in which objects and premises—as well as people, patients, and pets—are monitored. In the medical and healthcare sector, connecting up patients is being prioritized alongside connecting up digital health records that are accessible by different specialists, pharmacies, or associated health establishments. In the inventory, transport, and fleet management sectors, tracking and status applications are paramount for monitoring the location, status, and condition of stock and food shipments.

Another significant growth area is retail. Besides the integration of mobile banking services or credit card services into mobile phones, various wireless payment and special "contactless" technologies have been developed, which can now be embedded into mobile handsets.[12] For example, mobile operators in Japan and the Republic of Korea have integrated special circuit chips installed into mobile phones to provide payment systems for a number of years now.[13] Some phones also have near field communications (NFC) chips that can be programmed to transfer small sums of money to contactless cash registers.[14]

EXPLOSIVE GROWTH OF DATA

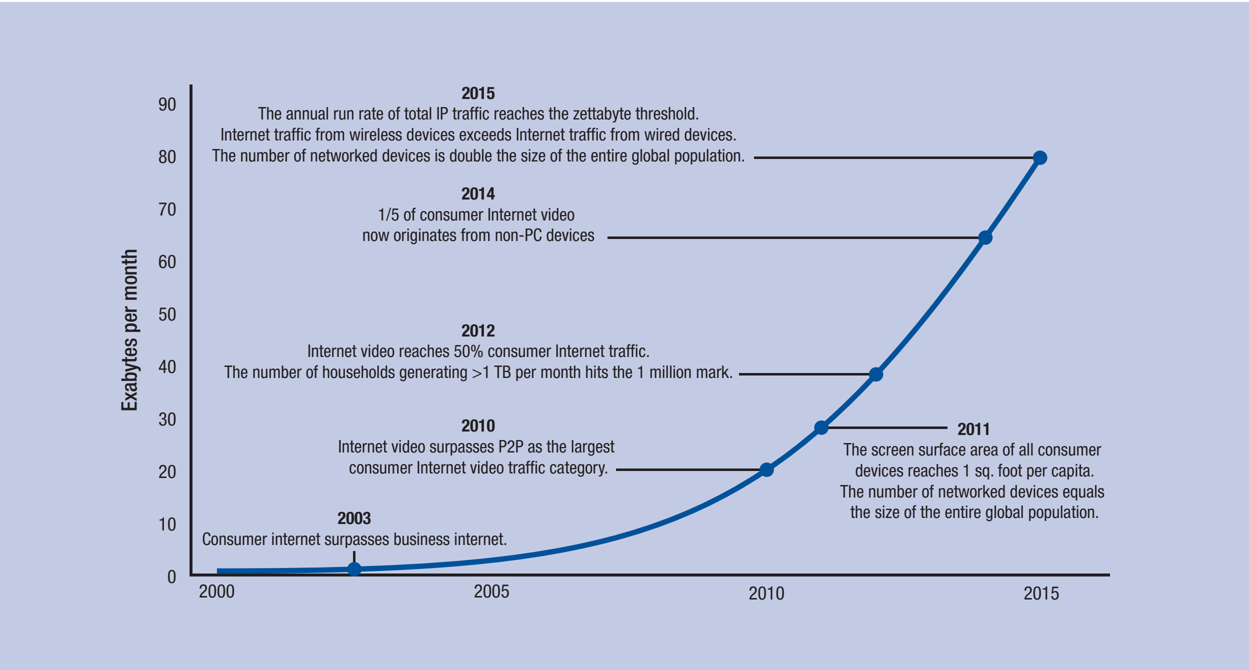
It is no longer the device or the connection that is most important—the data themselves are the new currency of our networked future. Data are now growing exponentially (Figure 3), with both stored and transmitted data showing strong expansion. According to some estimates, more data were created between 2008 and 2011 than in all history prior to 2008. The research consultancy IDC considers that, in 2010, the amount of data transmitted around the world exceeded 1 zettabyte for the first time, while estimating that the size of the digital universe now doubles every two years.[15] Cisco is not so sure, and predicts that annual global IP traffic will only reach the zettabyte threshold (966 exabytes, or nearly 1 zettabyte) in 2015 (Figure 3).[16] Of note, Cisco projects that traffic from wireless devices will exceed Internet traffic from wired devices by 2015—in the hands of end-users, the future Internet looks wireless, mobile,

Figure 2: Miniaturizing and multiplying: Getting smaller and more numerous



Source: ITU, 2005a.

