Metahaven

Captives of the Cloud: Part II

→ *Continued from "Captives of the Cloud: Part I"*

> *Is the future of the world the future of the internet?*
>
> – Julian Assange[1]

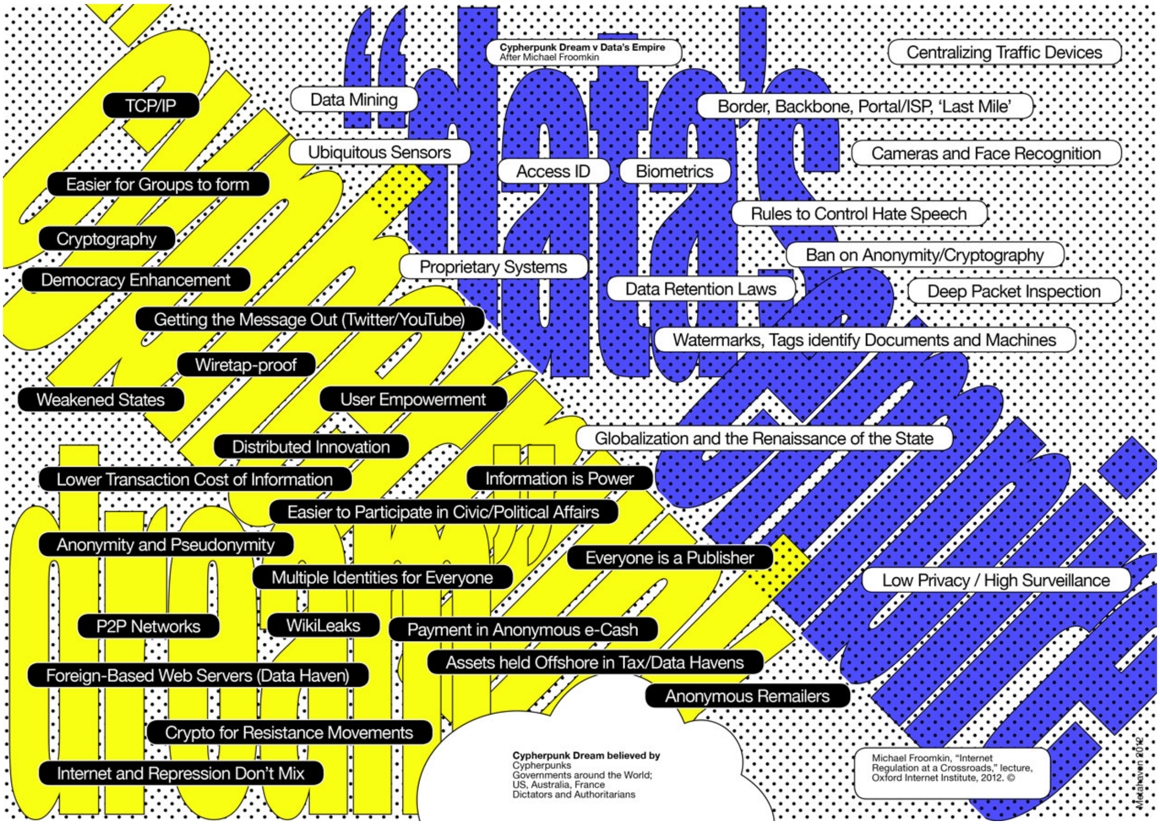
The cloud is the informational equivalent to the container terminal. It has a higher degree of standardization and scalability than most earlier forms of networked information and communication technology. From social networking to retail, from financial transactions to e-mail and telephone, these and many other services end up in the cloud. Surely, the internet already was a wholesale for all types of information and media formats. As Milton Mueller notes, these "used to be delivered through separate technologies governed by separate legal and regulatory regimes," while now having converged on the internet and its protocols.[2] In the cloud, such "digital convergence" goes even further: data becomes more effectively and thoroughly harvested, analyzed, validated, monetized, looked into, and controlled than in the internet; its centralization is not just one of protocol, but also of location.

The Form of the Cloud

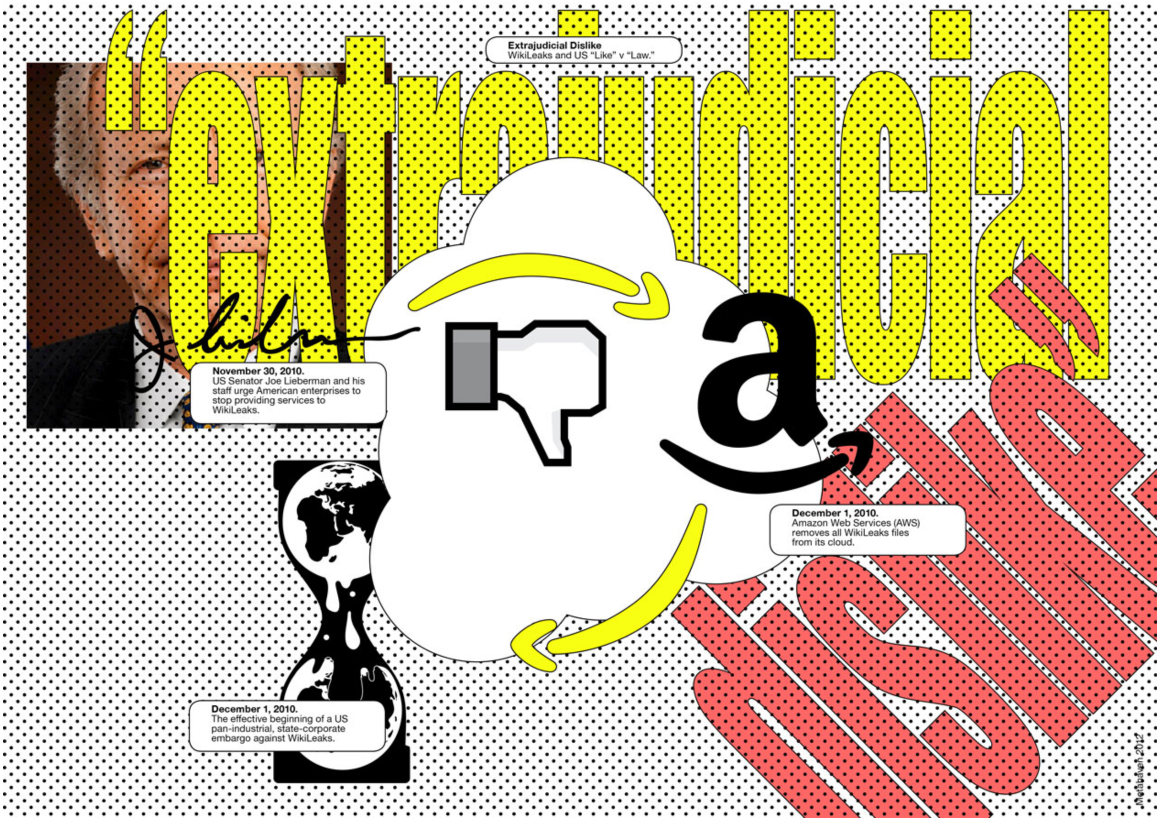
Many writers in recent decades have grappled with a seemingly borderless information society rooted in physical territories, and finding words for this condition has been key to most serious writing about information networks. For example, the term "space of flows" was coined in the 1990s by the Spanish sociologist Manuel Castells. It describes the spatial conditions of the global movement of goods, information, and money. According to Castells, the space of flows is

> constituted by a circuit of electronic exchanges (micro-electronics-based devices, telecommunications, computer processing, broadcasting systems, and high-speed transportation – also based on information technologies) that, together, form the material basis for the processes we have observed as being strategically crucial in the network society.[3]

Castells adds that this material basis is "a spatial form, just as it could be 'the city' or 'the region' in the organization of the merchant society or the industrial society."[4] As legal scholars Tim Wu and Jack Goldsmith note in their study *Who Controls the Internet?*, beneath "formless cyberspace" rests "an ugly physical transport infrastructure: copper wires, fiberoptic


