Metahaven

Captives of the Cloud: Part I

We are the voluntary prisoners of the cloud; we are being watched over by governments we did not elect.

Wael Ghonim, Google's Egyptian executive, said: “If you want to liberate a society just give them the internet.”[1] But how does one liberate a society that already has the internet? In a society permanently connected through pervasive broadband networks, the shared internet is, bit by bit and piece by piece, overshadowed by the “cloud.”

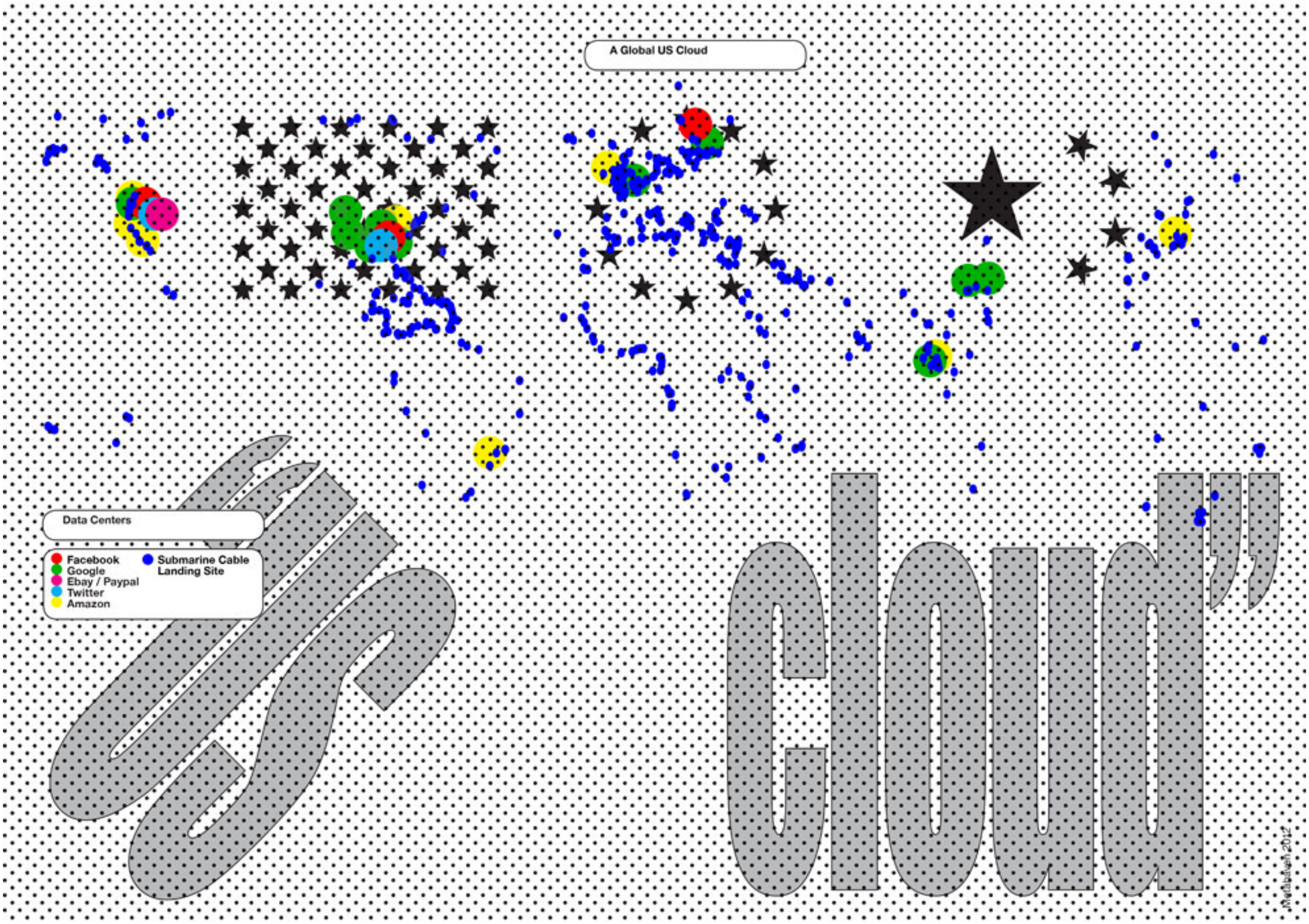
The Coming of the Cloud

The cloud, as a planetary-scale infrastructure, was first made possible by an incremental rise in computing power, server space, and trans-continental fiber-optic connectivity. It is a by-product and parallel iteration of the global (information) economy, enabling a digital (social) marketplace on a worldwide scale. Many of the cloud’s most powerful companies no longer use the shared internet, but build their own dark fiber highways for convenience, resilience, and speed.[2] In the cloud’s architecture of power, the early internet is eclipsed.

A nondescript diagram in a 1996 MIT research paper titled “The Self-governing Internet: Coordination by Design,” showed a “cloud” of networks situated between routers linked up by Internet Protocol (IP).[3] This was the first reported usage of the term “cloud” in relation to the internet. The paper talked about a “confederation” of networks governed by common protocol. A 2001 *New York Times* article reported that Microsoft’s .NET software programs did not reside on any one computer, “but instead exist in the ‘cloud’ of computers that make up the internet.”[4] But it wasn’t until 2004 that the notion of “cloud computing” was defined by Google CEO Eric Schmidt:

> I don’t think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing – they should be in a “cloud” somewhere. And that if you have the right kind of browser or the right kind of access, it doesn’t matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – you can get access to the cloud. There are a number of companies that have benefited from that. Obviously, Google, Yahoo!, eBay, Amazon come to mind. The computation and the data and so forth are in the servers.[5]

The internet can be compared to a patchwork of city-states, or an archipelago of islands. User



A selection of the global US social media cloud, resorting under the Patriot Act.

data and content materials are dispersed over different servers, domains, and jurisdictions (i.e., different sovereign countries). The cloud is more like Bismarck's unification of Germany, sweeping up formerly distinct elements, bringing them under a central government. As with most technology, there is a sense of abstraction from prior experiences; in the cloud the user no longer needs to understand how a software program works or where his or her data really is. The important thing is that it works.

In the early 1990s, a user would operate a "personal home page," hosted by an internet Service Provider (ISP), usually located in the country where that user lived. In the early 2000s, free online services like Blogspot and video sites like YouTube came to equal and surpass the services of local providers. Instead of using a paid-for local e-mail account, users would switch to a service like Gmail. In the late 2000s and the early 2010s this was complemented, if not replaced, by Facebook and other social media, which integrate e-mail, instant messaging, FTP (File Transfer Protocol), financial services, and other social interaction software within their clouds. Cloud-based book sales, shopping, and e-reading have brought about the global dominance of Amazon, the world's biggest cloud storage provider and the "Walmart of the Web."[6] By 2015, combined spending for public and private cloud storage will be $22.6 billion worldwide.[7] Given this transition, it is no exaggeration to proclaim an exodus from the internet to the cloud. The internet's dispersed architecture gives way to the cloud's central model of data storage and management, handled and owned by a handful of corporations.

The coming of the cloud is spelled out by Aaron Levie, founder and CEO of Box, one of Silicon Valley's fastest growing cloud storage providers. As Levie states, the biggest driver of the cloud is the ever-expanding spectrum of mobile devices – iPhones, iPads, Androids, and such – from which users tap into the cloud and flock around its server spine:

> If you think about the market that we're in, and more broadly just the enterprise software market, the kind of transition that's happening now from legacy systems to the cloud is literally, by definition, a once-in-a-lifetime opportunity. This is probably going to happen at a larger scale than any other technology transition we've seen in the enterprise. Larger than client servers. Larger than mainframes.[8]

Google, one of the world's seven largest cloud companies, has recently compared itself to a bank.[9] That comparison is apt. If data in the cloud is like money in the bank, what happens to it while it resides "conveniently" in the cloud?