Figure 3: Explosive growth in data



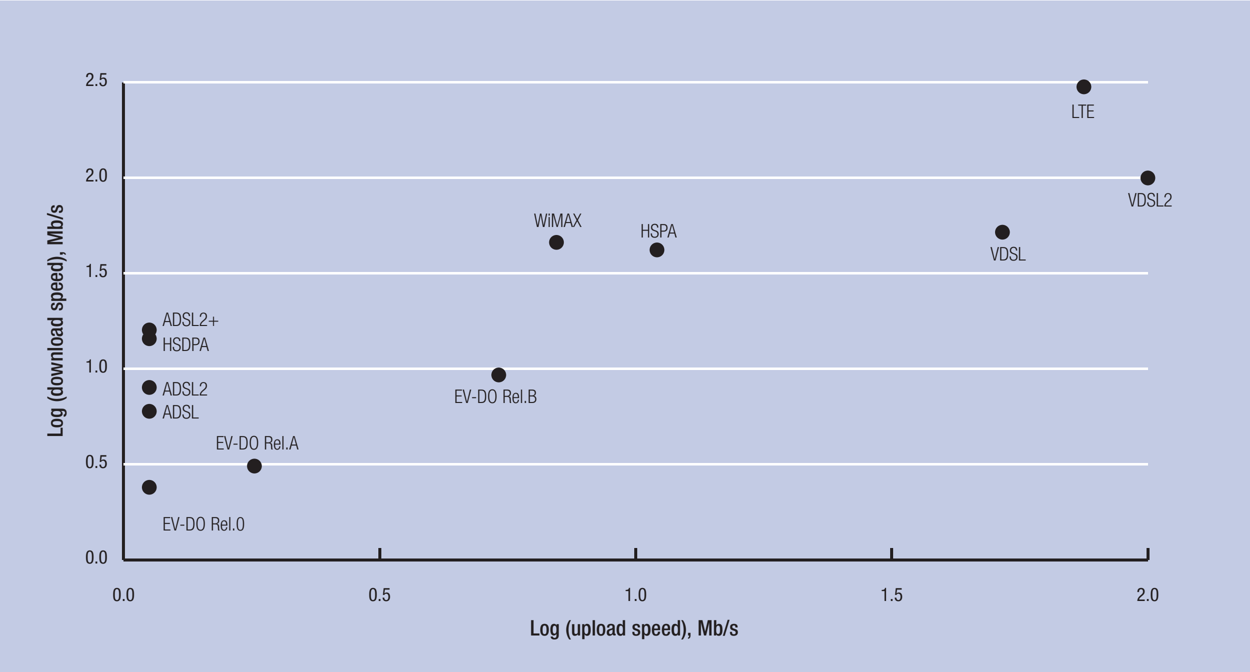
Source: Cisco, 2011.

and portable, even if fiber networks remain essential in the transport layer of the Internet to accommodate such growth in data.

Factors driving this growth in data include the greater availability of hardware, falling marginal costs of digital reproduction (which are now close to zero), automation, and easier digital delivery, with digital assets enjoying an extended lifespan online.[17]

In fact, unless investment in networks can keep up, we risk being overwhelmed by a data deluge: as one leading industry executive puts it, the current generation is the first generation where more data are not

Figure 4: Growth in theoretical throughput speeds and capacity, Mb/s



Source: ITU, with representative speeds cited from various sources: ITU (http://www.itu.int/dms_pub/itu-t/oth/1D/01/T1D010000040003PDFE.pdf); GSMA (www.gsmamobilebroadband.com/about/); Cisco (Pinola and Pentikousis 2008).

Notes: Throughput speeds converted using log to the base 10. ADSL = Asymmetric Digital Subscriber Line, several versions; EV-DO = Evolution Data Only, several releases; HSDPA = High-Speed Downlink Packet Access; HSPA = High-Speed Packet Access; LTE = Long-Term Evolution; VDSL = Very-High-Bit-Rate Digital Subscriber Line; WiMAX = Worldwide Interoperability for Microwave Access.

necessarily good.[18] In any case, it is clear that significant new investments are needed in many forms of information infrastructure. For example, Gartner predicts that global hardware spending on data centers (including servers, storage, and enterprise data center networking equipment) will surpass US$126.2 billion in 2015, up from US$87.8 billion in 2010.[19]

Given such rapid growth in data traffic, in order to continue providing adequate levels of quality of service, telecommunications operators and service providers are adopting more stringent network management practices that include data restrictions, traffic throttling, filtering, and/or the use of data caps or thresholds. Once the cap is exceeded, a subscriber must purchase additional download volumes, or their access speed is reduced or service terminated for that month. Such practices have influenced debates over “net neutrality.” These issues are increasingly likely to come to the fore if data traffic continues to grow at current rates.

Along with network and infrastructure investments, networked technologies are evolving rapidly to accommodate such massive growth in data. The most obvious development is perhaps in speed, with fixed fiber-to-the-home now capable of up to 100 Mb/s for consumers and up to 1 Gb/s for business. High-capacity wireless technologies have historically managed to achieve data rates and capacities of up to a tenth of the fastest equivalent wireline technology, with the latest data rates for LTE amounting to some 5–12 Mb/s download, and some 2–5 Mb/s upload. Its theoretical maximum download speeds are much higher, at 300 Mb/s download and upload speeds of 75 Mb/s (Figure 4).

