Continued from "Captives of the Cloud, Part II"

> *A Massive, Expanding Surveillance State With Unlimited Power And No Accountability Will Secure Our Freedom by Hans Christian Andersen.*
> – twitter.com/pourmecoffee[1]

> *Violence arms itself with the inventions of Art and Science in order to contend against violence.*
> – Carl von Clausewitz[2]

Metahaven

Captives of the Cloud, Part III: All Tomorrow's Clouds

> *Infrastructure is the technology that determines whether we live or die. Your infrastructure will kill you – if it fails, you fail.*
> – Smári McCarthy[3]

The internet began as a place too complicated for nation-states to understand; it ended up, in the second decade of the twenty-first century, as a place only nation-states seem to understand. This has left omnipresent cloud giants Google and Yahoo!, in their own words, "outraged." They are helpless bystanders to US spy agencies as they extraterritorially, without permission, and aided by the Brits, break into data center cables just to find out if the next Bin Laden is out there posting kitten videos on YouTube. In response, Germany and Switzerland cash in on "secure" clouds; Russia fortifies its digital walls, incarcerates Pussy Riot, and offers asylum to Edward Snowden. Ecuador, which hosts Julian Assange in its London Embassy as a political refugee, is to rebrand itself as a "haven for internet freedom."[4] These recent developments show the deep divide between the perspectives of various governments often claiming to restore national sovereignty over data space, and the very nature of the network itself, which is by definition transnational and borderless.

Internet and Society: The Dots Fight Back

General Keith Alexander is the director of the US National Security Agency. In his previous position as the head of the US Army Intelligence and Security Command, Alexander had an architectural firm decorate his so-called "Information Dominance Center" to look like the Starship Enterprise control room. This helped him gain political enthusiasm for spying. As *Foreign Policy* notes, "Lawmakers and other important officials took turns sitting in a leather 'captain's chair' in the center of the room and watched as Alexander, a lover of science-fiction movies, showed off his data tools on the big screen."[5] At the time of this writing, Alexander is to step down from his position after a taxing year at the helm of the spyboat. Before Edward Snowden gave thousands of the agency's top-secret documents to the press, Alexander used to publicly appear in full military attire. Sometimes he tried to win sympathy by taking the stage in a black T-shirt. In Las Vegas in 2012, Alexander urged digital troublemakers to join the NSA; he also pleaded that his agency operated lawfully and transparently. “We are overseen by everybody,” he said.[6] But that was 2012. There were Patriot Act abuses, National Security Letters, and overzealous US prosecutors going after The Pirate Bay, Megaupload, WikiLeaks, and Chelsea Manning. As early as 2002, Mark Klein, an AT&T technician, witnessed an NSA-controlled wiretapping room in full operation in a data center in San Francisco. Later, a handful of US Senators warned the media about a secret interpretation of the Patriot Act.[7] Nobody listened.

Then came Edward Snowden. As the magnitude of the NSA's surveillance of global internet and phone communications systems was being revealed, Keith Alexander changed his public relations tactics accordingly, appearing as an obedient, invisible bureaucrat. At Def Con 2013, Alexander presented his mission: “connecting the dots.” Hoovering up everything from everyone up to three degrees of separation, or “hops,” away from a known suspect in order to avert the next 9/11.[8] Columbia University law professor Eben Moglen called it, plainly, “spying on humanity.”[9] Alexander was simply following an organization-wide, 9/11-centered PR memo given out as a script to its representatives.[10] Meanwhile, the NSA boasted that its surveillance had thwarted fifty-four terrorist attacks. However, that number lacked a real basis in fact, as the website ProPublica concluded after research.[11]

Keith Alexander's spaceship-style ops room sparks the same dark pleasure as the happy smile that sits on a hand-drawn NSA diagram about infiltration into Google and Yahoo![12] Alexander – the man who plotted to ruin the reputation of islamic “radicalizers” by publicly revealing their porn site visits – is, after all, the pseudo-amicable human incarnation of neo-Stalinism.[13] The NSA uses corruption with martial agility. “Overseen” by opaque FISA courts, whose deliberations and decisions are secret, it has built a giant, data-slurping behemoth facility in Utah: a Wal-Mart holding everyone’s indeterminate digital past. Lost in a Berlusconian *bunga bunga* party, the NSA dreamed that its operations could go unseen forever. When asked by Congress if the NSA collected data on millions of Americans, the Director of National Intelligence, James Clapper, politely replied under oath: “No, sir … not wittingly.”[14] Clapper later apologized for misleading Congress by giving the “least untruthful answer.”[15]

In one cunning operation, the NSA wielded its power to influence the technical standards on which the internet itself relies, including the pseudo-random number generators that occupy our computers’ microchips. As Yochai Benkler asserts, the NSA “undermined the security of the SSL standard critical to online banking and shopping, VPN products central to secure corporate, research, and healthcare provider networks, and basic email utilities.”[16] Jennifer Granick calls the NSA “an exceedingly aggressive spy machine, pushing – and sometimes busting through – the technological, legal and political boundaries of lawful surveillance.”[17] Half-hearted attempts by the Obama Administration to curb the agency's powers do little to reverse the situation. A newly appointed oversight committee is, as Benkler notes, stocked with insiders of the national security shadow world, even as the President claims, in awe-inspiring legalese, that it consists of “independent outside experts.” Surprise: the Obama-appointed chief curator of the committee is James Clapper himself.[18] According to *Slate*, the proposed post-Snowden NSA reform bill, spearheaded by Democratic Senator Dianne Feinstein, “for the first time *explicitly authorizes,* and therefore entrenches in statute, the bulk collection of communications records, subject to more or less the same rules already imposed by the FISA Court. It endorses, rather than prohibits, what the NSA is already doing.”[19] Showing his deep understanding of the privacy concerns of ordinary people, President Obama ordered an end to the NSA’s spying on the IMF and the World Bank.[20]