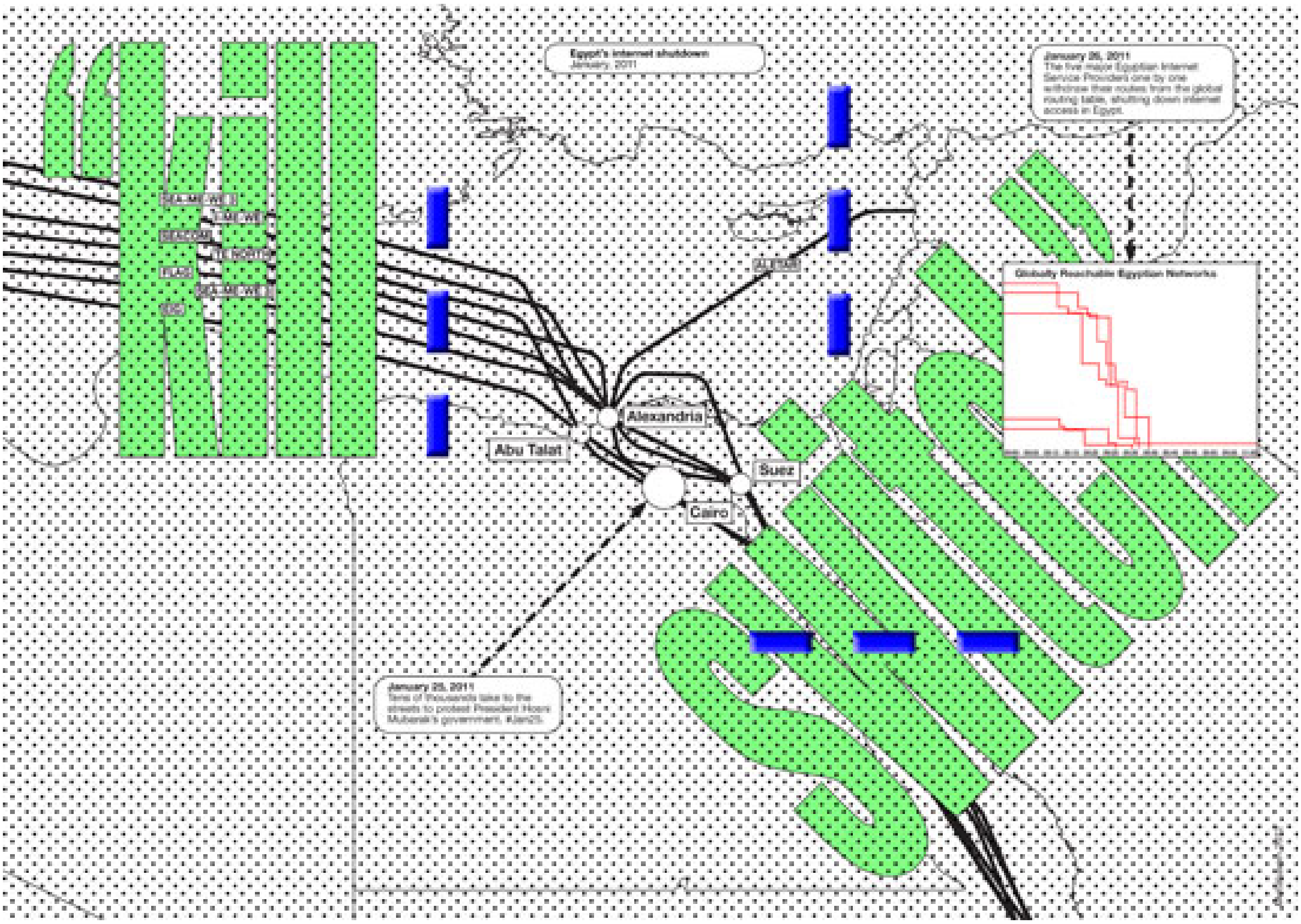
The US Cloud and the Patriot Act

Where and by whom sites are registered and data is hosted matters a great deal in determining who gains access to and control over the data. For example, all data stored by US companies (or their subsidiaries) in non-US data centers falls under the jurisdiction of the USA Patriot Act, an anti-terrorism law introduced in 2001.[10] This emphatically includes the entire US cloud – Facebook, Apple, Twitter, Dropbox, Google, Amazon, Rackspace, Box, Microsoft, and many others. Jeffrey Rosen, a law professor at George Washington University, has established that the Patriot Act, rather than investigating potential terrorists, is mostly used to spy on innocent Americans.[11] But the people being watched need not even be Americans. Via the cloud, citizens across the world are subject to the same Patriot Act powers – which easily lend themselves to misuse by authorities. Matthew Waxman of the Council on Foreign Relations outlines the situation:

> These kinds of surveillance powers have historically been prone to abuse. Some of the legal restrictions on surveillance that the Patriot Act was designed to roll back were actually the direct product of abuses by the FBI, the CIA, and other government agencies. During the 1960s and '70s, national security intelligence powers were used by government agents to spy on political opposition [and] cast abusively wide nets. That legacy of abuse has raised a lot of concerns about whether there is adequate oversight with respect to these new surveillance powers.[12]

The sociologist Saskia Sassen adds to this perspective:

> Through the Patriot Act [...] the government has authorized official monitoring of attorney-client conversations, wide-ranging secret searches and wiretaps, the collection of Internet and e-mail addressing data [...] All of this can be done without probable cause about the guilt of the people searched – that is to say, the usual threshold that must be passed before the government may invade privacy has been neutralized. This is an enormous accrual of powers in the administration, which has found itself in the position of having to reassure the public that it can be 'trusted' not to abuse these powers. But there have been abuses.[13]


kill
switch
Egypt's internet shutdown
January, 2011
January 28, 2011
The five major Egyptian Internet Service Providers one by one withdraw their routes from the global routing table, shutting down internet access in Egypt.
Globally Reachable Egyptian Networks
Alexandria
Abu Talat
Suez
Cairo
January 25, 2011
Tens of thousands take to the streets to protest President Hosni Mubarak's government. #Jan25.

The Mubarak “kill switch” which took Egypt off the internet in January, 2011.

Microsoft was the first cloud company to publicly confirm Patriot Act access to its data stored outside the US.[14] In August 2011, Google also confirmed that its data stored overseas is subject to "lawful access" by the US government.[15] A 2012 white paper by the law and privacy firm Hogan Lovells examined these findings, concluding that while the Patriot Act does give the US government access to the cloud, many other governments enjoy similar forms of access under their own laws – and further, that using the "location" of a cloud server to determine legal protection was a mistaken idea altogether.[16] The paper noted the widespread use of so-called Mutual Legal Assistance Treaties (MLATs), which streamline the exchange between countries of data needed for investigative purposes. Apart from treaty-backed requests, "informal relationships between law enforcement agencies […] allow for governmental access to data in the 'possession, custody, or control' of cloud service providers over whom the requesting country does not otherwise have jurisdiction." The legality of such informal relationships was not examined by the study. Neither did it backlog any recorded abuses of the Patriot Act, or discuss reports by two US Senators about a "secret interpretation" of the law, which would give the FBI far-reaching extra surveillance powers that the public is unaware of.[17]

One of the most powerful instruments the US government uses to look into the so-called "non-content information" of ISPs and cloud providers is the National Security Letter (NSL). NSLs demand specific information about users and are issued directly by the FBI. After the Patriot Act was signed into law, the number of letters issued rose exponentially: from 8,500 in 2000 to 39,346 in 2003. An NSL automatically includes a gag order that prohibits the recipient from notifying users about the request. The FBI need only assert that the information sought is "relevant" to an investigation.[18] The crucial question in the Hogan Lovells report – "Are government orders to disclose customer data subject to review by a judge?" – is answered with "yes" in Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, the United Kingdom, and the US. However, in the US this condition is only met if the cloud provider, after receiving the NSL, first challenges its built-in gag order. Only when the NSL is unsealed by a judge can the cloud provider inform the user about the existence of the letter. For the Hogan Lovells report, this procedure counts as judicial review.