However, measuring technological progress in terms of speed and data capacity alone is too simplistic—technological progress is transforming the way we live.

REGULATORY CONSEQUENCES

The impact of the Internet of Things promises to be more pervasive and far-reaching than merely convenient wireless payment systems, smart gadgets, and Internet-enabled devices (Box 1). The embedded Internet will blur boundaries between economies, societies, and industries. Many industries (including energy, transport, financial services, healthcare, and media) now rely on integrated information technology (IT) systems and infrastructure to monitor, control, manage, and deliver their services. Integrating Internet connectivity into devices and things opens up new risks that information will be unintentionally put into the hands of people who should not have access to it. These risks—as well as opportunities—arise in determining who exactly knows what, who can access what, and who can communicate with which device, as well as the dissemination and use of different data across different sectors. This section goes on to review the changing role of regulators, as well as some of the key regulatory consequences of a hyperconnected

ICT environment in open access and infrastructure-sharing, technical numbering and address issues, switching and roaming requirements, and net neutrality.

The changing role of regulators

Perhaps the greatest overall impact of the hyperconnected world lies in transforming the role of regulators in a converged telecommunication environment. Establishing a separate telecommunication/ICT regulator has been the basis of the sector reform process in many countries. By the end of 2011, 158 separate regulators had been established worldwide, in around four-fifths of all countries around the globe. Every year, ITU hosts a Global Symposium for Regulators (GSR) to debate the issues transforming the ICT environment and to consider their impact on the regulatory environment, and publishes the outcomes of the GSR in the form of best practice guidelines.[20]

In recognition of the technological convergence taking place between infrastructure and content, many telecommunication regulators are now moving to adopt growing responsibilities over the regulation and monitoring of content and broadcasting (Figure 5). Some other countries have also moved to expand the mandate of the regulator to include information technology, broadcasting content, and/or spectrum management.

In 2010, 16 percent of all telecommunication/ICT regulators worldwide included regulation over broadcasting content within their mandate (with a few sharing that responsibility with a ministry). Although Internet content is not regulated in more than 44 percent of countries worldwide, regulation of Internet content lies within the mandate of some 13 percent of telecommunication/ICT regulators. Thirty percent of regulators include IT in their mandate; they share this responsibility with the ministry or other government bodies in 12 percent of these cases.[21]

As the Internet becomes embedded in many more everyday objects, some observers suggest that the role of ICT regulators in a converged ICT environment will be far more pervasive and touch on many more facets of our hyperconnected lives than just competitive market structure, network interconnection, pricing, and consumer protection. The advent of high-speed networks and new kinds of content creates an important leadership role for government policymakers and ICT regulators in stimulating the demand for broadband and in promoting investment in infrastructure.[22] In fact, ICT regulators may become indirectly involved in many more spheres of influence, reflecting the involvement of ICT infrastructure and services in many aspects of our daily lives.

Open access and infrastructure sharing

Open access approaches and infrastructure sharing are likely to be the foundations for future network growth.[23] Various different approaches have been adopted by national governments. A number of countries (e.g., Australia, Malaysia, Qatar, and Singapore) have embarked on the creation of entirely new national broadband networks (NBNs), which deploy fiber optic technology throughout the core network and, crucially, in the access networks that extend to end-customers. Investments in these networks are huge (e.g., Australia's NBN will cost $A 43 billion, or US$45 billion), which has led to the re-nationalization of infrastructure in some countries in order to obtain economies of scale and preferential government borrowing rates.

Other countries (e.g., in Europe) are trying to work within existing regulatory frameworks to find means of improving investment incentives for network operators while maintaining competitive supply.[24] These strategies involve lightening the regulatory requirements on dominant operators (or those with significant market power) as a support or reward for the development of ubiquitous broadband networks.

