Robert Kenny

The challenges of regulating the Cloud

March 2011

COMMUNICATIONS
CHAMBERS

Contents

The author is grateful to Vodafone for the funding of this paper. The opinions contained are his own, and do not necessarily reflect the views of Vodafone.

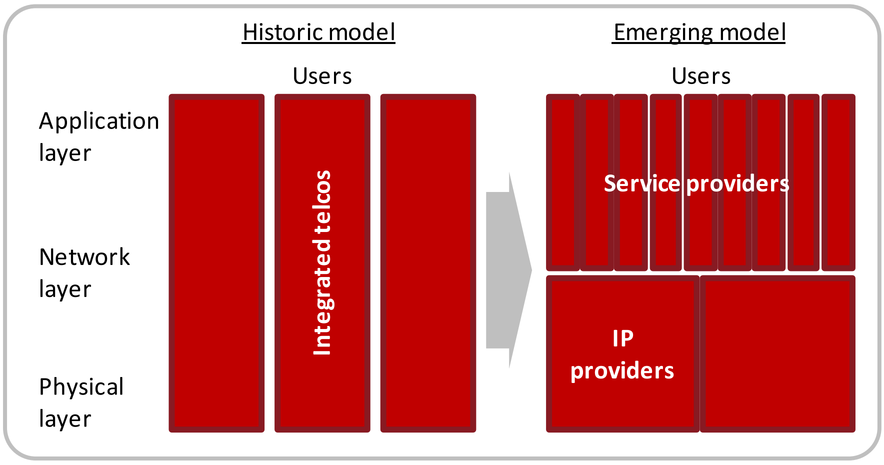
Introduction

The structure of communications services is undergoing fundamental change. Historically, integrated service providers (including, but not limited to the PTTs) provided 'the full stack', everything from underlying physical assets through to the user interfaces, billing, customer care and so on.

Telecoms regulation from the '80s on began to chip away at this model, introducing resellers, MVNOs and other entities who provided services without substantial infrastructure of their own. However, these were relatively minor departures from the integrated model, which remained dominant.

However, the advent of near-ubiquitous IP networks has drastically accelerated this change. The availability of the internet as an open, cheap transport layer enabling access to 530m global broadband subscribers[1] has resulted in an inrush of service providers. These typically own little in the way of network but, via software and servers, are able to provide attractive services over the internet.

Figure 1 Changing structures for communication services



This transition continues, with current focus being on the shift to 'the cloud' – that is, the shift from companies (and consumers) managing their own IT on their own premises to centralized provision of services, with companies accessing their information via web connections.

This restructuring has indisputably been hugely beneficial. It has reduced barriers to entry, enabled massive innovation and brought significant benefits to consumers. However, it has also brought negative consequences. In particular, it makes obsolete a number of assumptions that have underpinned historic regulation of communications and the

[1] Telegeography, *IPTV subs reach 45 million as telcos achieve 10% penetration rate*, 17 March 2011 http://www.telegeography.com/cu/article.php?article_id=36492&email=html

wider economy. In this paper we outline the magnitude of the transition, discuss some of the reasons this throws up substantial challenges for regulation and enforcement, and discuss a range of specific examples of where problems have arisen.

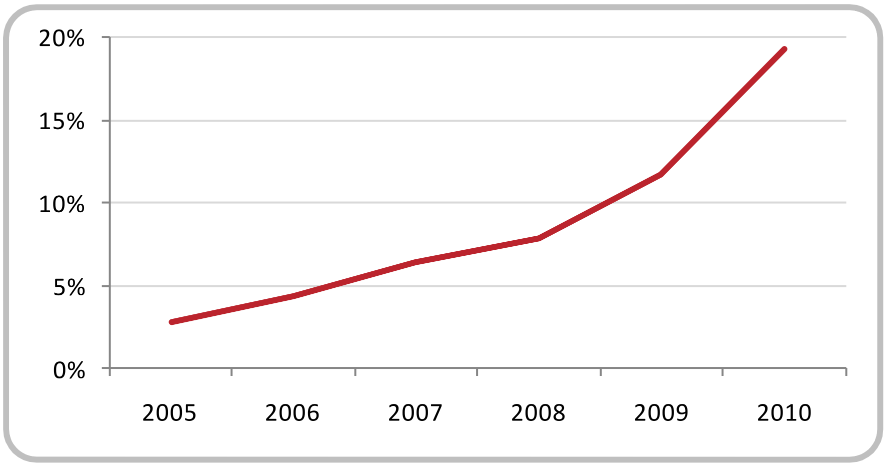
The rise of the independent service layer

The range of services available riding on the internet is of course massive. In this section we focus on some of the key communications services.

Voice services

Historically voice services have been the core of integrated telcos' business. However, international voice in particular has seen a rapid transition to 'over the top' VoIP services. Skype alone now represents 19% of international voice traffic:

Figure 2 Skype traffic as a percentage of international voice[2]



Today Skype has 663m registered users, and revenues of $860m[3]. Skype's origins are as a PC based service, but the rise of smartphones is giving impetus to a new set of VoIP providers such as Nimbuzz and Tru (in addition to Skpe's own mobile app). Juniper estimates there are already 100m users of 'mVoIP', and by 2015 there are expected to be 471bn minutes of mVoIP traffic[4].