Cypherpunk Dream v Data's Empire
After Michael Froomkin
Centralizing Traffic Devices
TCP/IP
Data Mining
Border, Backbone, Portal/ISP, 'Last Mile'
Ubiquitous Sensors
Cameras and Face Recognition
Access ID
Biometrics
Easier for Groups to form
Rules to Control Hate Speech
Cryptography
Ban on Anonymity/Cryptography
Proprietary Systems
Democracy Enhancement
Data Retention Laws
Deep Packet Inspection
Getting the Message Out (Twitter/YouTube)
Watermarks, Tags identify Documents and Machines
Wiretap-proof
Weakened States
User Empowerment
Globalization and the Renaissance of the State
Distributed Innovation
Lower Transaction Cost of Information
Information is Power
Easier to Participate in Civic/Political Affairs
Anonymity and Pseudonymity
Everyone is a Publisher
Multiple Identities for Everyone
Low Privacy / High Surveillance
P2P Networks
WikiLeaks
Payment in Anonymous e-Cash
Assets held Offshore in Tax/Data Havens
Foreign-Based Web Servers (Data Haven)
Anonymous Remailers
Crypto for Resistance Movements
Cypherpunk Dream believed by
Cypherpunks
Governments around the World;
US, Australia, France
Dictators and Authoritarians
Internet and Repression Don't Mix
Michael Froomkin, "Internet Regulation at a Crossroads," lecture, Oxford Internet Institute, 2012. ©
Metahaven 2012

“Cypherpunk Dream” versus “Data's Empire.” The dichotomy of the internet according to Michael Froomkin.


Extrajudicial Dislike
WikiLeaks and US "Like" v "Law."
“extrajudicial
dislike”
November 30, 2010.
US Senator Joe Lieberman and his staff urge American enterprises to stop providing services to WikiLeaks.
December 1, 2010.
Amazon Web Services (AWS) removes all WikiLeaks files from its cloud.
December 1, 2010.
The effective beginning of a US pan-industrial, state-corporate embargo against WikiLeaks.
Metahaven 2012

“Like” versus “Law”: An “Extrajudicial Dislike” by US Senator Joe Lieberman prompting an industrial embargo against WikiLeaks.

cables, and the specialized routers and switches that direct information from place to place."[5] James Gleick describes the network's data center, the cables, and the switches as "wheel-works," and the cloud as its "avatar."[6] The cloud presupposes a geography where data centers can be built. It presupposes an environment protected and stable enough for its server farms to be secure, for its operations to run smoothly and uninterrupted. It presupposes redundant power grids, water supplies, high-volume, high-speed fiber-optic connectivity, and other advanced infrastructure. It presupposes cheap energy, as the cloud's vast exhaust violates even the most lax of environmental rules. While data in the cloud may seem placeless and omnipresent, precisely for this reason, the infrastructure safeguarding its permanent availability is monstrous in size and scope. According to 2012 research by the *New York Times*, the cloud uses about thirty billion watts of electricity worldwide, roughly equivalent to thirty nuclear power plants' worth of output. About one quarter to one third of this energy is consumed by data centers in the United States. According to one expert, "a single data center can take more power than a medium-size town."[7]

A data center is a windowless, large, flat building. Its architecture is foreshadowed by the suburban big boxes of Walmart and the like. Unlike megamalls, the precise locations of data centers are secret. Companies don't usually advertise where data centers are: not the public image of their operations, but *their actual operations*, depend on them.[8] To users, the cloud seems almost formless, or transparent – always available, ever-changing, hanging in the air, on screens, in waves, appearing and disappearing, "formless cyberspace" indeed. Yet at the core of this informational ghost dance lies a rudimentary physical form – steel and concrete infrastructure. If the enormous, energy-slurping data factories are the cloud's true form, then these instances of the "space of flows" recall the medieval castle, the treasure chest, and the military base. They recall the political and military conflicts that have dominated geography since recorded history. As the architect and writer Pier Vittorio Aureli states,

> Any power, no matter how supreme, totalitarian, ubiquitous, high-tech, democratic, and evasive, at the end has to land on the actual ground of the city and leave traces that are difficult to efface. This is why, unlike the web, the city as the actual space of our primary perception remains a very strategic site of action and counteraction. ... But in order to critically frame the network, we would need to propose a radical reification of it. This would mean its transformation into a finite "thing" among other finite things, and not always see the network and its derivatives like something immaterial and invisible, without a form we can trace and change.[9]

In discussion with Aureli, the theorist Boris Groys asserts that the network is situated on (or below) a "defined territory, controlled by the military." On those terms, Groys claims,

> the goal of future wars is already established: control over the network and the flows of information running through its architecture. It seems to me that the quest for global totalitarian power is not behind us but is a true promise of the future. If the network architecture culminates in one global building then there must be one power that controls it. The central political question of our time is the nature of this future power.[10]

A Renaissance of the State

The early internet, in the hearts and minds of its idealists, was something of an anarchic place. John Perry Barlow prefigured the "cyber-idealist" position in his manifesto, "A Declaration of the Independence of Cyberspace," published in 1996. Barlow asserts that the network and its inhabitants are independent from the old-fashioned rules and regulations of territorial states, who have "no sovereignty where we gather":

> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here. ... Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonwealth, our governance will emerge. Our identities may be distributed across many of your jurisdictions.[11]

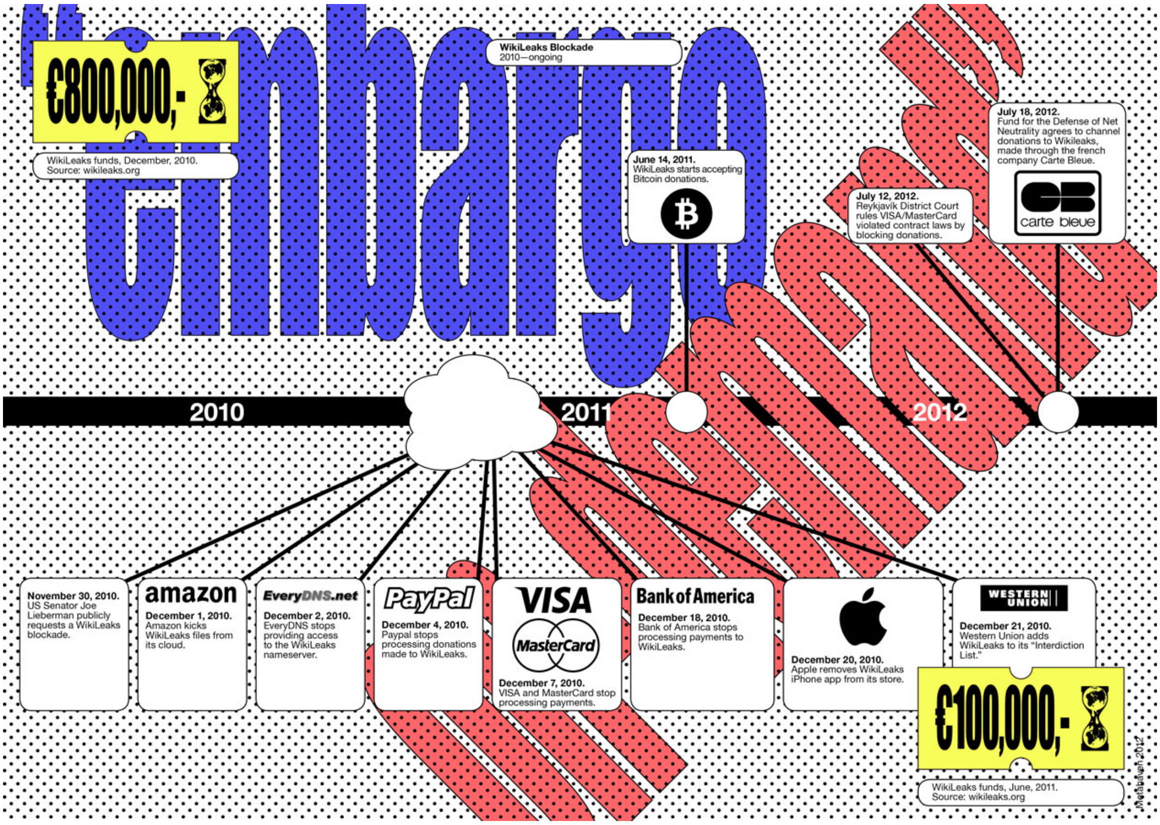
Barlow's manifesto declared cyberspace a socio-political commons. A space seemingly beyond gravity, beyond the state – "a world that all may enter without privilege or prejudice"; "a world where anyone, anywhere may express his or her beliefs." Barlow's ideas have somehow resonated; indeed, Saskia Sassen mentions that "a distinct issue concerning the relation between the state and digital networks is the possibility for the average citizen, firm, or organization operating in the internet to escape or override most conventional jurisdictions." Some of this thought, according to Sassen, is "still rooted in the earlier emphasis of the internet as a decentralized space where no authority structures can be instituted."[12] Milton Mueller comments that cyber-libertarianism "… was never really born. It was more a prophetic vision than an ideology or 'ism' with a political and institutional program. It is now clear, however, that in considering the political alternatives and ideological dilemmas posed by the global internet we can't really do without it …"[13]