Developing countries that lack the public funds to support a full NBN, as well as those with no existing privately owned fixed network infrastructure, can pursue various hybrid solutions (e.g., Tanzania and Mozambique). These initiatives usually involve public investment (typically in the form of low-interest loans) in a fiber backbone network, coupled with various forms of support and encouragement for privately funded access networks using a range of technologies (such as W-CDMA or Wideband Code Division Multiple Access

Box 1: Contactless payments: Near field communication payments in Turkey

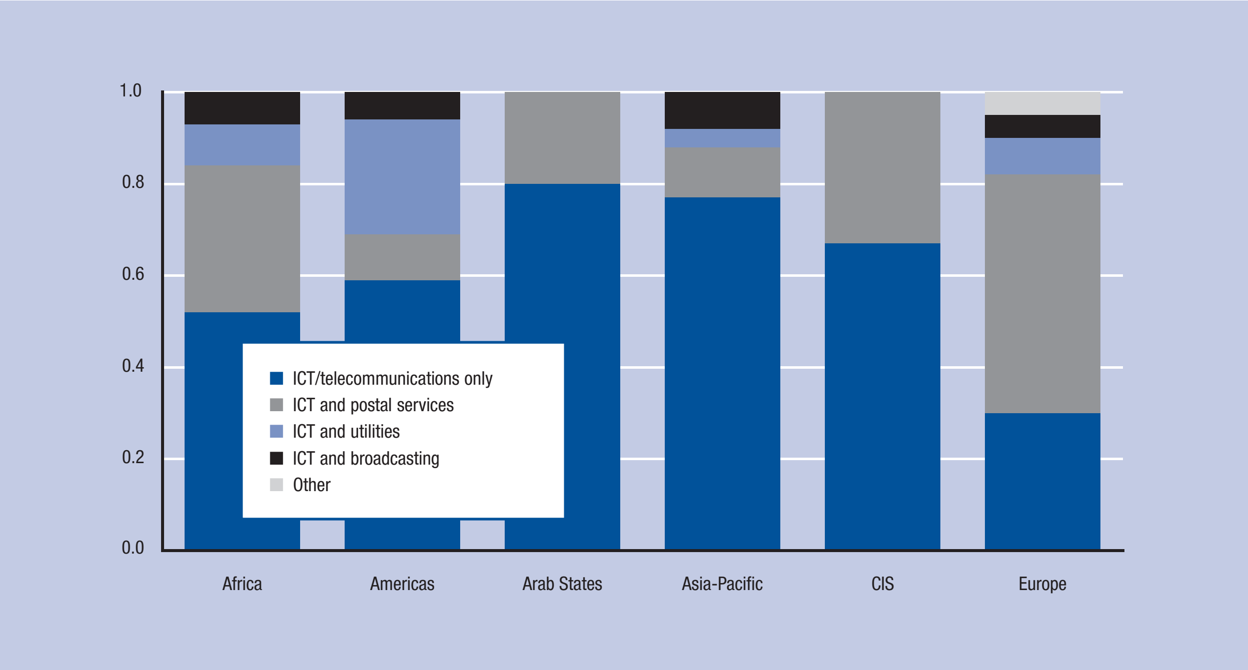
The World Bank's *ICT 4 Development Report 2012* (forthcoming) underlines the notion that growth in mobile money systems is built on a complex ecosystem spanning the mobile, retail, and financial sectors that are comprised of banks, mobile operators, the retail sector, policymakers, regulators, and consumers.

This is a point illustrated by the growth of near field communication (NFC) in Turkey. Turkish banks have embraced NFC enthusiastically as a form of wireless payment. With support from the Ministry and the Government of Turkey, and in conjunction with retailers, Turkish banks and mobile operators have promoted NFC as a quick, easy, and convenient way to pay for purchases. Operators and banks have launched consumer awareness campaigns to promote the advantages of this form of payment. They have been rewarded by consumer enthusiasm for the new technology, which has been deployed in many modern commercial shopping centers in large Turkish towns. It remains to be seen whether the success of NFC in Turkey can be replicated to the same extent elsewhere.

Source

World Bank, forthcoming; BBC 2011.

Figure 5: Converged regulation: The mandates of regulators, 2010



Source: ITU World Telecommunication/ICT Regulatory Database; ITU, Forthcoming.

Evaluation; HSDPA, or High-Speed Downlink Packet Access; and WiMAX, or Worldwide Interoperability for Microwave Access, for example).

Whichever strategy is adopted, open access usually means that all suppliers, whether in horizontal or vertical markets, are able to obtain access to the new network facilities on fair and equivalent terms. The definition of open access varies from country to country, depending on the regulatory model adopted; the terms and conditions of access clearly vary. Nevertheless, open access is essential to avoid monopolistic frameworks and is generally required wherever there are economic bottlenecks preventing competitive supply. However, open access is progressively less important moving up the infrastructure layers, provided that it is available at the lower layers and there is sufficient incentive in its regulation to encourage investment in infrastructure.[25]

Numbering and addressing issues

Given the massive growth forecast for connected devices, numbering and addressing issues could become a major concern in providing all these network-enabled devices with their own addresses. In a future where many consumer equipment and electronic devices will need connectivity and hence their own identifiers (although not necessarily their own Internet addresses), some stakeholders envisage a need for greater and better numbering resources (others argue that this is not a problem at present, as most M2M applications currently use GSM).