Global Standards

Initially known for its quirky minimalism and math, Google has been working hard on its emotional impact on the public. Its vice president for marketing said in 2012 that “if we don’t make you cry, we fail. It’s about emotion, which is bizarre for a tech company.”[21] Free email, chat, and social networking are the Coke and McDonalds of the internet. But they don’t promise Americanness. They promise connections. The largest cloud services are global standards. They are “natural,” thus dominant, focal points in the network, offering the largest potential social reward and likelihood of connection. “Network power” obscures less popular alternatives. The ultimate container of network power is the mobile app, which bypasses the shared internet and its protocols entirely. Instead, users are permanently within the corporation’s digital walls rather than in and out of it through their web browser.[22]

Google's top executives Eric Schmidt and Jared Cohen published *The New Digital Age,* a trailblazing book about their political ideas, and how Google interacts with American power abroad. WikiLeaks’s Julian Assange finds that in this paper-bound TED speech, a

> liberal sprinkling of convenient, hypothetical dark-skinned worthies appear: Congolese fisherwomen, graphic designers in Botswana, anticorruption activists in San Salvador and illiterate Masai cattle herders in the Serengeti are all obediently summoned to demonstrate the progressive properties of Google phones jacked into the informational supply chain of the Western empire.[23]

Indeed, every transaction on a Google server is an event under American jurisdiction.

Solutionism

The seizure of the internet by public-private technocrats, cloud providers, and secret services is an example of what Evgeny Morozov calls “solutionism.”[24] Solutionism takes problems from social and political domains and recalibrates them as issues to be dealt with by technology alone. It brings them under the control of programmers, systems managers, Silicon Valley entrepreneurs, and their political avatars. Privacy and civil liberties are brushed aside: technological bypasses to political, social, and legal problems present themselves everywhere as progress. Who rules the internet on whose behalf, as ridiculously archaic as the question may sound, is a political and legal issue highjacked by solutionism. Milton Mueller phrases it slightly differently, as “who should be 'sovereign' – the people interacting via the Internet or the territorial states constructed by earlier populations in complete ignorance of the capabilities of networked computers.”[25]

It is uncertain whether sovereignty is attainable at all; whether it, *as a concept*, holds up against the network, with its winner-takes-it-all technologies. Security expert Bruce Schneier says we must “take back” the internet: “Government and industry have betrayed the internet, and us ... We need to figure out how to re-engineer the internet to prevent this kind of wholesale spying. We need new techniques to prevent communications intermediaries from leaking private information.”[26]

“No Water = No Data Center”

Infrastructure gets political when things don’t work. As long as they do, no questions are asked. Drinking water is instantly political when nothing comes out of the faucet. Scarcity is a big politicizer. The broken internet grapples with an opposite problem: it bathes in an overabundance of apps and services, which thrive on the deterritorialization, expropriation, and extortion of life and data. Benjamin Bratton calls this “microeconomic compliance.”[27] It is probably the most convenient model of exploitation that has ever existed.

The people on the internet live in territories. They have citizenship. But this feedback loop doesn’t activate political agency. What, after all, really *is* the connection between these things – “indifference, weariness and exhaustion from the lies, treachery and deceit of the political class” perhaps, as Russell Brand aptly stated?[28] Snapchat and Instagram are vehicles of social (and geopolitical) lure, endlessly more attractive than our tacit complicity with the machinery of representative politics. No one talks about political revolution, but the “Twitter Revolution” makes headlines in mainstream media. The only problem with our digital tools is their underlying standardization. We have an exhausted political machine on the one hand – “citizenship” forced into tiresome, backward rituals of participation. And on the other hand, we have the splendor and immediacy of love, friendship, connection, and technology built on microecononomic and geopolitical compliance. It seems an all too easy win for the latter. People have not considered the internet as a democratically governable structure. Decisions on the internet are delegated to a giant “don't be evil” mix.

Carne Ross, a former British diplomat and founder of Independent Diplomat, is looking for a solution beyond technology. “The balance between the individual and state needs to be more fundamentally altered,” argues Ross. “New rules, in fact new kinds of rules, are needed. What is required is nothing less than a renegotiation of our contract with the state, and with each other.”[29] Ross's proposal is not technical or bureaucratic. It is political in the most personal sense. Its problem is that it draws on decision-making and enforcement structures which don't yet exist. People can look out for their common good only when they share common space and interest. They can work out their own polity better than central governments can, as Ross argues in his book *The Leaderless Revolution,* which promotes benign anarchism. Indeed, it is unclear how a renegotiation of the internet's social contract might be achieved without a unifying political mechanism for those on the network who can’t bargain with the status quo. For those forced into compliance with its already dominant standards. Or for those who don’t yet know the faces of their friends.