Confusingly and hilariously, one place where the *rhetoric* of borderless information freedom is most pervasive is in the cloud. The world's most powerful information companies have inserted some of the internet's foundational optimism in their mission statements. These tech giants talk about themselves as heartwarming charities. Every billionaire CEO is his own private Dalai Lama. Pseudo-liberal jabberwocky of assumed universal validity permeates the junkspace of mission statements, annual reports, and TED talks, especially when it comes to the cloud. Microsoft wants to help everyone around the world "realize their full potential."[14] Facebook aims to give "people the power to share and make the world more open and connected."[15] Skype makes it "simple to share experiences with the people that matter to you, wherever they are."[16] And Instagram, bought by Facebook, envisions "a world more connected through photos."[17]

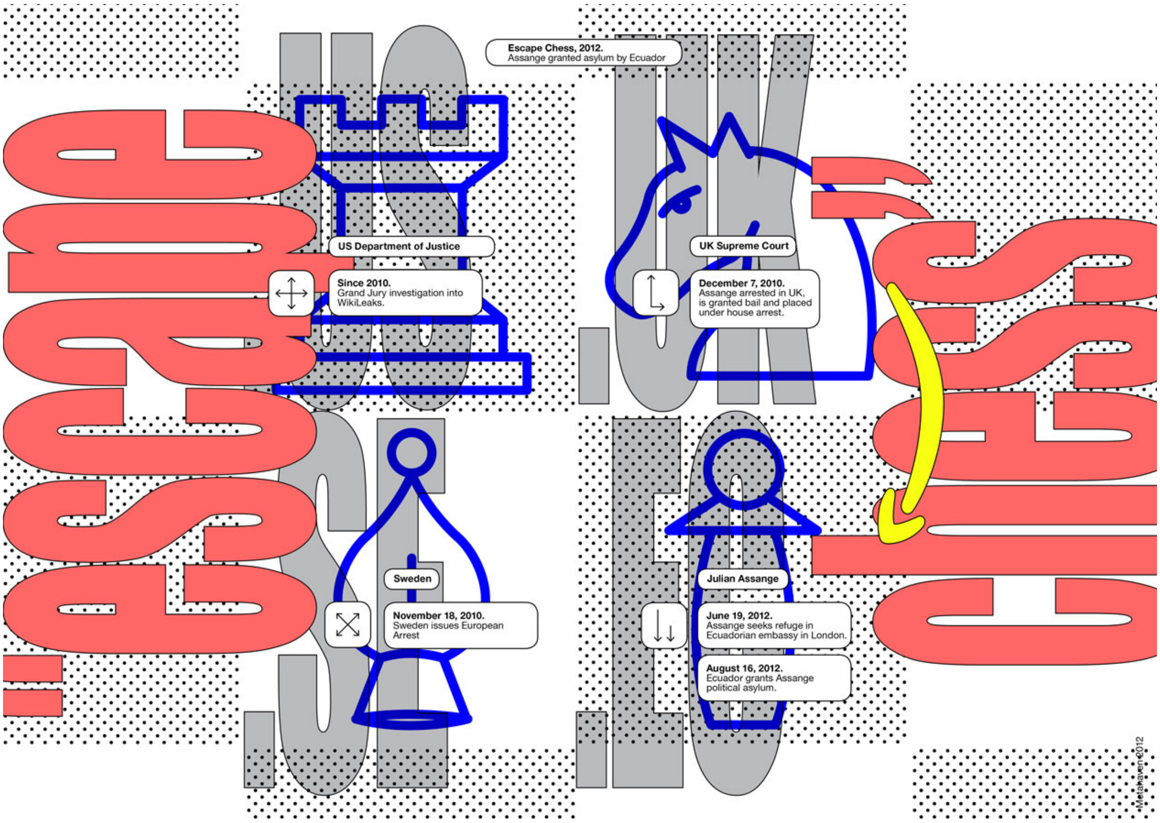
Cyber-utopianism never translated into a policy outlook of sorts. But it is still associated with a set of practices and spatial forms: online anonymity, cryptography, Peer-To-Peer (P2P) file sharing, TOR (The Onion Router) bridges, bulletproof hosting, and offshore data havens, to name a few examples. Michael Froomkin, a professor at the University of Miami School of Law, defined the data haven in 1996 as "the information equivalent to a tax haven."[18] This "place where data that cannot legally be kept can be stashed for later use; an offshore web host" appears omnipresent in the cyber-libertarian universe of thought, and is indeed an extreme form of keeping information away from antagonistically minded states, corporations or courts.[19] The data haven is the spatial form that, at least theoretically, enables the evasion of sovereign power, while establishing an enclosed territory on the face of the earth. The data haven once provided a business model for the Principality of Sealand, an unrecognized mini-state founded by a British family on a former war platform in the North Sea. A notorious example in internet law, Sealand was, in the early 2000s, home to the servers of HavenCo, a startup providing offshore data hosting beyond the reach of any jurisdiction.[20] HavenCo joined the dotcom boom with angel investment from Joi Ito (among others), who declared himself, still in 2002, "a great fan of the concept."[21] Sealand's fragile sense of half-tested nationhood would theoretically raise the bar for any opposing jurisdiction to physically invade the offshore host. It would, indeed, demonstrate that cyber-libertarian ideology could take full control of an experimental country, and reform the internet in its name. James Grimmelmann, a professor at New York Law School, is skeptical about Sealand and HavenCo's treatment of the law:

> HavenCo was selling the end of law. 'Third-world regulation' was a euphemism for minimal regulation – or none at all. In its search for the lowest common denominator, HavenCo was willing to divide by zero.[22]

Grimmelmann also questions HavenCo's effectiveness, as "for most purposes, cheap commodity hosting on one side of the Atlantic or the other could easily outcompete Sealand's more expensive boutique product in the middle of the North Sea."[23] Grimmelmann rhetorically continues, "in an age of YouTube, BitTorrent, and the darknet, who needs HavenCo?"[24] Sealand was the flagship store of the internet's anarcho-libertarian movement. The P2P BitTorrent platform The Pirate Bay famously tried to buy the ailing principality in 2007, offering citizenship.[25] Michael Froomkin, in a June 2012 lecture at the Oxford Internet Institute, sketched out an arresting and slightly dystopian view of the current internet. It looked like a complete dichotomy – a dialectic between two opposing visions, each serving broadly similar goals by completely antithetical means.[26] The dialectic was between "Cypherpunk Dream" and "Data's Empire" (see diagram), where most of the anarchic (Barlow-style) stuff would be on the first side, and most of the cloud and surveillance on the other. Oddly, two cloud-based services, YouTube and Twitter, still appeared under the Cypherpunk Dream, presumably because of the pivotal role both services play in online activism and "getting the information out." Froomkin connects Data's Empire to a "renaissance of the state" – a re-emergence of state power over the network and the networked, perhaps, Froomkin suggests, in an unwitting reaction to a largely unrealized spectre of internet utopianism and anarchy. While both the Cypherpunk Dream and Data's Empire seem to have a business model, the first one's is Ayn Rand-style anarcho-capitalism, while the latter's looks more like a digital form of industrial capitalism. The cloud, with its data factories, "scalability,"


embargo
€800,000,-
WikiLeaks funds, December, 2010.
Source: wikileaks.org
WikiLeaks Blockade
2010—ongoing
June 14, 2011.
WikiLeaks starts accepting Bitcoin donations.
July 12, 2012.
Reykjavík District Court rules VISA/MasterCard violated contract laws by blocking donations.
July 18, 2012.
Fund for the Defense of Net Neutrality agrees to channel donations to Wikileaks, made through the french company Carte Bleue.
carte bleue
2010
2011
2012
November 30, 2010.
US Senator Joe Lieberman publicly requests a WikiLeaks blockade.
amazon
December 1, 2010.
Amazon kicks WikiLeaks files from its cloud.
EveryDNS.net
December 2, 2010.
EveryDNS stops providing access to the WikiLeaks nameserver.
PayPal
December 4, 2010.
Paypal stops processing donations made to WikiLeaks.
VISA
MasterCard
December 7, 2010.
VISA and MasterCard stop processing payments.
Bank of America
December 18, 2010.
Bank of America stops processing payments to WikiLeaks.
December 20, 2010.
Apple removes WikiLeaks iPhone app from its store.
WESTERN UNION
December 21, 2010.
Western Union adds WikiLeaks to its "Interdiction List."
€100,000,-
WikiLeaks funds, June, 2011.
Source: wikileaks.org
Metahaven 2012