Potential shortages in address space through full allocation (but not necessarily use) of Internet Protocol version 4 (IPv4) addresses (for example, triggered by the allocation of the two last blocks of remaining IPv4 address space on February 1, 2011) could be averted in the long run by the transition to Internet Protocol version 6 (IPv6).[26] Introducing IPv6 will take the address space from around 4 billion (2^{32} or 4,294,967,296 addresses) to 128-bit addresses, so the new address space supports 2^{128} or a total of 3.4×10^{38} addresses, enough for a trillion tags to be assigned every day for a trillion years. Opinions are divided about how much of a problem shortages in IPv4 address space are likely to pose. Some observers see this as a major issue that requires transition to IPv6 as a matter of urgency; others argue that greater use of network address translation (NATing) and more efficient use of IPv4 address space (e.g., such as recovering unused IPv4 addresses) will permit continued expansion of the IPv4 space, including for mobile devices.[27]

However, some countries and some regulators are not yet making adequate investments in capacity building or preparedness for the IPv6 transition, while mobile networks may not yet be IPv6-enabled (and they are unlikely to be so for some time yet). According to Detecon, this could amount to the digital equivalent of a fault line running through the future Internet of Things, between its wireline and wireless halves. Detecon identifies four possible options for resolving this issue: (1) extending the existing mobile numbering range; (2) using a new mobile numbering range; (3) using an international mobile numbering range; and (4) using internal network numbers.[28]

Significant issues surround access and digital identity management more broadly. Today's secure numbering system means that, bar an erroneous wrong number, callers can be relatively confident that a message left on an answering machine should reach the intended recipient. In connecting up objects such as webcams, we may be confident we have accessed the right webcam to monitor our children at school or doing their homework at home remotely, but who else may also be able to access it?

Switching and roaming issues

Various issues arise with regard to switching and roaming. With regard to switching, M2M applications are often bound to a mobile operator for the device lifetime, mainly because: (1) M2M terminals are currently mainly based on GSM technology; (2) only operators can get E.212 (or international mobile subscriber identity—IMSI) numbers; and (3) regulators do not require the portability of IMSIs. This means that the mobile operator is at an advantage when clients want to negotiate a switch from one operator to another, or even in negotiating new rates. For large numbers of devices distributed all over a country (region or continent), switching subscriber identity module (SIM) cards to migrate devices from one mobile operator to another is simply not an option (Box 2).

With regard to roaming, many M2M applications (e.g., wireless payment systems) rely on full international mobile coverage. Providers cannot always negotiate competitive regional or global roaming solutions (for both the M2M application provider and the mobile operator) and often use intermediaries. This leaves intermediaries in a stronger negotiating position (regarding rates, etc.) than either the M2M application provider or mobile operator. There is a potential role for regulators here in considering whether intervention is necessary, and potentially in negotiating roaming requirements and rate interventions.

Net neutrality

Given the explosive growth in data, regulators are likely to become increasing concerned with traffic management practices. The ITU *GSR11 Discussion Paper* "Open Access and Regulation in the Digital Economy" identifies the main aspects of net neutrality as traffic management, transparency, non-discrimination, and potential differentiation between price and quality of service in traffic management.[29] Currently, many regulators are launching public consultations and investigations into traffic throttling practices, but many have stopped short of intervening, with most regulators content to call for greater transparency and disclosure in the industry's best interests to safeguard consumers. For example, the European Commission (EC) policy on net neutrality published in April 2011, *The Open Internet and Net Neutrality in Europe,*[30] calls for greater disclosure of traffic management practices to ensure that consumers are well informed (Table 1). The EC recognizes that traffic management is necessary to ensure the smooth flow of Internet traffic, particularly when there is network congestion—which looks increasingly likely to arise, given current growth rates in data traffic.

With regard to data, the assets at risk in a smart society include not only the networks, but also data and information assets (including customer identities and records). For example, the Ponemon Institute estimates that the cost of a data breach rose from US$6.8 million in 2009 to US$7.2 million in 2010, with the average cost per compromised record in 2010 reaching US$214,[31] up 5 percent from US$204 in 2009.[32] Information will be abundant and everywhere, but can we learn to live with such abundance—are we information-rich or information-overloaded? If we can learn to live with the data deluge, the prospects of personalized services tailored to customers and their search behavior offer tantalizing possibilities.

It is not just data breaches that are of concern: the data we willingly give away about ourselves are of equal concern in the web that never forgets—where instant status updates, sharing via retweets, and cascading distribution of information in online feeds are common. The speed with which we work and communicate is accelerating, while the scale and distribution of our

Box 2: M2M applications in the Netherlands

In 2010, Logica was commissioned by the Dutch Ministry of Economic Affairs to examine the technical solutions to the problem of migrating M2M providers for clients with large numbers of M2M devices. This poses a major logistical problem, where the thousands or tens of thousands of M2M devices are distributed all over the country, sometimes in hard-to-reach places.