Some version of a social contract between citizens and governments (and corporations) was demonstrated in 2012 when citizens across the world successfully prevented the Stop Online Piracy Act and the Protect IP Act from coming into effect.[30] “Social contract” here means the possibility for people to bargain with the powerful about measures that threaten the common good. Major websites like Google and Wikipedia sided with the protesters against SOPA/PIPA, which somewhat nuances the familiar picture of “evil corporations.” However, this type of legislation tends to silently return in a different guise, most recently with the highly secretive Trans-Pacific Partnership (TPP) agreement. The Intellectual Property portion of this agreement was leaked to WikiLeaks in November, 2013.[31]

A social contract for the internet requires governments and corporations to welcome its political inconveniences. It requires them to radically cut back on surveillance. It requires them to unambiguously legalize leaks, cyberprotests, and online civil disobedience as legitimate political expressions. As noted in Part II of this essay, in 2010 and 2011 UK- and US-based hacktivists used DDoS attacks to target private corporations that imposed a corporate embargo against WikiLeaks. The hacktivists responsible were hunted down and tried as criminals; the analogy between hacktivism and nonviolent civil disobedience was lost on the system and its judges. Cyberprotests express the *absence* of any verifiable and binding agreement between the system and its users. Digital equivalents to strikes and blockades are framed as crimes against property and profit.

The activist group NullifyNSA has taken on the task of disabling the NSA by shutting off the water supply to its data centers. The fascinating proposition is a stark reminder that the ability to spy and to store data is ultimately dependent on electricity and cooling. Thus, any “internet” operation is ultimately dependent upon the living environment and its resources. Michael Boldin, executive director of the Tenth Amendment Center and a NullifyNSA representative, explains that

> In Utah, the new data center is expected to need 1.7 million gallons of water per day to keep operational. That water is being supplied by a political subdivision of the state of Utah. Passage in that state of the 4th Amendment Protection act would ban all state and local agencies from providing material support to the NSA while it continues its warrantless mass surveillance. No water = no data center.[32]

NullifyNSA is politically on the libertarian-conservative Right. Its ideas are, as Boldin says,

> backed up by the advice of James Madison. The Supreme Court has repeatedly issued opinions over the years backing it up in a widely accepted legal principle known as the anti-commandeering doctrine. The cases go all the way back to the 1840s, when the court held that states couldn't be forced to help the feds carry out slavery laws. The latest was the Sebelius case in 2012, where the court held that states couldn't be compelled to expand Medicaid, even under threat of losing federal funding.[33]

NullifyNSA has all of the Right’s typical rigor and determination even while it, as Boldin summarizes, seeks to be “transpartisan” in its efforts:

> Our goal is single-minded – stopping NSA spying. It's a long haul, and it's going to take significant effort and resistance from groups and people not used to working together. But the time is now to set aside differences for the liberty of all.[34]

The group explains the interdependency between the digital and the physical domains accurately and plainly. Almost no one on the Left seems to have talked about data centers quite like this. Boldin points out the ecological disaster that is the NSA, adding that “a state like Utah is in a state of near-constant drought. The fact that all these precious resources are being used to spy on the world should be disgusting to nearly everyone.”[35] He goes on to analyze the NSA's distribution of data centers and its implications for the organization’s own perception of its vulnerabilities:

> Back in 2006, the NSA maxed out the Baltimore area power grid. Insiders were very concerned that expansion of the NSA’s “mission” could result in power outages and a “virtual shutdown of the agency.” In reading their documents and press releases over the years, we know that a prime motivation in expanding their operations in Utah, Texas, Georgia, Colorado and elsewhere was to ensure that loads of resources like water, electricity, and more, were distributed. That means they know they have an Achilles heel.[36]

After all, the NSA’s weak point may be its insatiable appetite for electricity rather than its breaches of the Constitution. NullifyNSA, a group of conservatives with a practical bent, hints at the under-investigated relationship between data centers and their physical geographies.[37]

The Possibility of an Iceland

"Data sovereignty" is a phrase of recent coinage describing two distinct trends in internet hosting. The first is the increasing tendency of nation-states to make networks that fit within national borders so they can completely control what goes on inside the network. Russia and China both have their own Facebook and Twitter, controlled at all times by the state. The only advantage of these networks is that they are not under the auspices of the NSA. Boutique data sovereignty is a viable economic strategy in the wake of global surveillance. Secure "email made in Germany" is now hot; user data are protected by supposedly watertight German privacy laws.[38] Swisscom, Switzerland's telecommunications company, which is majority-owned by the government, is developing a secure "Swiss cloud" aspiring to levels of security and privacy which US companies can't guarantee.[39] Luxembourg and Switzerland's recent wealth havens, or freeports for property in transit – mostly expensive art – also offer data storage.[40]

The second definition of "data sovereignty" is personal. Every internet user should "own" all of his or her online data. Jonathan Obar critiques the idea, but for the wrong reasons. He claims that personal data sovereignty is fallible because we have now "big data":

> Recent calls for personal data sovereignty, or the ability for a single individual to have control over all of their personal data, represent a similar fantasy. Had we the faculties and the system for enabling every digital citizen the ability to understand and continually manage the evolving data-driven internet, to control the data being collected, organized, analyzed, repurposed and sold by every application, commercial organization, non-commercial organization, government agency, data broker and third-party, to understand and provide informed consent to every terms of service agreement, and privacy policy – would we have time to actually use the internet? To work? To have a family? To do anything else? This is the fallacy of personal data sovereignty in a digital universe increasingly defined by big data.[41]