The WikiLeaks blockade: an embargo by a private "cloud" of companies, impacting the site's key resources. The actual embargo is below the timeline; some of the "countermeasures" are displayed above it.


escape
chess
.US
.UK
.SE
.EC
Escape Chess, 2012.
Assange granted asylum by Ecuador
US Department of Justice
Since 2010.
Grand Jury investigation into WikiLeaks.
UK Supreme Court
December 7, 2010.
Assange arrested in UK, is granted bail and placed under house arrest.
Sweden
November 18, 2010.
Sweden issues European Arrest
Julian Assange
June 19, 2012.
Assange seeks refuge in Ecuadorian embassy in London.
August 16, 2012.
Ecuador grants Assange political asylum.
Metahaven 2012

Escape Chess: Julian Assange's jurisdictional cat-and-mouse game with the powers that be.

standardization and centralization, indeed looks a little like an industrial revolution, yet it is one largely one without a working class. This industrial complex actually dislikes most things that are small. Indeed, many of Silicon Valley's cloud protagonists practice "acq-hiring": promising startups are purchased only to get hold of their talented staff, while the product or concept that staff worked on gets discarded.[27] One of the most arresting aspects of Froomkin's scheme however is not in the dialectic as such, but in the reason he suggests for why it came about in the first place.

The Legal Void of "Like" vs. "Law"

Cyber-libertarians, in hopes of evading the state's grasp, assumed that its coercive powers would be constrained by jurisdictional and constitutional limits. As James Grimmelmann concisely puts that thought, "HavenCo simultaneously thumbed its nose at national law and relied on international law to protect Sealand."[28] The possibility of states evading their own law, or international law, going rogue, sub- or supra-legal in their handling of disruptive actors, was not considered. The dream of offshore information freedom reflects this vision. But state power can be deployed in a legal void, as was recognized early on by James Boyle, a professor of law at Duke University. In his 1997 text *Foucault in Cyberspace*, Boyle refuted much of the legalistic optimism of cyber-utopianism:

> Since a document can as easily be retrieved from a server 5,000 miles away as one five miles away, geographical proximity and content availability are independent of each other. If the king's writ reaches only as far as the king's sword, then much of the content on the Net might be presumed to be free from the regulation of any *particular* sovereign.[29]

Even then, Boyle argued, de facto authority can still be exercised by the state, as

> the conceptual structure and jurisprudential assumptions of digital libertarianism lead its practitioners to ignore the ways in which the state can often use privatized enforcement and state-backed technologies to evade some of the supposed practical (and constitutional) restraints on the exercise of legal power over the Net.[30]

Boyle stressed that state power doesn't need to operate in ways that confront its constitutional limits. In a similar vein, Grimmelmann concludes that "no matter what a piece of paper labeled 'law' says on it, if it has no correspondence with what people do, it is no law at all."[31] And indeed, it isn't. A mere thirteen years after *Foucault in Cyberspace*, the controversial whistleblowing web site WikiLeaks found itself to be the living proof of this, as it became embargoed by US companies.

WikiLeaks began in 2007 as an "uncensorable" web platform for the release of leaked documents. Through an anonymous drop box, users could upload digital files to WikiLeaks. The material would be published only if it had not been published before, and if it were of historical, ethical, or political significance. The site first used a wiki format, where users and members would analyze and comment on on the leaks. The wiki format was since abandoned, but the name WikiLeaks remained. The site would be practically uncensorable for any government, since its hosting was set up in multiple jurisdictions. Its materials would be stored on servers in multiple countries, and thus be protected by the laws of these countries – a bit like a distributed version of the Sealand data haven. On July 29, 2009, as WikiLeaks published the high-exposure loan book of the bankrupt Kaupthing Bank, the site ran a discouraging note for its adversaries which demonstrated the legal firewalls it had constructed for itself against state and corporate power:

> No. We will not assist the remains of Kaupthing, or its clients, to hide its dirty laundry from the global community. Attempts by Kaupthing or its agents to discover the source of the document in question may be a criminal violation of both Belgium source protection laws and the Swedish constitution.[32]

Upon receiving a complaint from Kaupthing, a Reykjavik court silenced Iceland's national broadcaster RUV, which was planning to break the story on television. So instead of airing the story, the TV host pointed viewers to the WikiLeaks web site, where they could see the documents for themselves – to great social and political effects in Iceland. WikiLeaks could evade the gag order by hosting its information offshore – indeed, multiple times so. It was, as Boyle would say, beyond the power of a *particular* sovereign. WikiLeaks systematically won its jurisdictional chess games until, on November 28, 2010, it began releasing its biggest leak ever: a trove of hundreds of thousands of classified diplomatic communications from US embassies all over the world, now commonly referred to as "Cablegate."

WikiLeaks' source of income is crowdfunding; the site relies on public donations, processed by the Wau Holland Foundation based in Kassel, Germany. Wau Holland is reported to have collected about one million euros in donations to WikiLeaks in 2010. This, according to CBS News, would have paid WikiLeaks founder Julian Assange a salary of about sixty-six thousand euros that year.[33] The crowdfunding went through "conventional payment channels": PayPal, an online payment system owned by eBay, Western Union, and VISA and MasterCard, two corporations which together virtually dominate the credit card market. One could say that the WikiLeaks donations relied on a private "cloud" of intermediary, US-based companies. According to WikiLeaks' own account, funding after the release of the first cables peaked at an all-time high of 800 thousand individual donations in a single month.[34]

Upon the release of the cables, WikiLeaks' Sweden-based servers were hit by a vast distributed denial of service (DDOS) attack, which compelled the organization to make the move of hiring cloud space from Amazon Web Services (AWS). On December 1, 2010, a day after the site's move to the cloud, Amazon kicked all WikiLeaks files from its servers, marking the effective beginning of a pan-industrial, state-corporate embargo.[35] Amazon's decision was prompted by an aggressive call to arms from Joe Lieberman, senior US Senator for Connecticut, and chairman of the Senate Committee on Homeland Security. Lieberman urged American enterprises – including Amazon – to stop providing services to the whistleblowing site, even though he had no legal authority to enforce this.[36] His words amounted to nothing more than an opinion. Lieberman took the position of both accuser and judge, stating that "it sure looks to me that Assange and WikiLeaks have violated the Espionage Act."[37] The result was that WikiLeaks' vital infrastructure fell through, as key companies withdrew themselves from WikiLeaks without the check of a court. EveryDNS, a California-based domain name registry, stopped providing access to the wikileaks.org domain name server, so that the site would only be reachable if a user entered its IP address in the browser bar. MasterCard, PayPal, VISA, and Western Union ceased to process WikiLeaks donations. Apple removed a WikiLeaks iPhone app from its store, as was noted in Part I of this essay. These operations, together, amounted to an extra-legal embargo for which the organization was unprepared. Yochai Benkler, a professor of law at Harvard University, examines the embargo in detail in a 2011 article, analyzing how WikiLeaks became constrained by "a large-scale technical distributed-denial-of-service (DDoS) attack with new patterns of attack aimed to deny Domain Name System (DNS) service and cloud-storage facilities, disrupt payment systems services, and disable an iPhone app designed to display the site's content." Benkler asserts that the attack came from multiple sources, some of which were more clearly and directly involved and identified than others. Yet indirectly and opaquely, Yochai Benkler argues, the attack came on behalf of the Obama administration,