After extensive study, Logica concluded that number portability does not work for SIM cards, because the first five or six digits of an IMSI number (which conforms to ITU numbering standard E.212) are operator-specific, so in order to change operators, the IMSI numbers would have to change. Logica suggests that remotely updating IMSI numbers on SIM cards is another technical possibility, but there are no standardized solutions for this, only proprietary ones.[1] Instead, Logica identified a regulatory solution whereby large-scale M2M deployments could use their own SIM cards carrying their own IMSI and cryptographic parameters, so it is no longer necessary to change the data on the SIM-card, the solution used by some Mobile Virtual Network Operators (MVNOs) today.

Source

van der Berg, 2010.

Table 1: Status of net neutrality initiatives in selected countries

Stage in process	Position along the spectrum (least to most stringent)	Country
No consultation	Considered net neutrality, but found no problems requiring a consultation and subsequent rule; will continue to monitor	Denmark Germany Ireland Portugal
	Non-binding neutrality guidelines	Norway
In consultation stage	Information gathering on current practices to potentially establish rules	Italy
	Transparency/disclosure rules proposed, but no traffic management	United Kingdom
	Transparency/disclosure rules and traffic management/ non-discrimination rules proposed	Brazil Sweden
Rules/legislation adopted	Transparency/disclosure rules but no traffic management/ non-discrimination rules	European Commission
	Transparency/disclosure rules and traffic management/ non-discrimination rules	Canada Chile France Netherlands United States

Source: Telecommunications Management Group, Inc., quoted in World Bank and infoDev, 2011.

real-time communications are growing. It seems unlikely that separate models of regulation for telecommunication and data protection can be sustained in our converged era—how can regulation evolve to keep up? The debacle over the launch of Google Buzz and ongoing concerns over privacy settings on Facebook are already highlighting gaps in a converged regulatory environment.

STANDARDS AND INTEROPERABILITY IN A NETWORKED WORLD

In a hyperconnected world of so many networked devices, identification, interoperability, performance standards, and communication protocols are clearly essential to ensuring that different devices and systems can communicate across different networks.

The Internet of Things will contain billions of objects that must be uniquely identified, a challenge for which there is, so far at least, no internationally agreed solution. A unique identification scheme is probably the biggest challenge of the Internet of Things. Some identification schemes for identifying objects are based on bar codes. Other schemes are under development to address the needs of specific applications. ITU has launched an Internet of Things Global Standards Initiative, enabling experts to come together physically to conduct standards-based development work. For example, ITU-T Study Groups 11 and 13 are studying architectures and testing requirements for networks using tag-based identification, while ITU-T Study Group 17 is studying the security and privacy of tag-based identification mechanisms.

One of the biggest issues in identity management today is that identifiers used in one network might not be understandable or usable in another network. In the Internet of Things, consumers are likely to want to use different objects across multiple kinds of heterogeneous networks, which will need the identities of things to be "federated" or capable of being translated accurately and recognized by different networks.

The solution to this challenge does not necessarily involve a single global identity for a device on a network. Rather, a "zoo" or collection of associated identities—as exists today—may continue. For example, in some domains, an identity may be just an email address. In other areas, such as social networks, an identity is far more complex and more loaded. It may include a real name and links to other people. Some identities may be created temporarily (such as those used for tracking people at a conference, for example, or those used for contractors working within companies). Mapping identities like these together to make them interoperable, while accommodating privacy and security concerns, is a vital part of identity management.

Indeed, connecting up many different kinds of object to the Internet may present one of the greatest standardization challenges yet. Sectors likely to be touched by the need for standardization include e-health, e-government, automotive, geo-information, remote sensing, home networking (including home automation), e-commerce, and even the mitigation of climate change.

As with any new area of standardization, one of the first important steps is to agree the scope of the work and standard terminology, so experts from across different disciplines can all use the same language. ITU's Internet of Things Global Standards Initiative aims to develop a work plan for Internet of Things standardization and the detailed standards or Recommendations necessary for the deployment of the Internet of Things on a global scale, taking into account the work done in other standards development organizations in areas such as M2M, network aspects of identification (NID), ubiquitous sensor networks (USN), machine-oriented communication, and the web of things, among other areas.

CONCLUSIONS

We are moving toward an era of an embedded, ubiquitous, and invisible Internet. A hyperconnected world of communicating devices has consequences for us all in the way we live, as more and more of the everyday real world around us becomes reflected online. Status updates, location updates, changes in status or conditions: these will all become part either of what we know, or of what is known—or knowable—about us.