The saying goes that if your only tool is a hammer, all problems look like nails. Data may need to be prevented from becoming "big" in the first place. Obar inadvertently shows the conceptual similarity of "big data" to bad financial products that no one understands. Personal data have become the credit default swaps of the cloud, building a bubble economy as unsustainable as the subprime mortgages that triggered the 2008 financial collapse. The NSA participates in this corporate feeding frenzy as much as cloud providers do. There is, in this light, nothing strange about wanting more personal control over one's personal information. A clear model for it is still missing, but a 2011 paper by US Naval Graduate School students notes that "data sovereignty provides an explicit tool to break a level of abstraction provided by the cloud. The idea of having the abstraction of the cloud when we want it, and removing it when we don't, is a powerful one."[42] To break down the abstraction of the cloud, the internet needs to be more localized.[43]

An example of the boundaries between nation-state politics and online politics being traversed is Iceland – a sparsely populated island nation in the North Atlantic that has come to be one of the rare places in the West where political alternatives get a chance. On July 5, 2008, John Perry Barlow gave a speech at the Reykjavík Digital Freedoms Conference. The talk was titled "The Right to Know."[44] Barlow took his audience on a journey that began with the wordless prehistory of *homo sapiens;* he ended by pitching a somewhat unexpected update of the "data haven" – an offshore sanctuary for information prefigured by cyberpunk science fiction. Iceland, Barlow said, could become a "Switzerland of Bits" – a haven for digital freedom, a safe harbor for transparency, a sanctuary for the Enlightenment. Cyberspace, for Barlow, was both global and local, and "the more local it becomes, the more global it becomes."

A mere three months after Barlow's talk, Iceland's banks collapsed. Relative to country size, it was the largest banking crisis ever suffered by a single state.[45] Iceland's recovery from the banking crisis became an opportunity for national democratic and ethical reforms. A twenty-five-strong Constitutional Assembly rewrote the constitution, and a crowdsourcing effort introduced thousands of comments and hundreds of concrete proposals from citizens directly into the legislative process.[46] On June 16, 2010, Iceland's parliament cast a unanimous vote for IMMI, the Icelandic Modern Media Initiative. IMMI combined a "greatest hits" of freedom of speech and libel protection laws that existed in various other countries.[47] And while the idea for the Switzerland of Bits came from Barlow, a cofounder of the Electronic Frontier Foundation, WikiLeaks also had an influence on IMMI's legal architecture: Assange's whistleblowing platform ran separate hosting agreements with ISPs in various countries, benefiting from their laws.

The internet activist, software developer, and writer Smári McCarthy is IMMI's executive director. Much of the organization's impact depends on Iceland's ability to influence new international standards, and to attract companies and organizations to host data.[48] At the same time, McCarthy is involved in the development of MailPile, a secure email application and collective decision-making software that is in the political lineage of "liquid democracy" – a form of delegative democracy. A founding member of the Icelandic Pirate Party, much of McCarthy's work takes place on the cutting blade of law and code.

McCarthy describes IMMI as an "NGO somewhere half-way between a think tank and a lobby group." Can IMMI transform Iceland into a Switzerland of Bits? McCarthy is unambiguous in his answer: "Yes. And not just Iceland." He explains: "Look through the legal code, the social structure, and pretty easy entry points start to become obvious. Treat society as a Wiki – a publicly editable social space – and be bold."[49]

James Grimmelmann, who is a Professor of Law at the University of Maryland, comments:

> I think Iceland's plans are viable and well-considered. They are using Iceland's legal sovereignty, real-world isolation, global connectedness, and stable political system to advance a series of pro-expression policy goals. They're doing so in ways that don't fundamentally alter Iceland's nature as a modern democratic state, but rather play to the theoretical and practical strengths of that model. And McCarthy shows a good understanding of what the limits to this strategy are, in terms of effects beyond Iceland's borders.[50]

In Iceland, the classical data haven has evolved into a more advanced combination of policy, software, coding, and advocacy, removing itself from the anarcho-libertarian free-for-all. The internet, here, is an experiment with democracy. The development of online communication and coordination tools certainly falls within IMMI's scope. The organization's technical director, Eleanor Saitta, explains its larger democratic vision:

> The Internet is an $11 trillion economy, globally. It's a largely post-national economy (to a degree that quantizing it in the currency of a single nation feels mildly ridiculous), but the effects of that economy touch specific people, on specific pieces of ground. What Iceland is becoming is a nation deeply integrated with the internet at an economic level. There are ways in which that resonates strongly and typologically with the notion of the "island" – it's a resonance we use at IMMI, sometimes, to explain our work. However, the fact that it's happening in a Scandinavian country also makes a big difference. Iceland has obviously seen its economy turned upside down by the massive financial looting of the past decade, but the fundamental collectivist nature of the country remains. This stands in stark contrast with the hyper-libertarian, "damn anyone who can't keep up" attitude common among crypto-anarcho-capitalists.
>
> Building a data haven means something very different when you do it in a place where people live and have lived for centuries, in a place where it is a national project, not an also-ran that at best injects a little cash and at worst exists only as network colonialism. The notion of resilience is critical here, too. While some large hosting companies are tentatively approaching sustainability as a concept, they're doing so to get punishing energy budgets down to something manageable and to comply with regulatory forces. Resilience is much more than sustainability; it meshes very closely with left-information politics, and in doing so, combines to provide a basic political platform much stronger than each alone. Hence in Europe, the limitations of the Pirates as (until their recent initial steps) a single-issue party; likewise, the Greens, mostly working from a relatively obsolete sustainability-only platform.[51]