Super-Jurisdiction

In Egypt, during the revolution, Facebook and Twitter played the role of subversive, uncensorable alternative media – in part because the servers of these wildly popular services were beyond the reach of local authorities. Indeed, Hosni Mubarak's best bet to fend off the power of the internet was to switch it off entirely. To do so, "just a few phone calls probably sufficed."[19] While Mubarak's *ultima ratio* as a sovereign ruler over Egyptian soil proved sufficient to wall the country off from the network, the violent crudeness of this act also demonstrated the dictator's much more substantial *lack of power* over the network's larger infrastructure. Sovereign control over the cloud, in contrast to authoritarian power-mongering, is a sophisticated affair. One might draw a very different map here: the global spread of the US cloud, for example, results in a kind of "super-jurisdiction" enjoyed by its host country.

Super-jurisdiction can be seen in action in the 2012 seizure of Megaupload.com by the US Department of Justice (DOJ). Megaupload.com was a Hong Kong-based internet enterprise paying loving tribute to all kinds of Hollywood films (to say it politely). The site offered, according to its own self-description, "no-registration upload and sharing of files up to 1 gigabyte." It was seized in January 2012 by the DOJ and the FBI, backed by film industry copyright claimants. Megaupload.com stands accused of generating "more than $175 million in criminal proceeds" and causing "more than half a billion dollars in harm to copyright owners."[20]

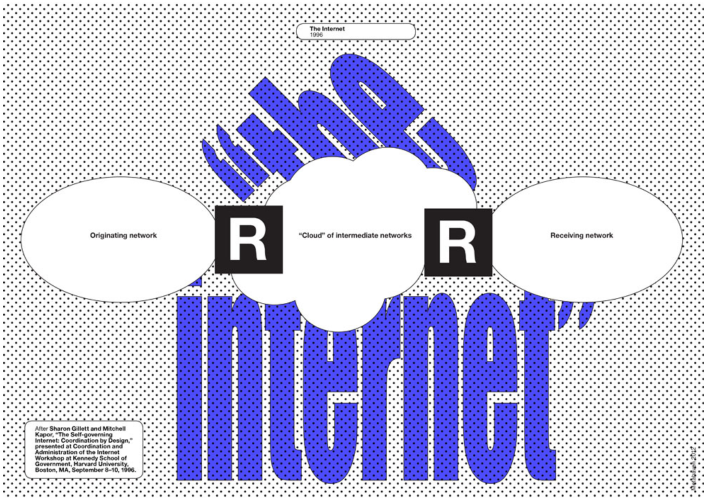
The site's founder, thirty-seven-year-old internet millionaire Kim Dotcom, and three of his associates were brought to a New Zealand court to face extradition to the US. They'd been living like self-styled oligarchs. In a gesture toward transparency, they said they had "nothing to hide."[21] In particular, Dotcom himself embodies the absurd saga of a contemporary, deeply self-parodying internet hooligan – a legal black hole turned persona, unprepared in every way to be "famous," yet accepting the challenge wholeheartedly. Megaupload.com was, at least in its own self-imagination, nothing more than a technical conduit between those who upload and those who download, its content-indiscriminate policy a typical example of laissez-faire anarcho-capitalism. The US government's prosecution of the site remains highly debated, because the DOJ interpreted the site's global user base as a willful conspiracy to break US law. As Jennifer Granick at Stanford Law notes, the DOJ referenced "unknown parties" (i.e., the users of Megaupload.com) as members of a conspiracy to conduct a crime in the US. Granick notes that such users "were located all over the world, and may or may not have acted willfully." Indeed, with Megaupload.com, the government alleges "an *agreement* to violate a US civil law, including by many people who are not subject to US rules." As Granick then asks, "Does the United States have jurisdiction over anyone who uses a hosting provider in the Eastern District of Virginia? What about over any company that uses PayPal?"[22] Indeed, these are the sorts of questions prompted by super-jurisdiction.

Super-jurisdiction means that the law of one country can, through various forms of cooperation and association implied by server locations and network connections, be extended into and enacted in another. The US, as a result of its unique position in managing the internet's core, also has jurisdiction over all so-called top level domains, no matter where they are hosted and by whom. All top-level domain names (dot-com, dot-org, dot-net, etc.) must be registered through VeriSign, a Virginia-based company. Using its jurisdiction over the domain name registry, in 2012 the DOJ seized Bodog.com, a gambling website operated from Canada. A US Customs Enforcement spokesperson confirmed to *Wired* that the US had in a similar manner seized 750 different domain names of sites it believed committed intellectual property theft.[23] Michael Geist, an internet law professor at the University of Ottawa, observes that, indeed, "All Your internets Belong to US":

> The message from the [Bodog] case is clear: all dot-com, dot-net, and dot-org domain names are subject to US jurisdiction regardless of where they operate or where they were registered. This grants the US a form of "super-jurisdiction" over internet activities since most other countries are limited to jurisdiction with a real and substantial connection. For the US, the location of the domain name registry is good enough.[24]

Cloud Surveillance

The various technical components that enable global communication – server, network, and client – all lend themselves to surveillance. *Access Controlled,* a MIT Press handbook on internet surveillance and censorship, states that "the quest for information control is now beyond denial."[25] It mentions the so-called "security first" norm, by which the combined threats of terrorism and child pornography create a mandate for the state to police the net without restriction. As the authors assert in their conclusion, "The security-first norm around internet governance can be seen, therefore, as but another manifestation of these wider developments. Internet censorship and surveillance – once largely confined to authoritarian regimes – is now fast becoming the global norm."[26] Indeed, if a lawsuit brought by the Electronic Frontier Foundation (EFF) against AT&T is any indication, the US government seems determined to expand its access to electronic communication. The EFF's star witness in the case was Mark Klein, a former AT&T technician who claimed to have seen, in 2002, the creation and ongoing use of a dedicated private room where the National Security Agency (NSA) had "set up a system that vacuumed up internet and phone-call data from ordinary Americans with the cooperation of AT&T."[27] Klein said the system allowed the government full surveillance of not just the AT&T customer base, but that of sixteen other companies as well.[28] The US government dismissed the case against the telecommunications provider, asserting the privilege of state secrets. The government has also dismissed cases against itself and other telecom companies that assisted with similar endeavors, including Sprint, Nextel, and Verizon.[29] If the allegations are true, according to *Access Controlled*, "they show that the United States maintains the most sophisticated internet surveillance regime."[30]