The outcome for our hyperconnected world might not necessarily be Big Brother, but it might not be far off either. Regulators and policymakers have a vital role to play at this point in time in establishing the *mores* and norms for the online world—in what is and is not acceptable and in developing principles and best practices going forward, so that the risks and opportunities of our hyperconnected world are managed appropriately to protect both consumers and citizens.

NOTES

1 Higgenbotham 2009.

2 Malas 2011.

3 Higgenbotham 2010.

4 The concept of the Internet of Things was first referred to by Mark Weiser in his 1991 paper, "The Computer for the 21st Century." ITU has adopted the following working definition of the *Internet of Things* (as of August 2011): "In a broad perspective, the IoT can be perceived as a vision with technological and societal implications. From the perspective of technical standardization, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst maintaining the required privacy."

5 ITU has recently established a new Focus Group on M2M service layer aspects at its TSAG. See ITU 2012; ITU-T. N.D.

6 ITU describes mesh networks as "A way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around blocked paths by 'hopping' from node to node until a connection can be established" in the glossary of ITU-D's *Trends in Telecommunication Reform 2009.* See ITU-D 2009.

7 Cisco 2010, p. 3.

8 ITU 2005a, 2005b.

9 World Bank and infoDev 2011.

10 ITU has designated the 2450 MHz and 5800 MHz bands for industrial, scientific, and medical (ISM) applications that "must accept harmful interferences." This is often interpreted to mean that they are considered unregulated. See *Frequently Asked Questions* on the ITU-R website, available at http://www.itu.int/ITU-R/terrestrial/faq/index.html.

11 Wi-Fi Alliance N.D.

12 World Bank, Mobile Trends report, forthcoming, written by Michael Minges.

13 Terri and Hayashi 2007.

14 Perez 2011.

15 IDC 2011.

16 Cisco 2011.

17 See Denton 2011.

18 *Google Think Quarterly* 2011.

19 Telecompaper 2011.

20 See ITU's regulatory website, http://www.itu.int/ITU-D/treg/index.html, for details of the latest Global Symposium for Regulators, GSR-2011 (http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR11/index.html), as well as previous GSR events, http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/index.html.

21 ITU 2011a.

22 ITU 2011b.

23 This section is extracted from Rogerson 2011.

24 Rogerson 2011.

25 Rogerson 2011. D. Rogerson, taken from his speech at the GSR 2011.

26 See, for example, Middleton 2011.

27 See, for example, Arbor Net's discussion of IPv6 in relation to World IPv6 Day sponsored by the Internet Society (ISOC) in Malan 2011.

28 Detecon presentation on M2M, "Machine-to-Machine Communications (M2M) Creating a business enabling environment for one of the most promising growth markets." Personal communication.

29 Rogerson 2011.

30 European Commission 2011.

31 Messmer 2011.

32 Messmer 2010.

REFERENCES

BBC. 2011. *BBC Click,* November. Available at http://news.bbc.co.uk/2/hi/programmes/click_online/default.stm.

Cisco. 2010. "Hyperconnectivity and the Approaching Zettabyte Era." Cisco White Paper, June 10. Available at http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/Hyperconnectivity_WP_e-book.pdf.

———. 2011. "Entering the Zettabyte Era." *Cisco©Visual Networking Index,* June 10. Available at http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI_Hyperconnectivity_WP.html .

Denton, A. 2011. "Intellectual Property Rights in Today's Digital Economy." *GSR11 Discussion Paper.* Geneva: ITU. Available at http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR11/documents/05-Intellectual-property-E.pdf.

European Commission. 2011. *Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions: The Open Internet and Net Neutrality in Europe* ("Open Internet Report"). April 19. Available at http://ec.europa.eu/information_society/policy/ecomm/doc/library/communications_reports/netneutrality/comm-19042011.pdf.

Higgenbotham, S. 2009. "Intel Inside Becomes Intel Everywhere." GigaOM, March 2. Available at http://gigaom.com/2009/03/02/intel-inside-becomes-intel-everywhere/.

———. 2010. "Ericsson CEO Predicts 50 Bn Connected Devices by 2020." GigaOM. Available at http://gigaom.com/2010/04/14/ericsson-sees-the-internet-of-things-by-2020/.

Google Think Quarterly. 2011. The Data Issue, March. Available at http://www.slideshare.net/ibrahimcesar/think-quarterly-the-data-issue.

IDC. 2011. *The 2011 Digital Universe Study: Extracting Value from Chaos.* Available at http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm.

ITU. 2005a. *ITU Internet Reports 2005: The Internet of Things.* Geneva: ITU. Available at http://www.itu.int/osg/spu/publications/internetofthings/.

———. 2005b. *ITU Internet Reports 2005: The Internet of Things, Executive Summary.* Geneva: ITU. Available at http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.