> having entailed an extra-legal public-private partnership between politicians gunning to limit access to the site, functioning in a state constrained by the First Amendment, and private firms offering critical functionalities to the site – DNS, cloud storage, and payments, in particular – that were not similarly constrained by law from denying service to the offending site. The mechanism coupled a legally insufficient but publicly salient insinuation of illegality and dangerousness with a legal void.[38]

James Boyle asserted that there can be a "formal language of politics organized around relations between sovereign and citizen, expressed through rules backed by sanctions," versus an "actual experience of power." The distinction is significant – it captures, spot on, the role of the state in the WikiLeaks embargo. The "actual experience of power" operates much more like a social network – Senator Lieberman occupying a powerful node, capable (or, believably suggesting being capable) of a potentially devastating set of cascading effects in case his friendly suggestions are not followed up – Don Corleone's offer you can't refuse, pure and simple. Power then is to personally govern the pressing and depressing of "Like" buttons, deciding on life or death, like Romans once presided over the fate of gladiators. Facebook's "Like" symbol – a thumbs up – has its origins in ancient Rome. Arguably, Lieberman clicked the "Dislike" – thumbs down – on WikiLeaks, causing a wave of consequences resulting from his private, social, network power, while backed by his stature as a Senator. James Grimmelmann comments:

> It is not just that Lieberman possesses the usual sovereign power, so that his public statements are raw threats. There is a political cost to him to pushing legislation; it will have to be checked by the judicial system, etc. Rather, he is a actor within a nexus of sovereign, economic, and social power, leveraging some of those in service of his goals.[39]

The WikiLeaks financial embargo by VISA and MasterCard was fought in an Icelandic court by DataCell, the company acting as WikiLeaks' local payment processor. A July, 2012 ruling required that Valitor, VISA and MasterCard's payment handling agent in Iceland, should resume processing donations to the site as a contractual obligation to DataCell. The ruling was touted (by WikiLeaks) as "a significant victory against Washington's attempt to silence WikiLeaks."[40] It remains, however, questionable as to whether the order against Valitor will actually restore funding to the site. James Grimmelmann doubts that US payment links to WikiLeaks are answerable to the Icelandic ruling. He suggests that

> global payment networks still have seams along national boundaries. Valitor, a company which can be thought of as Wikileaks' "accepting bank," will not necessarily have donation payments to process. The ruling does not affect the embargo still in place by VISA and Mastercard who continue to control the money flow between the issuing bank (on behalf of their customers) and Valitor.[41]

Sveinn Andri Sveinsson, a lawyer for DataCell, is less pessimistic. Sveinsson was quoted calling the victory a "good day for the freedom of expression."[42] Still, the case was decided as a matter of contractual law rather than constitutionality.[43]

The situation for WikiLeaks got worse when the organization's founder, Julian Assange, was accused of (but not charged for) sexual misconduct in Sweden. This led Interpol to issue a Red Notice – normally reserved for the likes of Muammar Gaddafi – for Assange's arrest, and an ensuing two-year standoff between Assange and UK prosecutors. After Assange lost his appeal against his extradition to Sweden at the Supreme Court in May 2012, the WikiLeaks founder escaped to the Ecuadorian Embassy in London, applying for (and receiving) political asylum – apparently not to evade Swedish accusations, but to prevent Assange's possible extradition to the United States on presumed charges of espionage.[44]

The lines along which Assange's legal team fought his extradition, followed by his move into the embassy, are in remarkable consistency with WikiLeaks' multi-jurisdictional hosting model. The case brought to the surface deep ambiguities in the treaties regulating extraditions, prompting the *Cambridge Journal of International and Comparative Law* to argue that the UK Supreme Court's decision displayed "a fundamental mistake" in its judgment.[45] At the embassy, meanwhile, Assange's life seems to have become fully equivalent to that of WikiLeaks' data. The Ecuadorian outpost here is like an offshore internet server, beyond the grasp of Western powers – and indeed, there was widespread anger when Britain briefly threatened Ecuador to annul the status of its London embassy's premises.[46]

Assange himself frequently deploys chessboard metaphors when talking about jurisdiction in a multipolar world. His personal television show, *The World Tomorrow*, was produced by RT, the Western branch of Russia's state broadcaster (which, as especially liberal commentators prefer to add, is "Kremlin-backed"). As Assange explained to the *Daily Mail* in September 2012, "if it proceeds to a prosecution then it is a chess game in terms of my movements. I would be well advised to be in a jurisdiction that is not in an alliance with the US ..." In Assange's view,

> we must see the countries of the world as a chess board with light and dark areas in ever shifting arrangements depending on our latest publication.[47]

If WikiLeaks, and Julian Assange, are making one thing clear, it is that the jurisprudential assumptions of cyber-libertarianism can have a visceral afterlife in the nondigital, material world. Traditional liberal-constitutional niches like freedom of expression and civil disobedience are no longer that convincing; they, in a sense, exhibit the same weaknesses as Sealand and the Pirate Bay in their wide-eyed expectation of state power curbed by law. The gross inequality in resources between the state and its idealist critics becomes painfully obvious when states deliberately shred to pieces, like discarded paperwork, legally certified limits on their executive power. It is becoming increasingly obvious that liberal-democratic conceptions like network neutrality, internet freedom, and freedom of expression, despite their key democratic value, don't give any actual protection to those who need them most. In a global internet under a renaissance of the state, it is not just the network, but *the networked*, who are the ultimate subject of power.

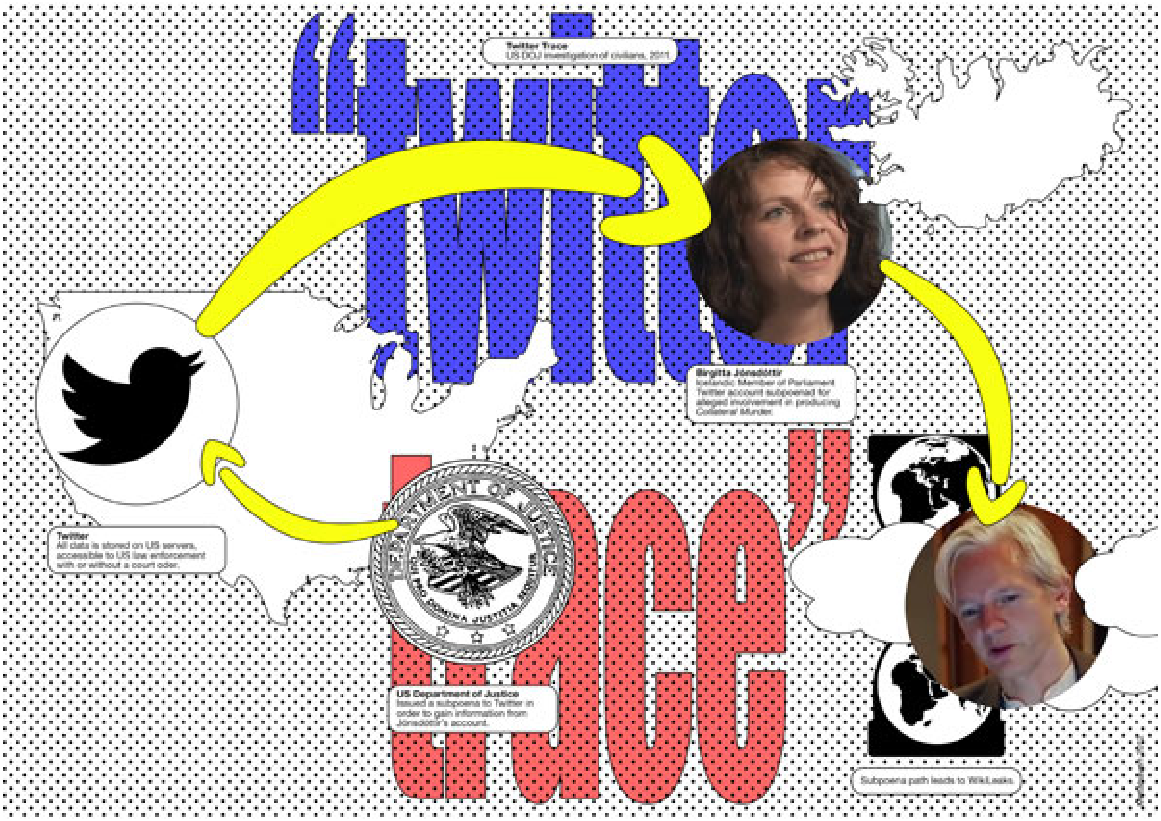
Captives of the Cloud, or: the Dissent of the Networked