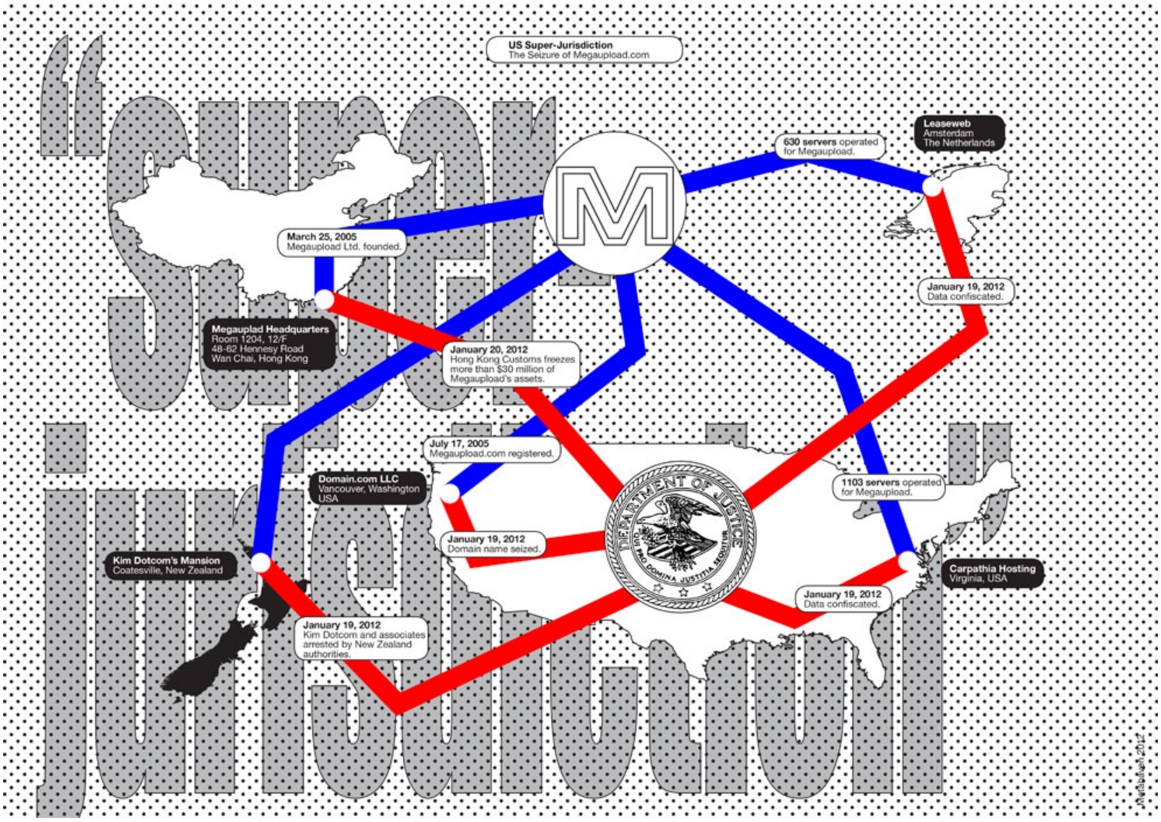

The Internet
1996
"the
internet"
Originating network
R
"Cloud" of intermediate networks
R
Receiving network
After Sharon Gillett and Mitchell Kapor, "The Self-governing Internet: Coordination by Design," presented at Coordination and Administration of the Internet Workshop at Kennedy School of Government, Harvard University, Boston, MA, September 8–10, 1996.
Metahaven 2012

The first mention of the notion of the "cloud" was in a 1996 diagram in an MIT research paper, redrawn here.

As technologies expand, the governance, legislation, and legalities of surveillance become increasingly complicated. In May 2012, CNET reported that the general counsel of the FBI had drafted a proposed law that would require social-networking sites, e-mail and voice-over-IP (VoIP) providers, as well as instant messaging platforms, to provide a backdoor for surveillance – a demand from the US government for cloud companies to "alter their code to ensure their products are wiretap-friendly."[31] In 2012, the UK Government announced the installation – in collaboration with telecom companies and ISPs – of so-called "black boxes" which would retrieve and decrypt communications from Gmail and other cloud services, storing the non-content data from these communications.[32] But the cloud is nothing like a national telephone network. Whenever the cloud is “wiretapped,” authorities listen into a global telecommunications oracle; the data of everyone using that cloud, regardless of where and who they are, and regardless of whether or not they are the suspect of a crime, is at least in principle at the disposal of law enforcement.

Most journalism routinely criticizes (or praises) the US government for its ability to spy on “Americans.” But something essential is not mentioned here – the practical ability of the US government to spy on everybody else. The potential impact of surveillance of the US cloud is as vast as the impact of its services – which have already profoundly transformed the world. An FBI representative told CNET about the gap the agency perceives between the phone network and advanced cloud communications for which it does not presently have sufficiently intrusive technical capacity – the risk of surveillance “going dark.” The representative mentioned “national security” to demonstrate how badly it needs such cloud wiretapping, inadvertently revealing that the state secrets privilege – once a legal anomaly, now a routine – will likely be invoked to shield such extensive and increased surveillance powers from public scrutiny.

Users' concerns about about internet surveillance increased with the proposed Stop Online Piracy Act (SOPA), which was introduced into the US House of Representatives in late 2011. How the government would police SOPA became a real worry, with the suspicion that the enforcement method of choice would be standardized deep packet inspections (DPI) deployed through users’ internet service providers – a process by which the “packets” of data in the network are unpacked and inspected.[33] Through DPI, law enforcement would detect and identify illegal downloads. In 2010, before SOPA was even on the table, the Obama Administration sought to enact federal laws that would force communications providers offering encryption (including e-mail and instant messaging) to provide access by law enforcement to unencrypted data.[34] It is, however, worth noting that encryption is still protected as “free speech” by the First Amendment of the US Constitution – further complicating, but not likely deterring, attempts to break the code. One way of doing so consists



The seizure of Megaupload.com; using super-jurisdiction to allege a global conspiracy.

of surrounding encryption with the insinuation of illegality. The FBI in 2012 distributed flyers to internet cafe business owners requesting to be wary of "suspicious behavior" by guests, including the "use of anonymizers, portals or other means to shield IP address" and "encryption or use of software to hide encrypted data." In small print, the FBI added that each of these "indicators" by themselves, however, constituted lawful conduct.[35]

Coercive Paternalism

"Real name" requirements by the cloud-based social networking platforms Facebook and Google+ expressly attack anonymity and pseudonymity online, affecting the fundaments of political speech. Real name directives require users to register with a service using the name that is in their passport. The reasons given by cloud services for such real name requirements are vague – perhaps for fear of sounding too directly authoritarian. The preferred route, instead, is that of fatherly advice. Facebook claims that it has a real name policy "so that you always know who you're connecting with," while Google states that it requires real names so "that the people you want to connect with can find you."[36] These explanations gesture towards a conception of normative social arrangements – requiring that your use the same name that you'd use among your friends, family, or coworkers. Alexis Madrigal points out a certain irony in the Google+ real name requirement:

> The kind of naming policy that Facebook and Google Plus have is actually a radical departure from the way identity and speech interact in the real world. They attach identity more strongly to every act of online speech than almost any real world situation does.[37]

Cloud providers such as Amazon use real name registration as a mechanism for accountability. Though Amazon still allows users to use a "pen name," the trademarked "real name" attribution is advertised as having the ability to "potentially increase your reputation in the community" as a retailer, seller, or reviewer.[38] Some see the real name badge as a step towards "fixing their flawed [and] exploitable review system" for reviewing books – a system notoriously dominated by biased "anonymous" users, often thought to be, and sometimes proven to be, other authors, their family members, or the books' publishers.[39] Though Amazon's reasoning for promoting the use of real names is more explicit than that of Facebook and Google+, one can imagine the marketing benefits of a synchronized real name system between social media and retail websites – and the connection that such a synchronicity might have with the government. Such requirements can be seen as aligned with plans of the US government to introduce a universal "trusted identity" or "internet ID" system for US citizens, a commission the White House granted to the US Commerce Department in 2011. According to White House Cybersecurity Coordinator Howard Schmidt, the effort entails nothing less than creating an "identity ecosystem" for the internet.[40]