———. 2011a. *Trends in Telecommunication Reform 2010/11.* Geneva: ITU. Available from http://www.itu.int/pub/D-REG-TTR.12-2010

———. 2011b. "Effective ICT Regulation Is Critical to Economic Growth." Press Release, March 31. Available at http://www.itu.int/net/pressoffice/press_releases/2011/07.aspx.

———. 2012. "ITU Establishes Focus Group on Machine-to-Machine Service Layer." *ITU-T Newslog,* January 16. Available at http://www.itu.int/ITU-T/newslog/ITU+Establishes+Focus+Group+On+MachinetoMachine+Service+Layer.aspx.

———. Forthcoming. *Trends in Telecommunication Reform 2011/12.* Geneva: ITU.

ITU-D. N.D.a. *Global Symposium for Regulators (GSR).* Available at http://www.itu.int/ITU-D/treg/index.html.

———. N.D.b. *11th Global Symposium for Regulators (GSR11) & 4th Global Industry Leaders' Forum (GILF).* Available at http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR11/index.html.

———. N.D.c. *Global Symposia for Regulators: The History.* Available at http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/index.html.

———. 2009. *Trends in Telecommunication Reform 2009.* Geneva: ITU. Available from http://www.itu.int/pub/D-REG-TTR.11-2009.

ITU-T. N.D. *Focus Groups. FG M2M* "Focus Group on Machine-to-Machine (M2M) Service Layer." Available at http://www.itu.int/en/ITU-T/focusgroups/m2m/Pages/default.aspx.

Malan, R. 2011. "World IPv6 Day: Final Look and 'Wagon's Ho!'" ARBORSERT. DDoS and Security Reports: The Arbor Networks Security Blog, June 9. Available at http://ddos.arbornetworks.com/2011/06/world-ipv6-day-final-look-and-wagons-ho/.

Malas, N. 2011. "Google Sees 15bn Connected Devices in Next Five to Eight Years." *total telecom,* March 3. Available at http://www.totaltele.com/view.aspx?ID=463304.

Messmer, E. 2010. "Data Breach Costs Top $200 per Customer Record." *NETWORKWORLD,* January 25. Available at http://www.networkworld.com/news/2010/012510-data-breach-costs.html.

———. 2011. "Corporate Data Breach Average Costs Hits $7.2 million." *NETWORKWORLD,* March 8. Available at http://www.networkworld.com/news/2011/030811-ponemon-data-breach.html.

Middleton, J. 2011. "More Machines than Man, Now . . . " telecoms.com, interview with Axel Pawlik, April 12. Available at http://www.telecoms.com/26419/more-machines-than-man-now%E2%80%A6/.

Mobile World Live. 2011. "Study: 24B Connected Devices by 2020 Creates US$1.2 Trillion Revenue Opportunity." *Mobile Business Briefing,* October 11. Available at http://www.mobilebusinessbriefing.com/articles/study-24b-connected-devices-by-2020-creates-us-1-2-trillion-revenue-opportunity/18105/.

Perez, S. 2011. "Getting Ready for Google Wallet, Sprint Switches on Nexus S 4G's NFC Chip." *ReadWriteWeb,* July 11. Available at http://www.readwriteweb.com/archives/google_wallet_coming_with_sprint_nexus_s_4g_update.php.

Pinola, J. and K. Pentikousis. 2008. "Mobile WiMAX." *Internet Protocol Journal* 11 (2), June. Available at www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_11-2/112_wimax.html.

Rogerson, D. 2011. "Open Access Regulation in the Digital Economy." GSR11 Discussion Paper. Geneva: ITU. Available at http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR11/documents/02-Open%20Access-E.pdf.

Telecompaper. 2011. "Data Centre Hardware Spending to Hit USD 99 Bin in 2011." October 14. Available at http://www.telecompaper.com/news/data-centre-hardware-spending-to-hit-usd-99-bln-in-2011.

Terri, B. and F. Hayashi. 2007. "Complex Landscapes: Mobile Payments in Japan, South Korea, and the United States." Payments System Research Briefings, September. Available at http://www.kansascityfed.org/Publicat/PSR/Briefings/PSR-BriefingSept07.pdf.

van der Berg, R. 2010. "Logica Report on Switching Costs for M2M." Logica. Available at http://www.prepaidmvno.com/2010/09/21/logica-report-on-switching-costs-for-m2m-rudolf-van-der-berg/.

Weiser, M. 1991. "The Computer for the 21st Century."Scientific American 265 (3): 94–104.

Wi-Fi Alliance. N.D. Organization. Available at www.wi-fi.org/organization.php.

World Bank. Forthcoming. *Information and Communications for Development Report 2012*. Washington DC: World Bank.

World Bank and infoDev. 2011. *Broadband Strategies Handbook*. Washington DC: International Bank for Reconstruction and Development/World Bank. Available at http://www.infodev.org/en/Publication.1118.html.