In early 2011, Birgitta Jónsdóttir, an Icelandic Member of Parliament, found out that the US Department of Justice sought information about her Twitter account. Jónsdóttir was under investigation because of her alleged involvement in the making of a WikiLeaks video called

Collateral Murder, which was edited and produced in Iceland in 2010.[48] The video documents the shooting of unarmed civilians in Baghdad by a US helicopter crew; the scene was filmed from the gun turret camera of an Apache attack helicopter. The video material used in *Collateral Murder* was received by WikiLeaks from a source in the US military, alleged to be Private First Class Bradley Manning. Manning is currently under a court martial pretrial for charges including "aiding the enemy." A Grand Jury investigation into WikiLeaks brought about the DOJ's interest in the Jónsdóttir's Twitter information, along with the account information of Jacob Appelbaum and Rob Gonggrijp, computer experts who are also alleged to have helped with the production of *Collateral Murder*. All Twitter user information is stored on servers in the US, which are accessible to US law enforcement with or without a court order. The subpoena was issued so that the receiving party was forbidden from talking about it; Twitter's lawyer however successfully lifted the gag order, so that Jónsdóttir, Gonggrijp and Appelbaum could be informed about the subpoena. On November 13, 2011, Jónsdóttir tweeted:

> A foreign government would have a hard time getting permissions for officials entering my offline home, same should apply to online home.[49]

Her message was retweeted over 100 times. The problem is that in the cloud, there is no equivalent to a "home." Cloud computing may sometimes mimic or emulate some of the virtues of the anarcho-libertarian internet, such as anonymous PGP keys and personalized security architecture.[50] Amazon Web Services – a company which extra-legally censored WikiLeaks on the request of Joe Lieberman – boasts that it errs on the side of "protecting customer privacy," and is "vigilant in determining which law enforcement requests we must comply with." Indeed, it heroically says, "AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis."[51] However, all cyber-anarchic playtime must happen under the gaze of the web's digital Walmart, without any definition of what a "solid basis" is. In addition, the possibility of revolving door interests between business and government can't be ruled out either. Amazon's current, Washington D.C.-based Deputy Chief Information Security Officer is reported to possess a "distinguished career in federal government security and law


"twitter trace"
Twitter Trace
US DOJ investigation of civilians, 2011
Birgitta Jónsdóttir
Icelandic Member of Parliament
Twitter account subpoenaed for alleged involvement in producing Collateral Murder.
Twitter
All data is stored on US servers, accessible to US law enforcement with or without a court oder.
US Department of Justice
Issued a subpoena to Twitter in order to gain information from Jónsdóttir's account.
Subpoena path leads to WikiLeaks.

Twittertracing in the cloud: the US Department of Justice, in its pursuit of WikiLeaks, subpoenaed Icelandic MP Birgitta Jónsdóttir's Twitter account.

enforcement."[52] A cloud service provider's own security staff may in various ways – socially, geographically, and through expertise – be already intimately connected to the very law enforcement agencies whose requests it is supposed to scrutinize. As Rebecca Rosen explains, the notion of data storage being handled by a cloud provider already removes some of the legal constraints on evidence-gathering by law enforcement, especially on subpoenas:

> Grand jury subpoenas are used to collect evidence. Unlike warrants, subpoenas can be issued with less than probable cause. The reasoning for the lower bar is in part that if someone does not want to turn over the requested evidence, he or she can contest the subpoena in court. Grand juries can subpoena not only the person who created a document but any third parties who might be in possession of that document. Under the Stored Communications Act, a grand jury can subpoena certain types of data from third parties whose only role is storing that data.[53]

This, then, reflects an outdated idea of a third party's role in a subpoena. At the time the law developed, it could be assumed that "any third party with access to someone's data would have a stake in that data and a relationship with the person who created it." As Rosen concludes, "in the old days of storing information in filing cabinets, subpoena power was constrained because people didn't save everything and investigators had to know where to look to find incriminating evidence."[54] A cloud provider is a new kind of third party; it manages and hosts vast troves of personal data belonging to its customers. But it is not a stakeholder in such data. Neither was the manufacturer of a filing cabinet a stakeholder in the private documents stored in it. There are many such filing cabinets in the cloud, storing the online self. Together, they form the scattered "online home" we inhabit. Information in the cloud perversely echoes the utopian dream of a weightless and autonomous internet, independent from the constraints of territory. But this utopian dream is, in reality, a centrally managed corporation. As James Gleick writes,

> all that information—all that information capacity—looms over us, not quite visible, not quite tangible, but awfully real; amorphous, spectral; hovering nearby, yet not situated in any one place. Heaven must once have felt this way to the faithful. People talk about shifting their lives to the cloud—their informational lives, at least. You may store photographs in the cloud; e-mail passes to and from the cloud and never really leaves the cloud. All traditional ideas of privacy, based on doors and locks, physical remoteness and invisibility, are upended in the cloud.[55]

Jónsdóttir, Appelbaum and Gonggrijp tried to find out if, and which, other social media companies had received similar subpoenas. They had reason to believe this would be the case, because Twitter is known (and often praised) for collecting relatively little information about its users; it would seem, as Glenn Greenwald wrote, "one of the least fruitful avenues to pursue" for the DOJ to rely solely on Twitter information.[56] Jónsdóttir's demands for transparency were flatly refused. US Attorney Neil MacBride wrote in a court filing that her request demonstrated an "overriding purpose to obtain a roadmap of the government's investigation." MacBride further stated that

> the subscribers have no right to notice regarding any such developments in this confidential criminal investigation – any more than they have a right to notice of tax records requests, wiretap orders, or other confidential investigative steps as to which this Court's approval might be obtained.[57]

This is a brazenly imperialist thing for MacBride to say. If the US government wants, for the purpose of a "confidential criminal investigation," to have the tax records of a non-US citizen like Jónsdóttir, it can't simply subpoena them from a US cloud service. It must file a case with a foreign government, and demonstrate probable cause. Apparently, to MacBride, obtaining information on a non-US subject from a US server is the same obtaining such information from foreign territory; smooth compliance is simply expected, and indeed presupposed. In a piece for the *Guardian*, Jónsdóttir referred to her legal ordeal as an example of ongoing attempts of the US to silence the truth as a means of maintaining power. She wrote that the DOJ's subpoena constituted a "hack by legal means."[58] Perhaps out of a misunderstanding of the mechanisms of social media, or out of genuine Orwellian intent, cloud subpoena procedures can take on grotesque dimensions. For example, in December 2011, the Boston District Attorney subpoenaed Twitter over the following material:

> Guido Fawkes, @p0isonANon, @occupyBoston, #BostonPD, #d0xcak3.[59]

The subpoena sought not just information on a specific user, but on all users connected to certain words and hashtags associated with the Occupy movement's activities in Boston, and the hacktivist collective Anonymous, at a given point in time. WikiLeaks, in linking to this story, tweeted that it was now time for Twitter to move its servers offshore.[60] The Australian journalist Bernard Keane concluded from the Boston DA's bizarre "fishing expedition" that

> the only real solution is social media networks outside the jurisdiction of nation-states. WikiLeaks is currently establishing its own social network, Friends of WikiLeaks, and Anonymous has established AnonPlus; there have also been anonymous microblogging sites such as Youmitter established, but their lack of critical mass is a key impediment, as is resilience in the face of surges in traffic, and they remain vulnerable, to the extent that it's enforceable, to authorities claiming to exercise jurisdiction over whatever servers are used to host the networks.[61]