Saitta sees the networked politics of the near future to be strongly interconnected with locality, so that the outcome is neither a purely nation-state-based affair nor commitment-free internet clicktivism. Such politics spring from a space of exception created both within the context of Iceland as a community and within the internet as a human network:

> As translated into the material context of neoliberal capitalism, this provides guidance for some specific corporation to decide where they wish to host servers, but the creation is an act of the commons ... Now, as to how network culture can create its own room in which to breathe, I think that's a much more interesting question, one where I think we will see networked

> post-institutional political non-state actors continuing to take a lead, to see that their politics leaks out from the internet into the real locality in which they may live. In creating room for themselves, they are in part looking at their place in the web of mutual obligation and stepping up to take their part in the deeper polis as much as they are drawing on and reinforcing the obligations of their localities to them.[52]

The design agenda for the future of the internet seems straightforward: become a networked, post-institutional, non-state actor and start right where you live with political reform. The idea of a "localized internet" anticipates increasing overlaps between digital and physical social structures. Eventually, all social structures take on physicality. Saitta:

> I joke that my ten year stretch goal is to kill the nation state, but really, I don't think that's particularly necessary. There will always be territorial organizational structures, but they're only one possible structure among many that can interact. I favor building up new alternatives, starting now. If we somehow magically did manage to destroy the nation state before there was anything to replace it, we'd all, quite frankly, be fucked. I'm a road fetishist. I really like roads. And power. And food. Those are all currently mostly provided by or coordinated through the state. Kill the state now, and life looks grim. That said, waiting until you've got a fully functional alternative before taking any kind of political action aimed at common emancipation is equally dumb, as is investing more effort in actively hostile systems when you can't actually change them. I'm a realist, in the end. I want less suffering, for everyone, in both the short and long term, and that doesn't come out of the barrel of any one ideology, just as surely as it isn't going to come by sticking to the straight and narrow of our status quo handbasket.[53]

Servers in the Clouds

The possibility for a network – centralized, decentralized, or distributed – to override jurisdiction and state power is a foundational dream of the internet, as well as a perpetual mirage shaped and inspired by science fiction. What was once thought to be "the internet" – a deterritorialized space amongst a world of nation-states – is known today to be incredibly saturated with the spatial implications of borders, jurisdictions, and sovereignty. New approaches to guaranteeing internet freedoms are increasingly becoming premised on literally eluding these spatial implications of a (perhaps always) reterritorialized internet.

The Pirate Bay is a famous Swedish-based P2P BitTorrent sharing service. Recently, access to its service was blocked in various countries and the site's three founders were sentenced on charges of enabling the violation of intellectual property by facilitating illegal downloads. At the time of this writing, the final sentences are still pending in Sweden, where the case has been brought to the Supreme Court. Apart from being a file sharing site, the Pirate Bay is also a kind of living manifesto for the cyber-anarchic internet; it has issued various memes, it had plans to buy the Principality of Sealand, and in March 2012, it issued an unusual announcement that detailed the next possibility for evading jurisdiction. The Pirate Bay announced that it would start hosting content on airborne drones, evading law enforcement and copyright claims.[54] The Pirate Bay's own tagline was: "Everyone knows WHAT TPB is. Now they're going to have to think about WHERE TPB is." While clearly part of the Pirate Bay's amazing array of publicity stunts and memes, the plan is not technologically impossible. In the same month, the website TorrentFreak interviewed Tomorrow's Thoughts Today, an organization exploring "the consequences of fantastic, perverse and underrated urbanisms," which has built a set of wirelessly connected drones operating like a mobile darknet.[55] These machines constitute what the organization says is "part nomadic infrastructure and part robotic swarm":

> We have rebuilt and programmed the drones to broadcast their own local wifi network as a form of aerial Napster. They swarm into formation, broadcasting their pirate network, and then disperse, escaping detection, only to reform elsewhere.[56]

Though some of the Pirate Bay's servers reportedly now operate out of a secret mountain lair,[57] its proposed Low Orbit Server Stations (LOSS) would host servers that redirect traffic to a secret location. Though the plan is, conceptually, a call for a deterritorialized internet space, it seems somewhat oblivious to the lingering legal implications of having a localized server. Tomorrow's Thoughts Today's *Electronic Countermeasures* project, on the other hand, is based equally on deterritoriality as well as locality. Liam Young, cofounder of Tomorrow's Thoughts Today, reflects:

> As a culture we are having to come to some kind of collective agreement about what copyright means in a digital age. Who owns information as it becomes a digital commodity. Industries and governments are too slow to adapt and projects like Electronic Countermeasures or The Pirate Bay drone servers are imagined for the purposes of examining these issues and speculating on new possibilities. The privatization of knowledge is something we all need to be thinking about. Moves toward the storage of all our data in the cloud, a cloud managed by private companies or nation states, is potentially very dangerous. Even if this drone network isn't implemented as a practical solution we would be just as interested if the work made us question what is happening and what alternatives there may be in data distribution.[58]

Young's "nomadic speculative infrastructures" are relatively harmless in areas that are already heavily covered by regulations. But in less regulated areas, they might become something more.