Email services and instant messaging

Hotmail, founded in 1996, was one of the first cloud services. It was followed by many other webmail offerings, and by September 2010 there were 127m unique users of webmail services in the US[5] (compared to a population of approximately 230m).

[2] Based on Telegeography data. Telegeography only tracks carrier voice and Skype, not other VoIP only providers

[3] Telecompaper, *Skype grows FY revenues 20%, reaches 663 mln users*, 8 March 2011
http://www.telecompaper.com/news/skype-grows-fy-revenues-20-reaches-663-mln-users

[4] Gigaom, *471 Billion Mobile VoIP Minutes By 2015*, 1 July 2010
http://gigaom.com/2010/07/01/mobile-voip-forecast/

[5] Compete, *Gmail's buzz – much bigger than its bite?*, 11 November 2010
http://blog.compete.com/2010/11/11/gmails-buzz-much-bigger-than-its-bite/

Radicatti estimate there were 2.4bn instant messaging accounts worldwide in 2010[6]. This compares to 1.2bn fixed phone lines worldwide[7] in 2009.

Filesharing

Peer-to-peer filesharing services such as BitTorrent, Gnutella and eDonkey have enabled consumers to both access and distribute large files, particularly video. Cisco estimate[8] that filesharing, which is predominantly P2P, represented 25% of global internet traffic in 2010. While now being overhauled by other forms of internet video (such as YouTube and IPTV), it nonetheless is expected to grow at 23% annually until 2014.

Video services

With the advent of widespread broadband, the internet has become a viable platform for television services. In the UK the BBC's iPlayer delivered 94m TV shows over the internet in February 2011[9]. In the US Hulu (an internet TV JV of leading broadcasters) had 143m viewing sessions in the same month[10].

User Generated Content and Social Networking

Services such as Facebook, YouTube and Twitter have provided new ways for consumers to communicate. Facebook is #1 or #2 in 17 of the top 30 internet markets in the world[11]. Users spend approximately 700bn minutes per month on Facebook[12], or roughly one hour, 40 minutes for every person on the planet. Put another way, the monthly time spent on Facebook is equivalent to the working hours of the combined workforces of France, the UK and the Netherlands. Despite having 500m active users, Facebook has a little over 2,000 employees – roughly a quarter of Telecom New Zealand.

While YouTube is not quite the scale of Facebook, it is a top 5 site (by reach) in seven out of the ten largest internet markets. It represents 10%

[6] Radicati Group, *Email Statistics Report, 2010*, April 2010 http://www.radicati.com/wp/wp-content/uploads/2010/04/Email-Statistics-Report-2010-2014-Executive-Summary2.pdf

[7] ITU, http://www.itu.int/ITU-D/ict/statistics/index.html

[8] Cisco, *Cisco Visual Networking Index*, 2 June 2010 http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf

[9] BBC, *iPlayer Monthly Performance Pack*, February 2011, http://www.bbc.co.uk/blogs/bbcinternet/img/BBC_iPlayer_performance_monthly_1102_FINAL.pdf

[10] comScore, *comScore Releases February 2011 U.S. Online Video Ranking*, 17 March 2011, http://comscore.com/layout/set/popup/Press_Events/Press_Releases/2011/3/comScore_Releases_February_2011_U.S._Online_Video_Rankings

[11] Communications Chambers analysis, based on Doubleclick Ad Planner data. February 2011 data

[12] Facebook website, http://www.facebook.com/press/info.php?statistics

of downstream internet traffic in Europe and North America[13]. Twitter has over 200m registered users, and is running at 140m tweets per day[14].

These and other social networks represent a significant and increasingly important addition to the ways in which people communicate.

Enterprise cloud services

Businesses use many of the services described above, but in addition there are a set of cloud services specific to them. Some of these represent an outsourcing of physical IT infrastructure (for instance using a web-hosting service rather than an on-premise server), others represent the use of software as a service. Salesforce.com was a pioneer in this area, providing a cloud-based CRM service. It has been followed by a plethora of other providers, offering cloud based accounting, HR, ERP, supply chain management and so on.

Cloud services were estimated[15] to be worth $68bn in 2010, and were expected to rise to $149bn by 2014.

[13] Sandvine, *Fall 2010 Global Internet Phenomena Report,* 20 October 2010 http://www.sandvine.com/downloads/documents/2010%20Global%20Internet%20Phenomena%20Report.pdf

[14] Twitter Blog, 14 March 2011, http://blog.twitter.com/2011/03/numbers.html

[15] Gartner, *Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010*, 22 June 2010 http://www.gartner.com/it/page.jsp?id=1389313

Challenges created

The movement of communications (and data) to a separate services layer creates a variety of challenges for regulators and law enforcement. These include:

- *Non-centralised services*. Peer-to-peer services such as BitTorrent do not have any central entity that can be attacked, making sanctions far harder.
- *Virtual services*. It is one of the attractions of cloud services that they can be accessed from wherever the user happens to be. However, this often means it is difficult to know where the user is located
- *Fragmentation*. The widespread availability of the internet has made it possible to provide a wide range of services with minimal owned infrastructure, in turn reducing barriers to entry (Skype would be one such example). While this is excellent from a competition perspective, it has led to substantial fragmentation of the market (the massive range of VOIP offerings being an example). This in turn makes it harder to comprehensively implement policies such as intercepts and the like, simply because there are more parties to deal with. For example, the FBI has recently observed that there has been "a transformation of communications services from a straight-forward relationship between a customer and a single CALEA-covered [telco] … to a complex environment in which a customer may use several access methods to maintain simultaneous interactions with multiple providers, some of whom may be based overseas or are otherwise outside the scope of CALEA". [16]
- *Service providers with 'less to lose'*. Associated with the larger number of providers caused by fragmentation is the fact that the average provider is smaller. Whereas a large corporate likely has considerable value in their brand and reputation, which they will wish to defend via good behaviour, a small entity may feel it has less to lose (either reputationally or financially), and so may be less pliable. Indeed, they may feel they simply cannot afford to provide carrier grade services such as emergency calls.
- *Service providers not dependent on governments for resources*. Telecoms providers are generally dependent on governments for both tangible and intangible assets. They have traditionally been licensed. While licence requirements have been significantly reduced over the last two decades, the denial of a licence

[16] Valerie Caproni, General Counsel, FBI, *Going dark: lawful electronic surveillance in the face of new technologies*, 17 February 2011 http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

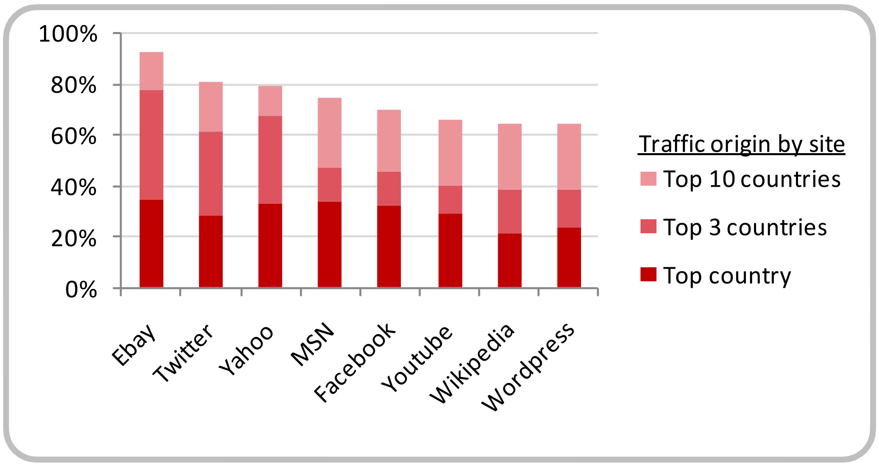
remains a powerful sanction for regulators to apply to a recalcitrant operator. Telcos may also depend on governments for spectrum (if they are wireless operators), number allocations, wayleaves and so on. Service providers generally have none of these dependencies, and as a result governments and NRAs have much less leverage over them

- *Uncharged services*. Many internet services, such as Twitter and Facebook and many others, are provided free to consumers. This means that authorities in a given country can not apply leverage by choking off money flow from customers to the service providers (or using this flow to identify the service provider in the first place)
- *Permanence*. Physical items, such as a book containing official secrets, can be pulped. A defamatory broadcast is transient. However, material released on the internet can be harder to remove. Even if the original source site deletes it, copies may be retained on services such as the Wayback Machine, which store images of the internet over time.
- *Global broadcast*. While a website, tweet or YouTube video may only be seen by a few people, it has the potential to be seen by a global audience, a far larger group than any terrestrial broadcaster has ever covered. This means the negative consequences of undesirable material can be far greater.
- *Extraterritoriality*. Services that would necessarily have been provided 'in country' previously (eg voice telephony) can now be provided by an overseas entity, at minimum increasing the cost of engaging with that entity, and possibly making it virtually impossible to apply sanctions directly (particularly if its country of domicile is unhelpful).

These last two challenges, global broadcast and extraterritoriality, highlight the importance of cross-border issues. While a number of service providers look like SMEs in their operations and physical presence, they look like MNCs in their customer bases.

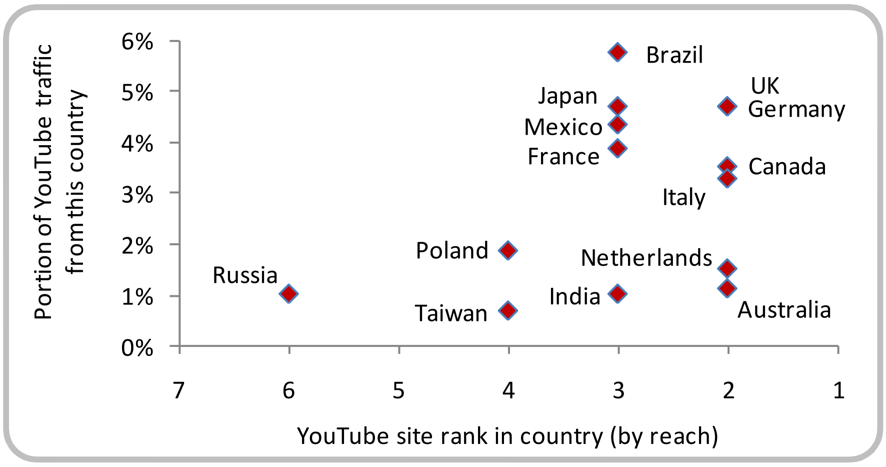
The internationalization of services is evident in the importance of non-domestic traffic to a wide range of sites. For instance, 'home market' (US) traffic is around 30% of total for each of the sites below:

Figure 3 Traffic origin for selected sites, by country rank for that site[17]



However, just because international traffic in aggregate is important to such sites, it does not imply that traffic from any one country is important (even if the site in question is one of the largest in that country). Taking YouTube as an example:

Figure 4 Countries' contribution to YouTube's traffic vs YouTube's rank in that country (select markets)[18]



Looking at Australia, YouTube has the second highest reach of all the sites tracked by AdPlanner. Thus it is a highly important player in that market. However, Australia represents 1.1% of YouTube's global traffic. Thus it is not a particularly important market from YouTube's perspective. This of course sets up an asymmetry in any Australian attempt to regulate YouTube – Australian authorities might have little leverage, and any mandate that imposed material costs on YouTube might simply cause them to exit the market.

[17] Communications Chambers analysis, based on Doubleclick Ad Planner data. Based on percentage of pageviews from top 30 countries covered by Doubleclick. February 2011 data

[18] Ibid. Note that Ad Planner does not report traffic for Google, its owner. Since Google is likely to be a top 3 site in most markets, YouTube's rank may be overstated by one in this data

Practical consequences

The challenges described above are more than theoretical – they are facing law enforcement agencies and regulators every day. The range of undesirable behaviour online is of course as rich and varied as that online. In this section we discuss practical examples.

Blocking information flow

All governments, liberal or autocratic, seek to block some information flow. Even the most democratic seek to stop the spread of official secrets, the broadcast of highly offensive material, or the unauthorised reproduction of copyright material. The advent of the internet has clearly made this control far more difficult to sustain.

Confidential information

A recent example is the US diplomatic cables released on Wikileaks starting 28 November 2010. The release of these cables was vehemently opposed by the US government. The White House called it a “reckless and dangerous action ... We condemn [it] in the strongest terms”[19]. Pressure was put on key suppliers to Wikileaks to withdraw service, and organisations such as Amazon, Mastercard, Paypal, EveryDNS.net (Wikileaks’ DNS provider) and others did so. The site was also subject to a ‘distributed denial of service’ (DDOS) attack. Despite this and various other efforts to limit dissemination of the cables, they are (at time of writing) discoverable in seconds via Google, and a steady stream of daily releases continues[20]. James Cowie, CTO of Internet monitoring firm Renesys, says Wikileaks are “for all intents and purposes, now immune to takedown by any single legal authority”, as a result of their diffuse structure[21].

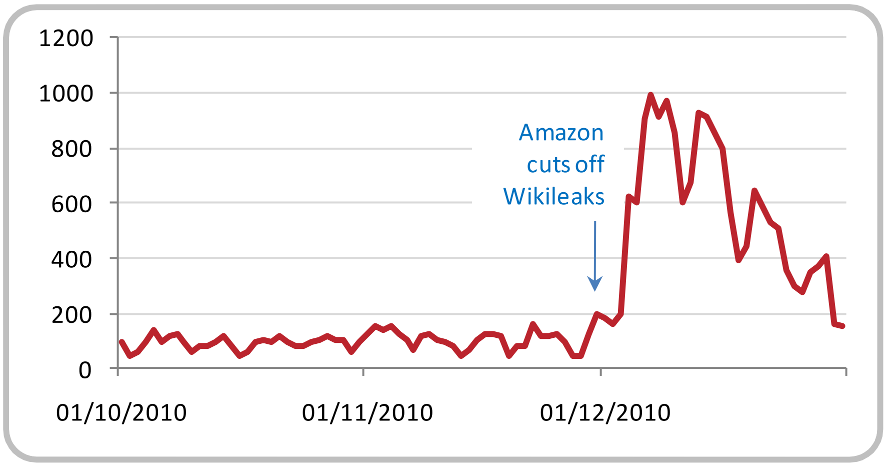
For instance, when Amazon ceased to provide service to Wikileaks, the files were quickly migrated to BitTorrent, leading to a surge in BitTorrent usage:

[19] The White House, *Statement by the Press Secretary*, November 28, 2010
http://www.whitehouse.gov/the-press-office/2010/11/28/statement-press-secretary

[20] While Wikileaks reportedly holds approximately 250,000 cables, only 6,000 have been published to date.

[21] Computerworld, *WikiLeaks nearly immune to takedown, says researcher*, 8 December 2010
http://www.computerworld.com/s/article/9200481/WikiLeaks_nearly_immune_to_takedown_says_researcher

Figure 5 BitTorrent Events (index) [22]



Intellectual property and piracy

Since the early days of the mass-market internet, the unauthorised dissemination of copyright material has been a concern. The music industry has been on the front line, because of the lower bandwidth requirements for audio tracks - the RIAA has been sending cease-and-desist letters to illegal music streaming sites since as far back as 1996[23]. The evidence from Korea, which has very high speed bandwidth, is that the same problems come to video content once these larger files can be readily downloaded. An armoury of weapons has been deployed against piracy including: law suits against file sharers, warning letters via ISPs, prosecutions, access blocking, DRM, education campaigns and so on.