Cass Sunstein, the Obama Administration's chief internet advisor, has recently argued for government policy against the spread of "rumors" on the internet; as noted by the *New Yorker*, one of the most persistent of such rumors was the theory that President Obama had been born in Kenya – and thus holds his presidency illegally.[41] Sunstein believes that certain properties of the internet gear public speech toward the uninformed forwarding and circulation of rumors and conspiracy theories. In "echo chambers" and through "cybercascades," one-sided opinion would spread rapidly and widely in the network without rebuttal. Supposedly balanced reporting by professional journalists in the mainstream media now has to compete for attention with, and gets often surpassed by, every other blog post, Facebook update, or tweet. The effortless ability for all Internet users to compose and live on a "Daily Me" – a news diet catered to fit and maintain an individual, already established, self-referential set of beliefs – would result in a fragmentation of the general public into factions which no longer expose themselves to views held by other factions. Sunstein claims that under such fragmentation, "diverse speech communities" are created "whose members talk and listen mostly to one another." And,

> When society is fragmented in this way, diverse groups will tend to *polarize* in a way that can breed extremism and even hatred and violence. New technologies, emphatically including the Internet, are dramatically increasing people's ability to hear echoes of their own voices and to wall themselves off from others.[42]

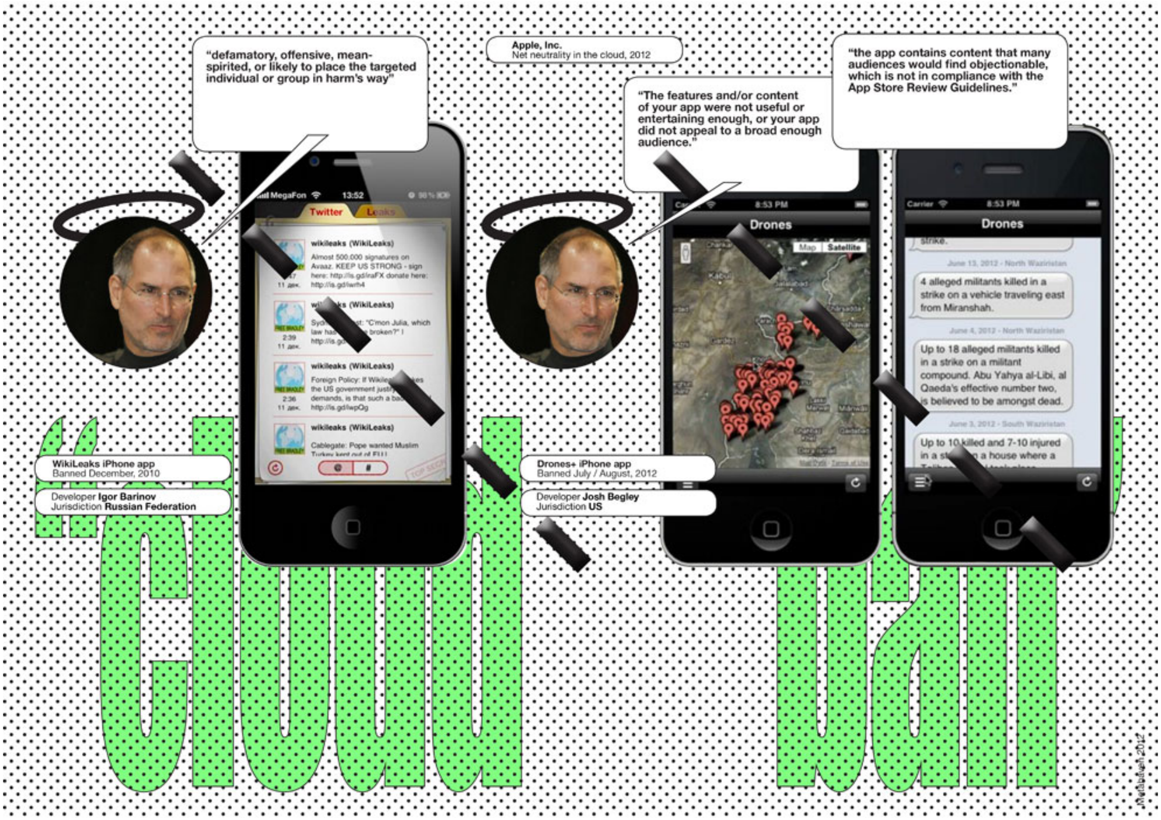
Sunstein is concerned with how rumors may impair the effectiveness of government, and undermine its legitimacy. Early 2008, he and a co-author published a paper on conspiracy theories around the 9/11 attacks. In the paper, Sunstein recommended that "Government agents (and their allies) might enter chat rooms, online social networks, or even real-space groups and attempt to undermine percolating conspiracy theories by raising doubts about their factual premises, causal logic or implications for political action."[43]

Nowhere is the coercive government stance toward online rumors as clear as in China. Beijing put forth regulations requiring users to register on social medial sites with their "real name identities" by March 2012 – regulation comparable to policies already spontaneously embraced by Facebook and Google. Sites including Sina Weibo, one of the country's largest microblogging sites, have begun implementing these regulations, which also forbid users from making statements against the state's honor or statements that may disrupt civil obedience.[44] Around the same time, social media sites across the country flared up over the ouster of political leader Bo Xilai from the Communist Party. The Chinese police swiftly detained six people and shut down sixteen websites over "rumors" surrounding the incident, including claims that military vehicles were entering Beijing.[45]

Cloud as a Political Space

The increasing prominence which cloud-based internet services, social media and VoIP technologies now enjoy over legacy tools of communication shows in how they enable new, virtually cost-free forms of organization. For social movements relying on collective action, this factor has proven to be key. Unsurprisingly, when social media platforms are suddenly "switched off," their ability to organize can be severely affected. Facebook, in the wake of nationwide anti-austerity protests in the UK in February 2011, deleted the profiles of dozens of political groups preparing to take part in further protests. In doing so, Facebook effectively disabled lawful political activism, which had, for obvious reasons, moved their coordination to the cloud. The reason for the purge is still not known and likely never will be. All the social networking behemoth could utter to justify its behavior was cryptic technospeak. Profiles had "not been registered correctly," as a Facebook spokeswoman explained.[46] In 2010, UK Prime Minister David Cameron and other Conservative politicians met in London with Facebook founder Mark Zuckerberg. Their admiration was mutual.[47]

Rebecca MacKinnon, a former CNN reporter and cofounder of the citizen media network Global Voices, asserts in her book *Consent of the Networked* that "we cannot understand how the internet is used unless we first understand the ways in which the internet itself has become a highly contested political space."[48] This applies equally, and equally urgently, to the cloud.