Failed States in International Waters

An island can be created either by expressly carving out law, or by not legislating at all. State power works both ways; negatively, some jurisdictions on the world map lack control over their borders and have no centrally administered rule of law – they are "'lawless' zones in various states of anarchy, poverty, decay and crime."[59] In international relations it has become customary to apply a set of rules to define statehood; a state needs to have control over borders, a centrally administered rule of law (even if a dictatorship), and to a considerable extent, it needs to comply with customary practices in "international society" or "the international system." As a normative categorization, this presupposes the institutional characteristics of Western statehood as the one legitimate form to which all states should aspire.

The term "failed state" was introduced in Western foreign policy to signify any state authority not substantially fulfilling either one of these criteria. Since the introduction of the term, various failed states have emerged, many of them in Africa: Somalia, Yemen, Sudan, and Mali are but a few examples. The designation of "failure" seems legitimate when applied to raging civil wars, violent conflicts, and their fallout. But it also points back to the political process, ideology, or entity that hands out the designation. In other words: one man's failed state is, potentially, another man's utopia. As Pierre Englebert and Denis M. Tull assert in their study on failed states and nation building in Africa:

> The goal of rebuilding collapsed states is to restore them as "constituted repositories of power and authority within borders" and as "performers and suppliers of political goods." Almost all African states, however, have never achieved such levels of statehood. Many are "states that fail[ed] before they form[ed]." Indeed, the evidence is overwhelming that most of Africa's collapsed states at no point in the postcolonial era remotely resembled the ideal type of the modern Western polity.[60]

Failed states can be seen as their own political model; a "failure" to produce outcomes compliant with accepted norms can be seen as a "success" in arenas where such norms are disputed. Failed states don't govern, don't hold a monopoly of violence, don't control borders, and don't enforce a rule of law. They are at the outer borders of the international system and the world political map. Insofar as they are still, partially at least, inside that system, they may present new opportunities for internet practice, new sovereignties for hosting, and new areas for nomadic infrastructure. James Grimmelmann outlines some of the complications that this model faces:

> The problem that failed states face is that it's difficult to create telecommunications infrastructure without security and a functioning economic system. They have domains that may not be effectively under their control and are backed up by an international body. Their internet infrastructure frequently relies on technological providers who operate from out-of-state; what is available is often of limited connectivity and quite expensive. *De facto*, these places of weak enforcement may tend to function as data havens – particularly when there are many of them – but the reliability of provisioning any specific content is low.[61]

A country like Cameroon presents a borderline case. There is digital infrastructure in the country, but its statehood appears to descend into failure anyway. In 2008, Ozong Agborsangaya-Fiteu warned that in his country, "unless there is clear political reform that will allow citizens to finally enjoy basic civil liberties – including full freedom of expression, free elections and the rule of law – a crisis is inevitable."[62] About a year later, internet security firm McAfee revealed that Cameroonian websites were the most dangerous in the world for their users – even more than Hong Kong websites. McAfee found that Cameroon boasts a shadow industry of "typo-squatting" domains. Typo-squatting exploits users who mistype a popular URL, leading them to a scam website. Cameroon's domain name extension (".cm") differs but one character from the ubiquitous ".com" – hence Cameroon's success in building popular Potemkin destinations based on typos. Facebook.cm, apparently, leads to a highly offensive porn ad.[63] Is the boom in "cybercrime" from countries with weak oversight some sort of data haven byproduct? Grimmelmann comments: "Yes, you could put it that way: I'm reminded of the Eastern European virus-writing 'industry.'"[64]

People before Clouds

In *The Truman Show* – with Jim Carrey starring as Truman, the unwitting protagonist of a real life sitcom – the series director, or "Creator," makes an emotional appeal to Truman in an attempt to convince him that reality *out there* is no better, and no more real, than reality *inside* the giant suburban Biosphere that was built for him. Truman's world is a world without visible signs of government; there are only signposts, and warnings, and red tape, at the *edges* of its liveable reality.

Government, for Truman, is the drone-like perspective of the series director. Isn't the point of view offered by NSA Director Keith Alexander similarly comforting? Keith Alexander begins almost every other sentence with the phrase "from my perspective." He won't really ever refer to anyone else's perspective, but it sounds as if he could. "From my perspective" sounds almost *modest*. Alexander has innumerable grandchildren and their love for iPads illustrates, for the General, the countless possibilities and threats of the "cyber." Alexander's NSA is about "saving lives," as if it were a virtual ambulance rushing to rescue the digitally wounded. He brags about his agency's "tremendous capabilities" as if he were a middle-aged computer room systems manager boasting about the robustness of his Apache server. How do we best escape the custody of this virtual father figure, and others standing in line to take over once he steps down? How do you liberate a society that has the internet?

No one really knows, but to begin with, we need to get rid of the deceptive gibberish of technocracy. We have become the enslaved consumers of nonsensical abstractions. No one has ever seen the cloud, or its main tenant, "big data." These are objects of ideology and belief, and at times, treacherous harbingers of Big Brother. Those who argue that we need new tools to fix the broken internet are right, but they shouldn't forget that we also need the right polities to use them. The spectacle of technology needs to be unleashed to further the ends of those who wish for a way of their own, rather than rule over others. People are real. Clouds aren't.

Reformist and legislative currents in the ongoing surveillance drama have put their stakes in institutions that are themselves the repositories of vested interests. This bureaucratic apparatus is incapable of reform, because it can't fire itself from the job it has done so badly for so long. Shielded from the most basic democratic accountability, an opaque data orgy plays out inside the boardrooms, spy bases, and data warehouses of surveillance.