However, the problem has proven to be a multi-headed hydra, with success tending to be short-lived. Frontier Economics estimate that the value of music tracks downloaded in 2008 was between $17bn and $40bn[24]. While the impact on the music industry will be much less than this (since people almost certainly pirate more music than they would otherwise have bought), there is no question that piracy is having significant economic impact. In the five largest EU markets, 23% of active internet users visit unlicensed music services, and album sales in 2010 were down 45% from the 2004 peak. [25]

A recent battle in this ongoing war has been over The Pirate Bay, a well known BitTorrent host. (BitTorrent is a distributed peer-to-peer file sharing technology). The Pirate Bay has been subject to prosecution of its

[22] Cisco, *Cisco 4Q10 Global Threat Report*, 7 Feb 2011 http://www.cisco.com/en/US/prod/collateral/vpndevc/Cisco_Global_Threat_Report_4Q10.pdf

[23] Recording Industry Association of America, *RIAA Demands Internet Service Stop Violating Record Companies' Rights*, 6 March 1996 http://www.riaa.com/newsitem.php?news_month_filter=3&news_year_filter=1996&resultpage=&id=E28A2717-1650-5BD9-A5EA-B908B161D1CF

[24] Frontier Economics, *Estimating the global economic and social impacts of counterfeiting and piracy*, February 2011 http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf

[25] IFPI *Digital Music Report 2011,* http://www.ifpi.org/content/library/DMR2011.pdf

founders, injunctions against its bandwidth provider and orders to ISPs to block consumer access (which has been successful in some markets). Nonetheless, it still receives 14m unique visitors per month[26]. More generally, BitTorrent represents 30% of upstream and 8% of downstream peak period traffic in Europe, suggesting massive volumes of filesharing, the majority of which is likely to be illegal (though legal uses, for instance by Wikipedia for video files, are increasing).

A challenge faced by those seeking to constrain or block both Wikileaks and The Pirate Bay is that it has become so cheap to provide such services. Peer-to-peer services inherently have lower storage and serving costs, since they rely on the PCs and bandwidth of participants for uploading. But even centralised services enjoy rapidly declining costs. Wikipedia, for instance, has a cost of US¢0.01 per pageview[27]. This allows such services to be provided on a volunteer or charitable basis. If there is even a moderate level of grassroots support for the service in question, activists can keep it operating, even if the prime movers are prosecuted.

Moreover, it is easy to switch between providers and countries for hosting. For example, The Pirate Bay has at various times been hosted in Sweden, Ukraine and the Netherlands.

Illegal content

Law enforcement agencies have made particularly strenuous efforts to shut down child pornography and paedophile sites. For example Europol (the European police agency) recently announced its investigation into 'boylover.net', a site with 70,000 members. 184 arrests have been made to date in 30 countries as a result of this investigation.[28]

While this particular site is now shut down, it is indicative of the challenges in blocking such material that the community was able to grow so large before police were able to intervene. As Europol has commented: "Child sex offenders and their networks make more and more use of sophisticated software in order to try to protect their anonymity, to make use of online storage and to use advanced encryption techniques to counteract digital forensic examination by police".[29]

[26] DoubleClick Ad Planner, February 2011

[27] Communications Chambers calculations based on Wikimedia Foundation data, December 2010
http://meta.wikimedia.org/wiki/Wikimedia_Foundation_Report,_January_2011

[28] New York Times, *More Arrests Likely in Pedophile Raid*, 17 March 2011
http://www.nytimes.com/2011/03/18/world/europe/18iht-child18.html

[29] Europol, *Child Sexual Exploitation 2010 Fact Sheet*, 2010
http://www.europol.europa.eu/publications/Serious_Crime_Overviews/Child_sexual_exploitation_factsheet_2010.pdf

There is also concern that the internet's ability to connect a vendor with niche audiences may mean that child pornography is now a profitable business, attracting organised crime.[30]

For these reasons, the availability of child pornography has been relatively stable despite the strenuous efforts to suppress it – the Internet Watch Foundation reports that there were 8,000 to 9,000 URLs showing child sexual abuse each year 2007-2009.[31]

Political dissent

Some governments have sought to control internet information flow as a way to block dissent, most infamously Egypt, which "threw the kill switch" during the recent uprising. Protests began on 25th January 2011. The Mubarak government became concerned that Twitter and Facebook were being used by protesters, and blocked access to these services. Nonetheless, the internet continued to be an important tool for protesters, both to co-ordinate amongst themselves and to communicate with the outside world. On the 27th January the government closed down virtually the entire Egyptian internet (by shutting down its Domain Name System). Even this did not entirely cut off the protestors, who were offered dial-up access using European modem banks.[32] Egypt returned to the internet on 2nd February.