"defamatory, offensive, mean-spirited, or likely to place the targeted individual or group in harm's way"
Apple, Inc.
Net neutrality in the cloud, 2012
"The features and/or content of your app were not useful or entertaining enough, or your app did not appeal to a broad enough audience."
"the app contains content that many audiences would find objectionable, which is not in compliance with the App Store Review Guidelines."
Twitter
Drones
Drones
WikiLeaks iPhone app
Banned December, 2010
Developer Igor Barinov
Jurisdiction Russian Federation
Drones+ iPhone app
Banned July / August, 2012
Developer Josh Begley
Jurisdiction US
"cloud ban"
Metahaven 2012

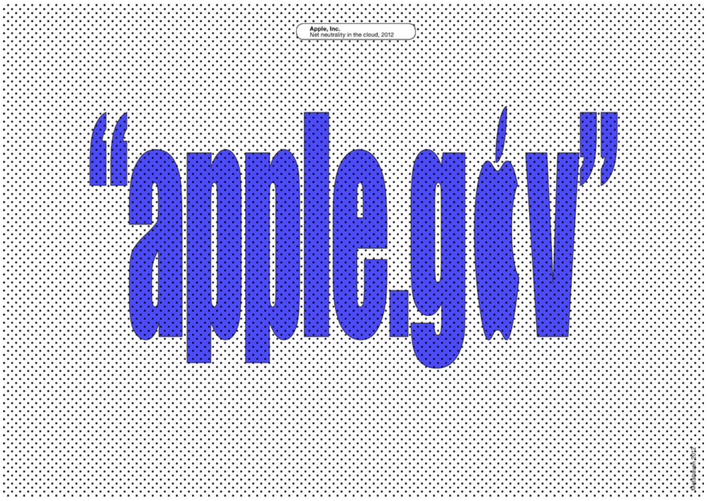
App neutrality? Apple's ban on two controversial iPhone apps in 2010 and 2012 shows a lack of network neutrality in the cloud.

The combined rights to a free flow of information, freedom of expession, and freedom from censorship, have been described as a compound right to “internet freedom.” Indeed, Google's Wael Ghonim at the beginning of this story suggested that unhindered access to, and use of, the internet enables the liberation of a society.

Here, the free flow of information is blocked by clearly identifiable authoritarian despots. To not have internet freedom, one must be under the oppression of a shameless tyrant, or be living in a “closed society” where the free flow of information is not sufficiently appreciated just yet. On January 21, 2010, US Secretary of State Hillary Clinton delivered a speech on US foreign policy and internet freedom, highlighting exactly this view. Clinton assured her audience in Washington, D.C. that “As I speak to you today, government censors are working furiously to erase my words from the records of history.”[49] Evgeny Morozov, a US-based, Belarusian-born internet scholar rightly criticized Clinton's “anachronistic view of authoritarianism.” As Morozov explained, “I didn't hear anything about the evolving nature of internet control (e.g. that controlling the internet now includes many other activities – propaganda, DDoS attacks, physical intimidation of selected critics/activists). If we keep framing this discussion only as a censorship issue, we are unlikely to solve it.” He went on to criticize the double standards the State Department advertised with regard to online anonymity:

> On the one hand, they want to crack down on intellectual property theft and terrorists; on the other hand, they want to protect Iranian and the Chinese dissidents. Well, let me break the hard news: You can't have it both ways and the sooner you get on with "anonymity for everyone" rhetoric, the more you'll accomplish. I am very pessimistic on the future of online anonymity in general – I think there is a good chance it will be eliminated by 2015 – and this hesitance by the State Department does not make me feel any more optimistic.[50]

Still, the definition of internet freedom remains relatively opaque. One example of this vagueness is provided by Internetfreedom.org, a global consortium, which aims to “inform, connect, and empower the people in closed societies with information on a free internet.”[51] Savetheinternet.com, a project of Free Press, breaks down internet freedom into somewhat more clearly defined categories – “net neutrality (wired and wireless), strong protections for mobile phone users, public use of the public airwaves and universal access to high-speed internet.”[52] The notion of net neutrality is as relevant to internet freedom as it is to the structure of the cloud, since the network's management is in the hands of a patchwork of government agencies and private enterprises who may (or may not) hold a bias toward certain information on the network, or a bias toward one another. Coined by the legal scholar Tim Wu in 2003, network neutrality was originally meant to benchmark and promote the open nature of the internet for the sake of innovation – an “end-to-end” infrastructure unbiased towards its content. As Wu stated, “A communications network like the internet can be seen as a platform for a competition among application developers. Email, the web, and streaming applications are in a battle for the attention and interest of end-users. It is therefore important that the platform be neutral to ensure the competition remains meritocratic.”[53] Network neutrality applies to a decentralized architecture, with clearly divided roles between ISPs, broadband service providers, content providers, and services and applications on the network. It justifies a *de facto* gentlemen's agreement through a joint economic interest in innovation and fair competition. Indeed, also political speech can be considered part of a competition – one of ideas on how to (not) govern ourselves. Venture capitalist Joichi Ito expressed this view in 2003, when he wrote that such a competition of ideas “requires freedom of speech and the ability to criticize those in power without fear of retribution.”[54]



Apple.gov: governmentality in the cloud.

Insofar as the cloud's software services use the shared internet, they can be considered applications run on the network. To this end, network neutrality applies to the cloud (for example, the cloud is expected to consume more and more bandwidth in the network, possibly at the cost of other applications and services). The concept of network neutrality is more difficult to apply *in* the cloud, since some of the nominal conditions to institute neutrality are absorbed by the cloud's combination of hosting and software services within a single black box. In the cloud, there is no more principled separation between the hosting of data, software, and client-side tools through which the data is handled and experienced. Indeed, the enormous success of the cloud is that it provides for all of these things at once.[55]

The Terms of Service of any cloud-based provider are a far cry from a binding agreement to net neutrality; they allow plenty of space for "cloudy bias." For example, in August, 2012, Apple banned "Drones+" from its App Store. This app, developed by NYU student Josh Begley, provides aggregated news on US drone strikes in Pakistan, Yemen and Somalia, and it includes a Google map on which the strikes are marked. The app also prompts the user whenever a new drone strike has occurred, and says how many casualties it had produced. Crucially, the information aggregated by the app is already completely public and freely available through various other sources including *The Guardian*'s iPhone app. Apple demonstrated its cloudy parody of network neutrality in the ever-changing reasons it gave for rejecting Drones+. Apple had problems with the Google logo appearing on the Google map. In July, the company stated in an e-mail that "The features and/or content of your app were not useful or entertaining enough, or your app did not appeal to a broad enough audience." By August, Apple changed its mind. The app contained "content that many audiences would find objectionable, which is not in compliance with the App Store Review Guidelines." Indeed, the company eventually concluded that Drones+, which does not show users any images of actual drone-related bloodshed, was "objectionable and crude."[56] The *New York Times* wondered how on earth it could be that

> the material Apple deemed objectionable from Mr. Begley was nearly identical to the material available through *The Guardian*'s iPhone app. It's unclear whether Apple is treating the two parties differently because *The Guardian* is a well-known media organization and Mr. Begley is not, or whether the problem is that Mr. Begley chose to focus his app only on drone strikes.[57]

One can endlessly ponder why Apple banned Drones+ from its cloud but admitted *The Guardian,* and one will never be finished weighing the arguments. The point is that if its cloud operated even under something remotely looking like network neutrality, Apple could not have reasonably rejected the app. The case also brings to mind Evgeny Morozov's earlier warning that government censorship of the network nowadays is more sophisticated than a crude Mubarak internet kill switch. As Rebecca MacKinnon writes,

> citizens are [...] vulnerable to abuse of their rights to speech and assembly not only from government but also from private actors. In democracies, it follows that citizens must guard against violations of their digital rights by governments and corporations – or both acting in concert – regardless of whether the company involved is censoring and discriminating on its own initiative or acting under pressure from authorities.[58]

It is highly unlikely that Drones+ was banned after direct government interference. But it isn't difficult to imagine an informal, unstated, and rather intuitive constellation of interests between Apple – universally praised by US politicians on both sides of the aisle – and the US Government. Shared interests and informal ties between private enterprise and government, based on mutual forms of "Like," rather than strict separations by Law, may account for *de facto* forms of censorship in the cloud, without the explicit order to enact it or the explicit obligation to justify it. In December 2010, Apple removed a WikiLeaks iPhone app from its store, citing its developer guidelines: "Any app that is defamatory, offensive, mean-spirited, or likely to place the targeted individual or group in harms [sic] way will be rejected."[59] Simultaneous to the WikiLeaks app being banned, other US cloud companies, including Amazon and PayPal, stopped providing services to WikiLeaks.