Groys's "future power" over the network is unlikely to pose direct, legal limits on free speech. Instead, like in the WikiLeaks embargo, it directly affects the material basis of those who speak. One is tempted to think of the ways in which the FBI pursued hacker collectives Anonymous and LulzSec after their DDoS attacks on MasterCard and VISA. The FBI fully exploited the real-world frailties and vulnerabilities of the hackers, who presented themselves as invulnerable superheroes online. But they weren't, in reality. The authorities made no qualms about the question whether or not Anonymous and LulzSec's cyber-conflict entailed acts of "civil disobedience." They were treated as cyber-terrorists, and the option for their practices to constitute a legitimate realm of civic protest was eclipsed – even though some of the most thorough previous analysis of Anonymous had focused on these possibilities.[62] One of the group's most prominent members, Sabu, was apprehended by the FBI and turned into an informant. *New York Magazine* wrote about Sabu, using his real name instead of his online pseudonym:

> On the day that he joined forces with the hacker collective Anonymous, Hector Xavier Monsegur walked his two little girls half a dozen blocks to their elementary school. "My girls," he called them, although they weren't actually his children. Monsegur, then 27, had stepped in after their mother – his aunt – returned to prison for heroin dealing.[63]

Ars Technica adds that "worried about the fate of two children in his charge, Monsegur has allegedly been aiding the FBI since his arrest last summer – aid which culminated in arrests today of several LulzSec members."[64] The *Guardian* completes this story, as

> Monsegur ... provided an FBI-owned computer to facilitate the release of 5m emails taken from US security consultancy Stratfor and which are now being published by WikiLeaks. That suggests the FBI may have had an inside track on discussions between Julian Assange of WikiLeaks, and Anonymous, another hacking group, about the leaking of thousands of confidential emails and documents.[65]

The space of flows is absolutely not smooth. It looks like a data center, and the coal plant that powers it. It looks like Julian Assange's room in the Ecuadorian Embassy in London. It looks like the Principality of Sealand. It looks like Sabu's social housing unit on Manhattan's Lower East Side. The landing from the digital onto the material is hard; it comes with a cruelty and intensity we haven't even begun to properly understand. Along these lines, we might grasp an emerging political geography of information, resources, and infrastructure. In such a geography, the state and the cloud are among the most important layers, but they are not the only layers by far. Saskia Sassen writes that we need to problematize "the seamlessness often attributed to digital networks. Far from being seamless, these digital assemblages are 'lumpy,' partly due to their imbrications with nondigital conditions."[66]

Once again, the world indeed is lumpy enough for us not to draw easy conclusions. This story is not over yet. Tomorrow's clouds are forming.

×

'Written by Daniel van der Velden and Vinca Kruk. Research Assistant: Alysse Kushinski. Design Assistants: Rasmus Svensson, Allison Kerst and Michael Oswell. All images courtesy of Metahaven. Metahaven 2012.

To be continued in "Captives of the Cloud: Part III. Tomorrow's Clouds."

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] Julian Assange, in: "The Julian Assange Show: Cypherpunks Uncut (p.1)", *RT.com*, July 29, 2012. See http://www.youtube.com/watch?v=i85fX9-sKYo

[2] Milton Mueller, *Networks and States. The Global Politics of Internet Governance.* Cambridge (MA): The MIT Press, 2010, 9-10.

[3] Manuel Castells, *The Information Age: Economy, Society and Culture, Vol I: The Rise of the Network Society* (Malden, MA: Blackwell 1996 [2000]), 442.

[4] Ibid.

[5] Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006), 73.

[6] James Gleick, *The Information: A History, a Theory, a Flood,* (New York: Pantheon Books, 2011), 396.

[7] James Glanz, "The Cloud Factories: Power, Pollution and the Internet," *New York Times*, September 22, 2012. See http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html?pagewanted=1&ref=technology.

[8] When, for example Dutch filmmaker Marije Meerman, while working on a documentary about the financial crisis and the role of high-speed trading, wanted to find data centers servicing the New York Stock Exchange, she found no official record of where these were located. Instead, Meerman tracked them down by looking for clues on the web sites of the construction companies that built them, and by flipping through local files of New Jersey town hall meetings. Eventually, she mapped a ring of data centers around New York City. See Marije Meerman, lecture at Mediafonds, Amsterdam, January 12, 2012, and http://itunes.apple.com/us/app/money-speed-inside-black-box/id424796908?mt=8.

[9] Pier Vittorio Aureli. In Pier Vittorio Aureli, Boris Groys, Metahaven, and Marina Vishmidt, "Form." In *Uncorporate Identity* (Baden: Lars Müller, 2010), 262.

[10] Boris Groys. In Pier Vittorio Aureli, Boris Groys, Metahaven, and Marina Vishmidt, "Form." In *Uncorporate Identity* (Baden: Lars Müller, 2010), 263.

[11] John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, February 8, 1996. See https://projects.eff.org/~barlow/Declaration-Final.html.

[12] Saskia Sassen, *Territory – Authority – Rights. From Medieval to Global Assemblages*, (Princeton/Oxford: Princeton University Press, 2006, 2008), 330.

[13] Milton Mueller, *Networks and States*, 268.

[14] "About Microsoft" See http://www.microsoft.com/about/en/us/default.aspx.

[15] See Gillian Reagan, "The Evolution of Facebook's Mission Statement." *New York Observer*, July 13, 2009. See http://observer.com/2009/07/the-evolution-of-facebooks-mission-statement/.

[16] See "About Skype" see http://about.skype.com/.

[17] See Instagram FAQ http://instagram.com/about/faq/.

[18] A. Michael Froomkin, "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases,"*University of Pittsburgh Journal of Law and Commerce* 395 (1996). See http://osaka.law.miami.edu/~froomkin/articles/ocean.htm.

[19] See "Data Haven by Bruce Sterling from Islands in the Net", technovelgy.com. See http://www.technovelgy.com/ct/content.asp?Bnum=279.

[20] The Principality of Sealand is discussed at length in our book, *Uncorporate Identity*. In our interview with hacker, cryptographer, and internet entrepreneur Sean Hastings, a self-styled inventor of Sealand's data haven, Hastings declared that "the world needs a frontier. Every law, for good or ill, is an imposition on freedom. The frontier has always been a place for people who disagree with the morality of current law to be able to get away from it." Sean Hastings, in "The Rise And Fall Of The Data Haven, Interview with Sean Hastings," Metahaven and Maria Vishmidt eds., *Uncorporate Identity* (Baden: Lars Müller, 2010), 65. Later examples include Seasteading, an enterprise founded by Patri Friedman, designed to be a set of sovereign floating sea vehicles under ultraminimal governance without welfare or taxes. In

2011, Seasteading received funding from Paypal founder Peter Thiel. This “libertarian sea colony” was directly modeled after the Principality of Sealand, mixed with the gated community, the ranch, and the cruise ship. It is uncertain whether such physical havens, if realized in the first place, will ever escape their founding vision of conservative-libertarian frontier romanticism. See Cooper Smith, “Peter Thiel, PayPal Founder, Funds ‘Seasteading,’ Libertarian Sea Colony,” Huffington Post, August 19, 2011, see http://www.huffingtonpost.com/2011/08/18/peter-thiel-seasteading_n_930595.html.

[21] Joi Ito, “Havenco Doing Well According BBC.” Quoted from Slashdot, July 10, 2002. See http://joi.ito.com/weblog/2002/07/10/havenco-doing-w.html

[22] James Grimmelmann, “Sealand, Havenco, And The Rule Of Law.”*Illinois Law Review* 405, 2012, 460. See http://illinoislawreview.org /wp-content/ilr-content/articles/2012/2/Grimmelmann.pdf

[23] Grimmelmann, “Sealand, Havenco, And The Rule Of Law.” 462.

[24] Grimmelmann, “Sealand, Havenco, And The Rule Of Law.” 463.

[25] Cory Doctorow, “Pirate Bay trying to buy Sealand, offering citizenship.” boingboing.net, January 12, 2007. See http://boingboing.net/2007/01/12/pirate-bay-trying-to.ht ml.

[26] Michael Froomkin, “Internet Regulation at a Crossroads.” Lecture at Oxford Internet Institute, University of Oxford, June 2012. YouTube. See http://www.youtube.com/watch?v=b2aVcdcr4MA.