Intercepting information flow

Integrated telcos have long been required to assist law enforcement with wiretaps. In the US the Communications Assistance for Law Enforcement Act (CALEA) requires that telecommunications services be capable of being tapped. However, the proliferation of providers in recent years has created problems. According to Valerie Caproni, General Counsel of the FBI, as a result of a lack of technical expertise or resources at some providers, "on a regular basis, the government is unable to obtain communications and related data, even when authorized by a court to do so. We call this capabilities gap the "Going Dark" problem"[33]. Caproni cites an example of a known arms smuggling ring that could not be shut down because it was using a communications provider that was unable to provide an intercept capability.

[30] See for instance UNODC, *The Globalization of Crime*, 2010 http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

[31] IWF, *Annual report 2009*, http://www.iwf.org.uk/accountability/annual-reports/2009-annual-report. Note that due to changes in hosting practices, IWF does not regard the 2010 figure as comparable to these earlier numbers

[32] FDN, Internet Censorship in Egypt: a humble action from FDN, 28 January 2011 http://blog.fdn.fr/post/2011/01/28/Censure-de-l-internet-en-%C3%89gypte-:-une-humble-action-de-FDN

[33] Valerie Caproni, General Counsel, FBI, *Going dark: lawful electronic surveillance in the face of new technologies*, 17 February 2011 http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

This inability is not limited to small start-ups. At the time of writing RIM is embroiled in a dispute with the Indian government, which is seeking access to Blackberry Enterprise Sever emails in that country. RIM has maintained that it is simply not possible for it (or underlying wireless carriers) to provide this, since the relevant encryption keys are held by its corporate customers, not RIM itself. The government has responded by threatening to ban Blackberry services entirely. The Indian authorities have been sensitised to these issues by the 2008 Mumbai terrorist attack, which they believe was coordinated in part using Blackberry devices[34].

The targets of wiretapping may well seek out services that are more challenging to tap. So, though they are only a small part of the overall market, they can nonetheless be a serious problem. For example, mobile VoIP is growing fast (as noted above), but by 2015 only 6% of Western European mobile customers are expected to be using it[35]. However, the targets of wiretaps are perhaps likely to be within this 6%, and thus mVoIP has the potential to be a challenge for law enforcement.

The proliferation of communications methods also creates a cost problem, even if it is technically possible to tap each method – the US cost per intercept order was $52,200 in 2009.[36]

Intercepts of non-voice communications are also important, but are also becoming more difficult. Recently convicted terrorist Rajib Karim, a British Airways employee, was found to have used a 'Russian Doll' approach to his security, making use of eight layers of disguise and encryption. Rather than using email or voice calls, he communicated with his allies by uploading coded files to file-sharing websites. Breaking his encryption took Scotland Yard nine months[37].

The challenge of breaking codes now readily available to consumers has led to a number of changes to UK legislation. For instance the Terrorism Act of 2006 increased the period suspects could be held without trial to 28 days, in part to allow more time for code-breaking. The Regulation of Investigatory Powers Act 2000 made it an offense for a suspect to withhold a computer password requested by the police – a man was recently jailed for four months for doing just this[38].

[34] Guardian, *BlackBerry to 'allow Indian government to monitor messages'*, 17 November 2010, http://www.guardian.co.uk/technology/2010/nov/17/india-blackberry-monitored-emails

[35] Analysys Mason, *Mobile VoIP: operators must re-evaluate their core portfolio*, March 2011 http://www.analysysmason.com/Research/Content/Reports/RDMV0_Mobile_VoIP_Mar2011/

[36] US Courts, *Wiretap Report 2009*, http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2009.aspx

[37] Daily Mail, *British Airways computer expert guilty of transatlantic plane bomb plot after using 'most sophisticated' code yet to talk to terrorists,* 1 March 2011 http://www.dailymail.co.uk/news/article-1361495/British-Airways-expert-guilty-terrorism-plane-bomb-plot.html

[38] Information Age, *Man jailed for withholding encryption key*, 6 October 2010 http://www.information-age.com/channels/security-and-continuity/news/1289178/man-jailed-for-withholding-encryption-key.thtml

In addition to these various technical challenges, there are also areas where legislation has not kept up with technology. Caproni of the FBI has observed that “CALEA does not cover … social networking sites, or peer-to-peer services”, meaning that there is no legal authority for intercepts in these areas. [39]

Privacy issues

The potential for wide dissemination of information, the permanence of information on the internet and its international nature all create significant privacy challenges. Privacy regulations and expectations differ materially from country to country. For instance, data protection rules are much stronger in Europe than in the US. While there are (for some jurisdictions) strict rules on transferring personal data across borders, such rules are of little use if, for example, the consumer himself has perhaps unknowingly provided their data to a server and/or entity that is outside his home market. For any website the location of its servers and its legal domicile are not likely to be evident.

Conversely, if (say) a US entity stores data regarding a US consumer with a cloud provider in France, that data then becomes subject to French data protection rules, even if the data is repatriated. As the World Privacy Forum puts it, “Once an EU Member State’s data protection law attaches to personal information, there is no clear way to remove the applicability of the law to the data”[40].

However, the EU has been struggling to assert control. Vivianne Reding emphasised in a recent speech that privacy “for European citizens should apply independently of the area of the world in which their data is being processed … There should be no exceptions for third countries' service providers controlling our citizens' data. … For example, a US-based social network company that has millions of active users in Europe needs to comply with EU rules.”[41] This was widely interpreted as being aimed at Facebook.