The political, legal and jurisdictional consequences of the cloud are slowly becoming apparent – right at the time when we are unlikely to withdraw from it. The cloud is just too good. We won't stop using our iPhones, iPads, Androids and Kindles. Paypal is still our frenemy. Happily the captives of the cloud, we will tweet our critiques of it, and Facebook-broadcast our outcries over its government back doors. But the story is not over yet. Will the anarcho-libertarian roots of the internet kick back at the cloud's centralized architecture – or are they forever overrun by it? Has the cloud assumed its final form, or is there still a time and a place for surprises?

×

Written by Daniel van der Velden and Vinca Kruk. Research

assistant: Alysse Kushinski. Design assistant: Rasmus Svensson. All images courtesy of Metahaven. Metahaven 2012.

→ *To be continued in "Captives of the Cloud: Part II."*

Metahaven is an Amsterdam-based design collective on the cutting blade between politics and aesthetics. Founded by Vinca Kruk and Daniel van der Velden, Metahaven's work – both commissioned and self-directed – reflects political and social issues through research-driven design, and design-driven research. Research projects included the *Sealand Identity Project*, and currently include *Facestate,* and *Iceland as Method*. Solo exhibitions include *Affiche Frontière* (CAPC musée d'art contemporain de Bordeaux, 2008) and *Stadtstaat* (Künstlerhaus Stuttgart/Casco, 2009). Group exhibitions include *Forms of Inquiry* (AA London, 2007, cat.), *Manifesta8* (Murcia, 2010, cat.), the *Gwangju Design Biennale 2011* (Gwangju, Korea, cat.), *Graphic Design: Now In Production* (Walker Art Center, Minneapolis, 2011, and Cooper-Hewitt National Design Museum, New York, 2012, cat.) and *The New Public* (Museion, Bolzano, 2012, cat.). Metahaven's work was published and discussed in *The International Herald Tribune*, *The New York Times, Huffington Post*, *Courrier International, Icon, Domus*, *Dazed*, *The Verge*, *l'Architecture d'Aujourd'hui*, and *Mute*, among other publications. Vinca Kruk is a Tutor of Editorial Design and Design Critique at ArtEZ Academy of Arts in Arhem. Daniel van der Velden is a Senior Critic at the Graphic Design MFA program at Yale University, and a Tutor of Design at the Sandberg Instituut Amsterdam. In 2010, Metahaven released *Uncorporate Identity*, a design anthology for our dystopian age, published by Lars Müller.

[1] Wael Ghonim, cited in Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York City: Basic Books, 2012), xx.

[2] Brandon Teddler, “To The Cloud!,” *Ezine Mark,* February 20, 2012. See http://cloud.ezinemark.com/t o-the-cloud-7d3407dff%2043c.html.

[3] Sharon Gillett and Mitchell Kapor, “The Self-governing Internet: Coordination by Design,” presented at Coordination and Administration of the Internet Workshop at Kennedy School of Government, Harvard University, Boston, MA, September 8–10, 1996. See http://ccs.mit.edu/papers/CCSWP197/ccswp197.html.

[4] John Markoff, “An Internet Critic Who Is Not Shy About Ruffling the Big Names in High,” *New York Times,* April 9, 2001. See http://www.nytimes.com/2001/04/09/technology/09HAIL.html?ex=1230872400&en=5d156fc75d409335&ei=5070.

[5] Eric Schmidt, “Conversation with Eric Schmidt Hosted by Danny Sullivan,” Search Engine Strategies Conference, August 9, 2006. See http://www.google.com/press/podium/ses2006.html.

[6] “Amazon: The Walmart of the Web,” *The Economist,* October 1, 2011. See http://www.economist.com/node/21530980.

[7] Nathan Eddy, “Cloud Computing to Drive Storage Growth: IDC Report,” *eWeek,* October 21, 2011. See http://www.eweek.com/c/a/Cloud-Computing/Cloud-Computing -to-Drive-Storage-Growth-IDC -Report-193712/.

[8] Nick Bilton, “Data storage server, and founder, move quickly.” *International Herald Tribune,* August 28, 2012.

[9] Barb Darrow, “Amazon Is No. 1. Who’s Next in Cloud Computing?,” *GigaOM*, March 14, 2012. See http://gigaom.com/cloud/amazon-is-no-1-whos-next-in-cloud-computing/. Cade Metz, “Google: ‘We’re Like a Bank for Your Data,’” *Wired,* May 29, 2012. See http://www.wired.com/wiredenterprise/?p=20996.

[10] Zack Whittaker, “Summary: ZDNet’s USA PATRIOT Act Series,” *ZDNet,* April 27, 2011. See http://www.zdnet.com/blog/igeneration/summary-zdnets-usa-patriot-act-series/9233.

[11] Jeffrey Rosen, “Too Much Power,” *New York Times,* September 8, 2011. See http://www.nytimes.com/roomfordebate/2011/09/07/do-we-still-need-the-patriot-act/the -patriot-act-gives-too-much-power-to-law-enforcement.

[12] Matthew C. Waxman, “Extending Patriot Act Powers,” interview by Jonathan Masters, www.cfr.org, February 22, 2012. See http://www.cfr.org/counterterrorism/extending-patriot-ac t-powers/p24174.

[13] Saskia Sassen, *Territory, Authority, Rights. From Medieval to Global Assemblages*, Princeton and Oxford: Princeton University Press, 2006 (2008), 180.

[14] Paul Taylor, “Privacy Concerns Slow Cloud Adoption,” *Financial Times,* August 2, 2011. See http://news.softpedia.com/news/Google-Admits-Handing-over-European-User-Data-to-US-Intelligence-Agencies-215740.shtml.

[15] Lucian Constantin, “Google Admits Handing over European User Data to US Intelligence Agencies,” *Softpedia,* August 8, 2011. See http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf.

[16] Winston Maxwell, and Christopher Wolf, “A Global Reality: Governmental Access to Data in the Cloud,” *A Hogan Lovells White Paper,* May 23, 2012. See http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf.

[17] Mike Masnick, “Senators Reveal That Feds Have Secretly Reinterpreted The PATRIOT Act,” *Techdirt,* May 26, 2011. See http://www.techdirt.com/articles/20110525/15411414434/senators-reveal-that-feds-have -secretly-reinterpreted-patr iot-act.shtml.

[18] Kim Zetter, “Unknown Tech Company Defies FBI In Mystery Surveillance Case,” *Wired,* March 14, 2012. See http://www.wired.com/threatlevel/2012/03/mystery-nsl /.

[19] Ryan Singel, “Egypt Shut Down Its Net With a Series of Phone Calls.” *Wired,* January 28, 2011. See http://www.wired.com/threatlevel/2011/01/egypt-isp-shutdown/.