Those who promote that we should, in response, encrypt all our communications, seem to have a strong point. Anonymizing technologies and other protections bring to mind the sort of privacy that was once expected from a sealed envelope or a safe. Yet on the other hand, the very argument for total encryption is the flipside of solutionism; it seeks for technology to solve a political problem. Encryption can't, by itself, heal the internet.

Separate from these two strands is a third possibility: a localized internet, one that wields the double-edged sword of political and technological reforms, and saves the network from being a looming abstraction manipulated by Silicon Valley entrepreneurs. We should be able to explain the network to each other in the simplest possible terms, in mutual agreement. We should not need to be under the gray cloud of a super-jurisdictional, abstract *Totalstaat.* We deserve to wake up from the dreamless lethargy that is induced by the techno-managerial matrix, and look each other in the eye.

New polities, new technologies, and new jurisdictions are needed – all three of them, in abundance. Democracy and people need to forever come before clouds. Drinking water needs to always be prioritized over spying. Life itself is the enemy of surveillance.

×

To be continued in Captives of the Cloud IV (slight return): Fix My Geopolitics!

Written by Daniel van der Velden, Vinca Kruk, and Alysse Kushinski (research assistant).

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] August 16, 2013.

[2] Carl von Clausewitz, *On War*, trans. J. J. Graham (London, 1873). See http://www.clausewitz.com/readings/OnWar1873/BK1ch01.html.

[3] Smári McCarthy, "Iceland: A Radical Periphery in Action. Smári McCarthy interviewed by Metahaven," *Volume* 32 (2012): 98–101.

[4] See http://www.buzzfeed.com/rosiegray/ecuador-bids-to-be-seen-as-the-home-of-internet-freedom

[5] See http://www.foreignpolicy.com/articles/2013/09/08/the_cowboy_of_the_nsa_keith_alexander?page=full

[6] See http://www.wired.com/threatlevel/2012/07/nsa-chief-denie s-dossiers/

[7] Senator Ron Wyden: "We're getting to a gap between what the public thinks the law says and what the American government secretly thinks the law says." Quoted in Mike Masnick, "Senators Reveal That Feds Have Secretly Reinterpreted the PATRIOT Act," *Techdirt,* May 26, 2011.

[8] "All of your friends, that's one hop. Your friends' friends, whether you know them or not – two hops. Your friends' friends' friends, whoever they happen to be, are that third hop. That's a massive group of people that the NSA apparently considers fair game." Quoted in Philip Bump, "The NSA Admits It Analyzes More People's Data Than Previously Revealed," *The Atlantic Wire*, July 17, 2013. See http://www.theatlanticwire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287/

[9] See http://snowdenandthefuture.info/PartI.html

[10] See http://america.aljazeera.com/articles/2013/10/30/reveale d-nsa-pushed911askeysoundbitetojustifysurveillance.html

[11] See http://www.theatlanticwire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287/

[12] See http://www.washingtonpost.com/world/national-security/ns a-infiltrates-links-to-yahoo -google-data-centers-worldwide-snowden-documents-say/201 3/10/30/e51d661e-4166-11e3-8 b74-d89d714ca4dd_story.html

[13] A document that reveals this NSA plot was published by the *Huffington Post.* The document's origin is "DIRNSA," the agency's director. See Glenn Greenwald, Ryan Gallagher, Ryan Grim, "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers,'" *Huffington Post,* November 26, 2013, http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html?1385526024

[14] Ruth Marcus, "James Clapper's 'least untruthful' answer," *The Washington Post,* June 13, 2013. See http://articles.washingtonpost.com/2013-06-13/opinions/39950057_1_oversight-national -intelligence-national-secur ity-agency

[15] Jason Howerton, "James Clapper Apologizes For Lying To Congress About NSA Surveillance: 'Clearly Erroneous'," *The Blaze,* July 2, 2013. See http://www.theblaze.com/stories/2013/07/02/james-clapper -apologizes-for-lying-to-congress-about-nsa-surveillance -clearly-erroneous/

[16] Yochai Benkler, "Time to tame the NSA behemoth trampling our rights," *The Guardian,* September 13, 2013. See http://www.theguardian.com/commentisfree/2013/sep/13/nsa-behemoth-trampling-rights

[17] Jennifer Granick, "NSA SEXINT is the Abuse You've All Been Waiting For," *Just Security,* November 29, 2013. See http://justsecurity.org/2013/11/29/nsa-sexint-abuse-youve-waiting/

[18] See http://www.huffingtonpost.com/2013/08/13/james-clapper_n_3748431.html

[19] David Weigel, "New NSA Reform Bill Authorizes All the NSA Activity That Was Making You Angry," *Slate,* November 1, 2013. See http://www.slate.com/blogs/weigel/2013/11/01/new_nsa_reform_bill_authorizes_all_the_nsa_activity_that_was_making_you.html

[20] Mark Hosenball, "Obama halted NSA spying on IMF and World Bank headquarters," *Reuters,* October 31, 2013. See http://www.reuters.com/article/2013/10/31/us-usa-securit y-

imf-idUSBRE99U1EQ20131031

[21] Claire Cain Miller, “Google Bases a Campaign on Emotions, Not Terms,” *The New York Times*, January 1, 2012. See http://www.nytimes.com/2012/01/02/technology/google-hones-its-advertising-message-playing-to-emotions.html?_r=2&

[22] See our discussion of network power in the book *Uncorporate Identity*.