As with other areas, international aspects create particular challenges for enforcement. According to the OECD: “efforts by [privacy] authorities in the cross-border context are sometimes limited by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints”.[42]

[39] Valerie Caproni, General Counsel, FBI, *Going dark: lawful electronic surveillance in the face of new technologies*, 17 February 2011 http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

[40] World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, 23 February 2009 http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

[41] Vivian Reding, *Your data, your rights: Safeguarding your privacy in a connected world* [speech], 16 March 2011

[42] OECD, R*eport on the cross-border enforcement of privacy law*, 2006 http://www.oecd.org/dataoecd/17/43/37558845.pdf

Privacy breaches caused by providers are often inadvertent. Both AOL[43] and Netflix[44] have in the past released substantial data-sets into the public domain, believing they had anonymised them. In both cases this belief proved to be false. Other privacy issues have stemmed from corporations misjudging what their users found acceptable. For instance, Google Buzz initially published its users' lists of regular contacts to other users, before being rapidly withdrawn in face of widespread complaints.

However, while these episodes drew considerable attention from technology commentators, it seems likely that the actual harm caused was far less than that associated with data theft (discussed in more detail below), which often involves significant loss of privacy as a by-product.

This problem is certainly not getting better. According to the Privacy Rights Clearinghouse, which tracks US data breaches of all types, 2010 was the worst year on record for number of incidents. In a typical year they track over 400 incidents (undoubtedly a fraction of the total, since most go unreported), involving millions of records.

Emergency services

As noted above, the virtualisation of services breaks the link between the service and the location at which is provided. For emergency services that rely on geographic location, this is a problem. As Skype's draft IPO prospectus puts it: "we are unable to determine the exact location of a caller ... Our users have the ability to use our products nomadically … They can also log in on up to five devices simultaneously at a variety of locations"[45]. Consequently Skype simply declares that it does not provide emergency services. VoIP access provider Vonage relies on the user manually updating a home location record.

The US tightened requirements for VoIP 911 services from 2005 onwards, in part in response to incidents in Texas (a robbery/shooting) and Florida (where a child stopped breathing and later died) in which Vonage subscribers were unable to get through to emergency services[46]. The FCC is currently seeking comment on an NOI[47] on even tighter requirements, such as a possible mandate that VoIP operators incorporate an ability to automatically detect a user's Internet connectivity, identify a user's

[43] New York Times, *A Face Is Exposed for AOL Searcher No. 4417749*, 9 August 2006
http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=2&scp=2&sq=aol%20data&st=Search

[44] CDT, *Netflix Needs to Put "Privacy Risks" in Their Queue*, 30 September 2009
http://www.cdt.org/blogs/erica-newland/netflix-needs-put-privacy-risks-their-queue

[45] Skype, *Amendment No. 2 to Form S-1 Registration Statement*, 4 March 2011
http://www.sec.gov/Archives/edgar/data/1498209/000119312511056174/ds1a.htm#rom83085_12

[46] CNET, *Deadly delay on Vonage 911?*, 9 May 2005
http://news.cnet.com/Deadly-delay-on-Vonage-911/2100-1037_3-5700493.html

[47] FCC, NPRM and NOI, 23 September 2010
http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0927/FCC-10-177A1.pdf

location, and prompt a user to confirm his/her location, prior to enabling calling features.

A further problem is that VoIP services rely on the router in the home. In the event of a power outage, this will generally fail (though some come with battery power), by contrast to a traditional line-powered PSTN connection.

Spam

Spam is an unwanted consequence of the extremely low cost of sending emails. Spammers further reduce their costs (and increase their own security) by using 'botnets', large groups of otherwise innocent computers infected with viruses, to send their mass mailings. Botnets are in effect 'cloud services' for the spammer. For much of 2010 spam was running at over 300bn messages per day. It is also a major cross-border problem – leading sources of spam are Vietnam, Brazil and India[48].

In addition to being a problem in of itself, spam promotes illegal pharmaceuticals and fake designer goods, spreads malware, and supports phishing and various frauds.

In recent months there have been some major successes in the suppression of spam, thanks to successful efforts to take down botnets and the sites that facilitate spammers' affiliate revenue. By December volumes had dropped to 100bn messages per day, and are likely now lower. In March 2011 a group led by Microsoft took down the infamous 'Rustock' botnet. This required a highly coordinated effort, involving several companies, five different hosting providers, the US courts, US Marshals and Dutch and Chinese law enforcement[49].

Attacking botnets is just one of a range of techniques being used to counter spam. Others include reputation-based filtering, content based filtering, the use of CAPTCHAs and so on.