[20] Claire Connelly and Lee Taylor, “FBI Shuts down Megaupload.com, Anonymous Shut down FBI,” News.com.au, January 20, 2012. See http://www.news.com.au/technology/fbi-shuts-down-megauploadcom-charges-seven-with-online-piracy/story-e6frfro0-1226249114650#ixzz1k8bkZU4v.

[21] Ibid.

[22] See Jennifer Granick, “Megaupload: A Lot Less Guilty Than You Think,” Center for Internet and Society at Stanford Law School, January 26, 2012. See http://cyberlaw.stanford.edu/node/6795.

[23] David Kravats, “Uncle Sam: If It Ends in .Com, It’s .Seizable,” *Wired,* March 6, 2012. See http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/.

[24] Michael Geist, “All Your Internets Belong to US, Continued: The Bodog.com Case,” michaelgeist.ca, March 6, 2012. See http://www.michaelgeist.ca/content/view/6359/135/.

[25] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, Massachusetts: The MIT Press, 2010), 6.

[26] Ibid., 11.

[27] Ellen Nakashima, “A Story of Surveillance,” *The Washington Post,* November 7, 2007. See http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html.

[28] Ibid.

[29] Dan Levine, “US Court Upholds Telecom Immunity for Surveillance,” *Thomson Reuters,* December 29, 2011. See http://newsandinsight.thomsonreuters.com/Legal/News/2011/12_-_December/U_S__court_upholds_telecom_immunity_for_surveillance/.

[30] Ronald Deibert et. al., *Access Controlled,* 381.

[31] Declan McCullagh, “FBI: We Need Wiretap-Ready Web Sites – Now,” *CNET,* May 4, 2012. See http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now /.

[32] Geoff White, “‘Black Boxes’ to Monitor All Internet and Phone Data,” *Channel 4*, June 29, 2012. See http://www.channel4.com/news/black-boxes-to-monitor-all-internet-and-phone-data.

[33] Alex Wawro, “What Is Deep Packet Inspection?,” *PC World*, February 1, 2012. See http://www.pcworld.com/article/249137/what_is_deep_packet_inspection.html.

[34] Declan McCullagh, “Report: Feds to Push for Net Encryption Backdoors,” *CNET*, September 27, 2010. See http://news.cnet.com/8301-31921_3-20017671-281.html.

[35] See http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/.

[36] “Facebook’s Name Policy – Facebook Help Center,” facebook.com. See http://www.facebook.com/help/?faq=112146705538576&in_context.“Google-Page and Profile Names – Google+ Help,” plus.google.com. See http://support.google.com/plus/bin/answer.py?hl=en&answer=1228271.

[37] Alexis Madrigal, “Why Facebook and Google’s Concept of ‘Real Names’ Is Revolutionary,” *The Atlantic,* August 5, 2011. See http://www.theatlantic.com/technology/archive/2011/08/why-facebook-and-googles-concept-of-real-names-is-revolutionary/243171/.

[38] “Amazon.com Help: Pen Names and Real Names,” amazon.com. See http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=14279641.

[39] Mark T. Kieczorek, “Amazon Real Name Badge,” *Maktaw*, July 23, 2004. See http://www.marktaw.com/technology/AmazonRealNameBadge.html. Amy Harmon, “Amazon Glitch Unmasks War Of Reviewers,” *New York Times,* February 14, 2004. See http://www.nytimes.com/2004/02/14/us/amazon-glitch-unmasks-war-of-reviewers.html?pagewanted=3&src=pm.

[40] Declan McCullagh, “Obama to Hand Commerce Dept. Authority over Cybersecurity ID,” *CNET*, January 7, 2011. See http://news.cnet.com/8301-31921_3-20027800-281.html?tag=contentMain;contentBody.

[41] Elizabeth Kolbert, “The Things People Say,” *The New Yorker*, November 2, 2009.

See http://www.newyorker.com/arts/critics/books/2009/11/02/091102crbo_books_kolbert?currentPage=all.

[42] Cass R. Sunstein, *Republic.com 2.0*, (Princeton and Oxford, Princeton University Press, 2007), 44.

[43] Cass R. Sunstein, Adrian Vermeule, “Conspiracy Theories.” *Harvard University Law School Public Law & Legal Theory Research Paper Series*, Paper No. 199, University of Chicago Law School, 2008, 22. See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1084585.

[44] Michael Kan, “Beijing to Require Users on Twitter-like Services to Register With Real Names,” *PC World,* December 16, 2011. See http://www.pcworld.com/businesscenter/article/246360/beijing_to_require_users_on_twitterlike_services_to_register_with_real_names.html?tk=rel_news.

[45] Michael Bristow, “China Arrests Over Coup Rumours,” *BBC News,* March 31, 2012. See http://www.bbc.co.uk/news/world-asia-china-17570005. Dav id Eimer, “China Arrests Six Over Coup Rumours,” *The Telegraph,* March 31, 2012. See http://www.telegraph.co.uk/news/worldnews/asia/china/9177717/China-arrests-six-over-coup-rumours.html.

[46] Shiv Malik, “Facebook Accused of Removing Activists’ Pages,” *The Guardian,* April 29, 2012. See http://www.guardian.co.uk/technology/2011/apr/29/facebook-accused-removing-activists -pages.

[47] Tim Bradshaw, “Mark Zuckerberg Friends David Cameron,” *Financial Times,* June 21, 2012. See http://blogs.ft.com/tech-blog/2010/06/mark-zuckerberg-friends-david-cameron/#axzz1yC7waUhe.

[48] MacKinnon, *Consent of the Networked,* xxii.

[49] “Internet Freedom.” The prepared text of U.S. of Secretary of State Hillary Rodham Clinton's speech, delivered at the Newseum in Washington, D.C. Foreign Policy, January 21, 2010. See http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom?page=0,2.

[50] Evgeny Morozov, “Is Hillary Clinton launching a cyber Cold War?” *Foreign Policy Net.Effect,* January 21, 2010. See http://neteffect.foreignpolicy.com/posts/2010/01/21/cyber_cold_war.

[51] See http://www.internetfreedom.org/.

[52] See http://www.Savetheinternet.com/.

[53] Tim Wu, “Network Neutrality, Broadband Discrimination.” *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003. See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863.

[54] Joichi Ito, “Weblogs and Emergent Democracy.” See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863.

[55] On a related note, cyberlaw professor Jonathan Zittrain in 2008 wrote *The Future Of The Internet – And How To Stop It*, a book focusing on the rise of the web's “tethered appliances,” which, like North Korean radio sets, can be attuned to exclude or disregard certain content, and are designed not to be tinkered with by their users. Zittrain argued that such closed service appliances – emphatically including design icons like iPods and iPhones, for example – would in fact contribute to stifle the generative and innovative capacity of the web. See Jonathan Zittrain, *The Future Of The Internet – And How To Stop It,* New Haven and London: Yale University Press, 2008.

[56] Christina Bonnington and Spencer Ackerman, “Apple Rejects App That Tracks U.S. Drone Strikes.” *Wired*, August 30, 2012. See http://www.wired.com/dangerroom/2012/08/drone-app/.

[57] Nick Wingfield, “Apple Rejects App Tracking Drone Strikes.” *New York Times Blog,* August 30, 2012. See http://bits.blogs.nytimes.com/2012/08/30/apple-rejects-app-tracking-drone-strikes/.

[58] MacKinnon, ibid., 119.

[59] Gregg Keizer, “Apple boots WikiLeaks app from iPhone store.” *Computerworld,* December 21, 2010. See http://www.computerworld.com/s/article/9201920/Apple_boots_WikiLeaks_app_from_iPhone_store.