[27] See Liz Gannes, “The Vanity of the ‘Acqhire’: Why Do a Deal That Makes No Sense?” *AllThingsD*, August 10, 2012. See http://allthingsd.com/20120810/the-vanity-of-the-acqhire -why-do-a-deal-that-makes-no -sense/

[28] Grimmelmann, “Sealand, Havenco, And The Rule Of Law.” 479.

[29] James Boyle, *Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors,* 1997. See http://law.duke.edu/boylesite/foucault.htm.

[30] Ibid.

[31] Grimmelmann, “Sealand, Havenco, And The Rule Of Law.” 484.

[32] “Icelandic bank Kaupthing threat to WikiLeaks over confidential large exposure report.” *WikiLeaks.org,* July 31, 2009. See http://wikileaks.org/wiki/Icelandic_bank_Kaupthing_threat_to_WikiLeaks_over_confidential_large_exposure_report,_31_Jul_2009.

[33] See Xeni Jardin, “WSJ obtains Wikileaks financial data: spending up, donations down.” *Boingboing*, December 24, 2010.See http://boingboing.net/2010/12/24/wsj-obtains-wikileak.html and Joshua Norman, “WikiLeaks’ Julian Assange Now Making $86k/year.” *CBS News*, December 24, 2010. See http://www.cbsnews.com/8301-503543_162-20026597-5035 43.html.

[34] See “Banking Blockade.” *WikiLeaks.org.* See http://wikileaks.org/Banking -Blockade.html.

[35] Ryan Paul, “Wikileaks kicked out of Amazon’s cloud.” *Ars Technica*, December 1, 2010. See http://arstechnica.com/security/2010/12/wikileaks-kicked -out-of-amazons-cloud/.

[36] Alexia Tsotsis, “Sen. Joe Lieberman: Amazon Has Pulled Hosting Services For WikiLeaks.” *Techcrunch*, December 1, 2010. See http://techcrunch.com/2010/12/01/amazon.

[37] Paul Owen, Richard Adams, Ewen MacAskill, “WikiLeaks: US Senator Joe Lieberman suggests New York Times could be investigated.” *The Guardian*, December 7, 2010. See http://www.guardian.co.uk/world/2010/dec/07/wikileaks-jo e-lieberman-new-york-times-investigated.

[38] Yochai Benkler, “WikiLeaks and the Protect-IP Act: A New Public-Private Threat to the Internet Commons,” *Daedalus* 4 (2011), 154–55.

[39] James Grimmelmann, e-mail to author. July 17, 2012.

[40] Charles Arthur, “WikiLeaks claims court victory against Visa.” *The Guardian*, July 12, 2012. See http://www.guardian.co.uk/media/2012/jul/12/wikileaks-court-victory-visa.

[41] James Grimmelmann, e-mail to author, July 17, 2012.

[42] Omar R. Valdimarsson, “Iceland Court Orders Valitor to Process WikiLeaks Donations.” *Bloomberg*, July 12, 2012. See http://www.bloomberg.com/news/2012-07-12/iceland-court-orders-valitor-to-process-wikileaks-donations-1-.html.

[43] Charles Arthur, *The Guardian*. Ibid. See http://www.guardian.co.uk/media/2012/jul/12/wikileaks-court-victory-visa.

[44] William Neuman and Maggy Ayala, “Ecuador Grants Asylum to Assange, Defying Britain.” *The New York Times*, August 15, 2012. See http://www.nytimes.com/2012/08/17/world/americas/ecuador -to-let-assange-stay-in-its-embassy.html?pagewanted=all&_r=0

[45] Tiina Pajuste, “Assange v Swedish Prosecution Authority: the (mis)application of European and international law by the UK Supreme Court - Part I.” *Cambridge Journal of International and Comparative Law*, June 20, 2012. See http://www.cjicl.org.uk/index.php?option=com_easyblog&view=entry&id=22&Itemid=101

[46] The British authorities sent a letter to Ecuador saying that “You need to be aware that there is a legal base in the UK, the Diplomatic and Consular Premises Act 1987, that would allow us to take actions in order to arrest Mr Assange in the current premises of the embassy. We sincerely hope that we do not reach that point, but if you are not capable of resolving this matter of Mr Assange’s presence in your premises, this is an open option for us.” See Mark Weisbrot, “Julian Assange asylum: Ecuador is right to stand up to the US.” *The Guardian*, August 16, 2012. See http://www.guardian.co.uk/commentisfree/2012/aug/16/julian-assange-asylum-ecuador

[47] Sarah Oliver, “‘It’s like living in a space station’: Julian Assange speaks out about living in a one-room embassy refuge with a mattress on the floor and a blue lamp to mimic daylight.” *The Daily Mail,*September 29, 2012. See http://www.dailymail.co.uk/news/article-2210522/Its-like -living-space-station-Julian -Assange-speaks-living-room-embassy-refuge-mattress-floor-blue-lamp-mimic-daylight.html

[48] See Raffi Khatchadourian, “No Secrets. Julian assange’s mission for total transparency.” *The New Yorker*, June 7, 2010. See http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?currentPage=all.

[49] Twitter. See https://twitter.com/ioerror/statuses/135980031037022208.

[50] See “AWS Security and Compliance Center.” See http://aws.amazon.com/security/.

[51] See “Amazon Web Services: Risk and Compliance White Paper July 2012.” See http://d36cz9buwru1tt.cloudfront.net/AWS_Risk_and_Compliance_Whitepaper.pdf.

[52] See Malcolm Ross, “Appian World 2012 – Developer Track.”*Appian.com*, March 16, 2012. See http://www.appian.com/blog/uncategorized/appian-world-2012-developer-track.

[53] Rebecca J. Rosen, “How Your Private Emails Can Be Used Against You in Court.” *The Atlantic*, July 8, 2011. See http://www.theatlantic.com/technology/archive/2011/07/how-your-private-emails-can-be -used-against-you-in-court/241505/

[54] Ibid.

[55] James Gleick, *The Information*, 395–96.

[56] Glenn Greenwald, “DOJ subpoenas Twitter records of several WikiLeaks volunteers.” *Salon.com*, January 8, 2011. See http://www.salon.com/2011/01/08/twitter_2/singleton/.

[57] Kevin Poulsen, “Feds: WikiLeaks Associates Have ‘No Right’ To Know About Demands For Their Records.” *Wired*, June 2, 2011. See http://www.wired.com/threatlevel/2011/06/wikileaks-twitt er/

[58] Birgitta Jónsdóttir, “Evidence of a US judicial vendetta against WikiLeaks activists mounts.” *The Guardian*, July 3, 2012. See http://www.guardian.co.uk/commentisfree/2012/jul/03/evidence-us-judicial-vendetta-wikileaks-activists-mounts?INTCMP=SRCH.

[59] Bernard Keane, “The Boston fishing party and Australians’ rights online.” *Crikey*, January 17, 2012. See http://www.crikey.com.au/2012/01/17/the-boston-fishing-party-and-australians-rights-online/.

[60]

Twitter. See http://twitter.com/wikileaks/status/159247260121706496

[61] Bernard Keane, ibid.

[62] See Gabriella Coleman, *The Many Moods Of Anonymous*: Transcript. Discussion at NYU Steinhardt, March 4, 2011. See http://www.onthemedia.org/2011/mar/04/the-many-moods-of-anonymous/transcript/

[63] Steve Fishman, “Hello, I Am Sabu ... “ *New York Magazine*, June 3, 2012. See http://nymag.com/news/features/lulzsec-sabu-2012-6/

[64] Nate Anderson, “LulzSec leader ‘Sabu’ worked with FBI since last summer.” *Ars Technica*, March 6, 2012. See http://arstechnica.com/tech-policy/2012/03/report-lulzse c-leader-sabu-worked-with-fb i-since-last-summer/

[65] Charles Arthur, Dan Sabbagh and Sandra Laville, “LulzSec leader Sabu was working for us, says FBI.” *The Guardian*, March 7, 2012. See http://www.guardian.co.uk/technology/2012/mar/06/lulzsec -sabu-working-for-us-fbi

[66] Saskia Sassen, Ibid., 382-3.