[23] Julian Assange, “The Banality of ‘Don’t Be Evil’,” *The New York Times,* June 1, 2013.

[24] See “Evgeny Morozov on technology – The folly of solutionism,” *The Economist.com,* May 2, 2013.

[25] Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Boston, MA: MIT Press, 2010), 268.

[26] Bruce Schneier, “The US government has betrayed the internet. We need to take it back,” *The Guardian,* September 5, 2013. See http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

[27] See http://www.e-flux.com/journa l/some-trace-effects-of-the- post-anthropocene-on-accelerationist-geopolitical-aesthetics/

[28] See http://www.youtube.com/watch?v=3YR4CseY9pk

[29] Carne Ross, "Citizens of the world, unite! You have nothing to lose but your data," *The Guardian,* October 31, 2013. See http://www.theguardian.com/commentisfree/2013/oct/31/citizens-world-unite-data?CMP=twt_gu

[30] The US Congress withdrew the bills proposing SOPA and PIPA in February 2012 after widspread protests. Around the same time, the Anti-Counterfeiting Trade Agreement (ACTA) was successfully defeated by citizens in the European Union.

[31] See https://wikileaks.org/tpp/pressrelease.html

[32] Michael Boldin/NullifyNSA, email to authors, December 4, 2013.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] For NullifyNSA, see http://nullifynsa.com/

[38] Elizabeth Dwoskin and Frances Robinson, "NSA Internet Spying Sparks Race to Create Offshore Havens for Data Privacy," *The Wall Street Journal,* September 27, 2013. See http://online.wsj.com/news/articles/SB10001424052702303983904579096082938662594

[39] Caroline Copley, “Swisscom builds ‘Swiss Cloud’ as spying storm rages,” *Reuters,* November 3, 2013.

[40] See http://www.economist.com/news/briefing/21590353-ever-more-wealth-being-parked-fancy-storage-facilities-some-customers-they-are

[41] Jonathan A. Obar, “Phantom Data Sovereigns: Walter Lippmann, Big Data and the Fallacy of Personal Data Sovereignty” (March 25, 2013). See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239188

[42] See https://www.usenix.org/legacy/events/hotcloud11/tech/final_files/Peterson.pdf

[43] See the extensive study by Anselm Franke, Eyal Weizman, and Ines Geisler, “Islands: The Geography of Extraterritoriality” *Archis 6* (Amsterdam: Artimo, 2003): 19–21, http://www.scribd.com/doc/81773982/Franke-a-Weizman-e-i-the-Geography-of-Extraterritoriality

[44] See https://www.youtube.com/watch?v=snQrNSE1T7Y

[45] See http://www.economist.com/node/12762027?story_id=12762027

[46] “The Constitutional Council hands over the bill for a new constitution.” *Stjornlagarad,* July 29, 2011. See http://stjornlagarad.is/engl ish/

[47] “Iceland’s media law: ‘The Switzerland of bits,’” *The Economist*, June 17, 2010. See http://www.economist.com/blogs/babbage/2010/06/icelands_media_law

[48] "Birgitta Jónsdóttir – Samara/Massey Journalism Lecture.” Uploaded on July 21, 2011. See http://www.youtube.com/watch?v=MyFKP1VXFww

[49] “Iceland: A Radical Periphery in Action. Smári McCarthy interviewed by Metahaven,” *Volume* 32 (2012): 98–101.

[50] James Grimmelmann, email to authors, July 17, 2012.

[51] Eleanor Saitta, email to authors, November 4, 2012. See http://mthvn.tumblr.com/post/38457685064/decentralizationdesignandthecloud

[52] Ibid.

[53] Ibid.

[54] See http://arstechnica.com/tech-policy/2012/03/pirate-bay-plans-to-build-aerial-server-drones-with-35-linux-computer /

[55] See https://torrentfreak.com/worlds-first-flying-file-sharin g-drones-in-action-120320/

[56] Electronic Countermeasures GLOW Festival video, Liam Young. See http://www.tomorrowsthoughtstoday.com/

[57] “The Pirate Bay Ships New Servers to Mountain Complex,” *Torrent Freak,* May 16, 2011. See http://torrentfreak.com/the-pirate-bay-ships-new-servers -to-mountain-complex-110516/ .

[58] See http://mthvn.tumblr.com/post/41818910653/opensourcesky

[59] Franke, Weizman, Geisler, ibid.

[60] Pierre Englebert and Denis M. Tull, “Postconflict Reconstruction in Africa. Flawed Ideas about Failed States,” *International Security,* Vol. 32, No. 4 (Spring 2008): 106.

[61] James Grimmelmann, email to authors, July 17, 2012.

[62] Ozong Agborsangaya-Fiteu, “Another failed state? Cameroon's descent,” *International Herald Tribune,* April 10, 2008. See http://www.nytimes.com/2008/04/10/opinion/10iht-edcameroon.1.11865189.html?_r=0

[63] Andy Greenberg, “Cameroon's Cybercrime Boom,” *Forbes.com,* December 2, 2009. See http://www.forbes.com/2009/12/01/cybercrime-mcafee-spyware-technology-cio-network-cameroon.html

[64] James Grimmelmann, email to authors, July 20, 2012.