However, these tools have had relatively little impact on the amount of spam sent - while there have been minor variations over time, Messagelabs report that spam has been approximately 85% of all emails sent each year since 2005.[50] There has been more persistent success in spam filtering – Microsoft reports that only 1 in 48 spam messages make it to an inbox, down from around 1 in 12 in 2006.[51]

[48] Cisco, *Cisco 4Q10 Global Threat Report*, 7 Feb 2011
http://www.cisco.com/en/US/prod/collateral/vpndevc/Cisco_Global_Threat_Report_4Q10.pdf

[49] Microsoft. *Taking Down Botnets: Microsoft and the Rustock Botnet*, 17 March 2011
http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx

[50] MessageLabs, *2010 Annual Security Report*, http://www.messagelabs.co.uk/resources/mlireports.aspx

[51] Microsoft, *Security Intelligence Report*, H1 2010
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b5f9eddc-70dc-4b11-996b-1bc6987c44b9

The overall cost of spam is hard to measure – it comprises network capacity to carry the messages, the lost productivity from time spent deleting spam (or recovering inappropriately filtered messages) and the sums spent on email security to mitigate spam. This last figure alone was over $5bn in 2010.[52]

Data theft

The internet has greatly facilitated data theft, and some episodes have been on an epic scale. For instance, in 2008 hacker Albert Gonzalez and two Russian co-conspirators stole data relating to 130m credit and debit cards from Heartland Payment Systems. They made use of servers in the US, Latvia, the Netherlands and Ukraine, and anonymous web currencies to transfer their proceeds.[53] Heartland's loss was at least $130m, largely in compensation to Visa and American Express. Gonzalez' gain is unknown, though $1m in cash was found buried in his parents' garden.

He was sentenced to 20 years for this crime[54], but his co-conspirators are still unknown (other than by their aliases). David Navetta of the Info Law Group observed: "Unfortunately cybercrimes are often committed from very remote locations all over the world, and the criminals try very hard to cover their tracks. Cybercrime is a relatively low risk (of getting caught) and high reward crime".[55]

The challenges posed by cross-border data theft and other cybercrime have been well understood for many years. The 2001 Budapest Convention on Cybercrime (ratified by 46 countries) gives police powers to access servers in other countries without the permission of the authorities, as long as the system owners sanction the access.[56]

Online crime appears to be on an upward trend – the FBI's Internet Crime Complaint Centre received 303,000 complaints in 2010, up almost 50% since 2007 (though slightly down from 2009). UNODC estimate the value of just one category, online identify fraud, at $1bn[57], though other estimates are significantly higher,

[52] Radicati Group, *E-mail Security Market, 2010-2014*, 2010
http://www.radicati.com/wp/wp-content/uploads/2010/05/Email-Security-Market-2010-2014-Brochure.pdf

[53] DoJ, *USA vs Albert Gonzalez, Hacker 1 & Hacker 2* [indictment], 17 August 2009
http://www.justice.gov/usao/nj/Press/files/pdffiles/2009/GonzIndictment.pdf

[54] Reuters, *Hacker Gonzalez gets 20 years for Heartland breach*, 26 March 2010
http://www.reuters.com/article/2010/03/27/urnidgns852573c400693880002576ef004839d-idUS329727399120100327?pageNumber=1

[55] GovInfoSecurity, *Heartland Hacker Sentenced to 20 Years*, 26 March 2010
http://www.govinfosecurity.com/articles.php?art_id=2344

[56] Computer Weekly, UN rejects international cybercrime treaty, 20 April 2010,
http://www.computerweekly.com/Articles/2010/04/20/240973/UN-rejects-international-cybercrime-treaty.htm

[57] UNODC, The Globalization of Crime, 2010
http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

Conclusions

The battle between malefactors and the authorities online is sometimes seen as a technical arms race, and in some aspects, such as encryption and decryption, it is.

However, there are other aspects at least as important as the technology that make regulating cloud services challenging. As we have seen, the internet is inherently international, and that creates practical problems for those seeking to co-ordinate responses to misdeeds. Addressing boylover.net and Rustock required sustained cross-border co-ordination. This is expensive, depends on all jurisdictions seeing the issue as a problem, and is time consuming. Thus the number of situations where it is a viable approach is limited.

The fact that 'schools of minnows' provide services also makes it more difficult for authorities to reach comprehensive solutions. This is the practical challenge faced by those trying to silence Wikileaks, or tap US voice communications in an IP world.

Services such as YouTube also grant power to a far wider group – individuals have the ability to reach a far greater audience than ever before. Of course, YouTube has the ability to revoke this power from a user, but the sheer volumes of traffic on the site mean that by the time it notices that it should, it may be too late (as in the Italian bullying case).

'The authorities', whether regulators or law enforcement, are almost by definition centralised. Whether this is the best structure to meet the highly diffuse challenges of misdeeds on the internet remains to be seen. Certainly sites such as Wikipedia and YouTube rely primarily on the collective actions of their own members to police their own content.

As authorities 'clutch at the cloud' they are already facing hard choices. What can be controlled by traditional, centralised approaches and is also sufficiently undesirable to be worth blocking notwithstanding the likely increasing expense? What can and should be controlled, but requires a new approach? And finally, what has simply become 'unregulatable' in this new world?

About the author

Robert Kenny (rob@commcham.com) is a founding partner of Communications Chambers, a growing association of leading experts in the fields of telecoms, media and technology which advises on issues of strategy, policy and regulation.

Previously he was MD of Human Capital, a consulting firm. Past roles include heading Strategy and/or M&A for Hongkong Telecom, Reach and Level 3 (all multi-billion dollar telcos). He was also a founder of IncubASIA, a Hong Kong based venture capital firm investing in online businesses.