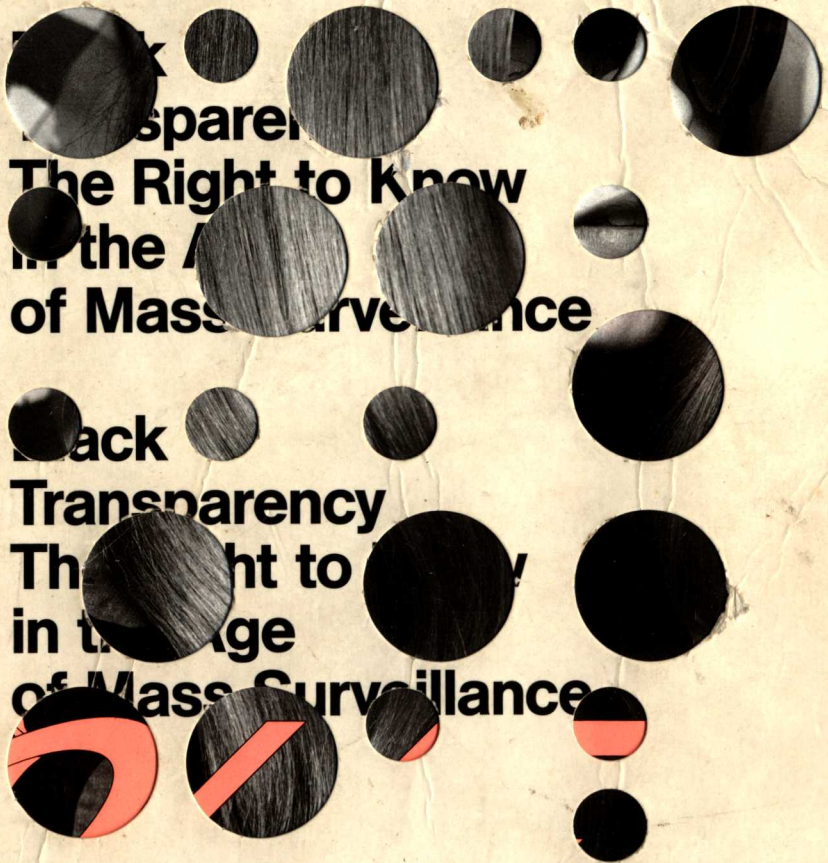


**Black
Transparency
The Right to Know
in the Age
of Mass Surveillance**

Metahaven



SternbergPress ✨



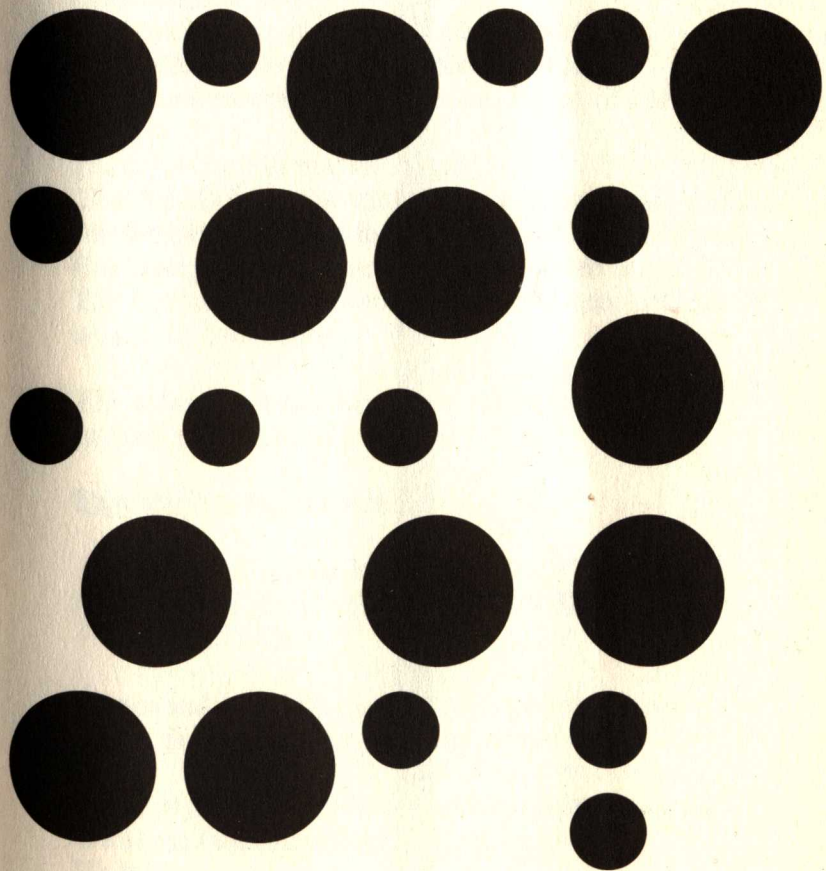
*Transparent Camouflage, 2011-13
Exhibition view of "Frozen Lakes,"
Artist's Space, New York, 2013
Photo: Denise Aron*

**BLACK TRANSPARENCY:
THE RIGHT TO KNOW
IN THE AGE OF MASS SURVEILLANCE**

The place where the traveller found himself seemed unpropitious for obtaining either shelter or refreshment, and he was likely to be reduced to the usual expedient of knights-errant, who, on such occasions, turned their horses to graze, and laid themselves down to meditate on their lady-mistress, with an oak-tree for a canopy. But the Black Knight either had no mistress to meditate upon, or, being as indifferent in love as he seemed to be in war, was not sufficiently occupied by passionate reflections upon her beauty and cruelty, to be able to parry the effects of fatigue and hunger, and suffer love to act as a substitute for the solid comforts of a bed and supper. He felt dissatisfied, therefore, when, looking around, he found himself deeply involved in woods, through which indeed there were many open glades, and some paths, but such as seemed only formed by the numerous herds of cattle which grazed in the forest, or by the animals of chase, and the hunters who made prey of them.

—Sir Walter Scott, *Ivanhoe: A Romance*

BLACK TRANSPARENCY



***CURSOR BLINKING
ATHENS, GREECE—DAY
PROTESTERS AND POLICE ENGAGE IN
SKIRMISHES AND RIOTS IN THE STREETS***

VOICE

This is largely incoherent.
This is the blinking cursor of our silence.

Here's democracy.
And then there's what protects democracy.
An irredeemable machine of mental murder.
A national security state-in-a-state. A Law of Silence.

Leaders assure us that all is well.
That we do have the values of democracy, and that its
weaponized protection keeps everybody safe and free.
But these protective operations are themselves secrets.
The executive means accrued to carry them out can be
used to different ends.

The entities of weaponized protection care for their own
survival before everything else.

They are just like humans.

***THE PROTESTERS CONGREGATE TOWARD
A WHITE STATUE IN THE BACKGROUND
EXPLOSIONS***

Silence and invisibility are the principal currencies of our
utopia. Soon, everything will be a secret.

But what about ourselves? Aren't we silent ourselves?
We haven't said anything in a long time.
We battle.
We throw Molotov cocktails, fight the police, and dance
on the wings of a government airplane.

We look into our phones that look into our lives.
The bare possessions of a nonperson living in a non-place.

A laptop.
A backpack.
A night with friends.
An on-and-off relationship.
A temporary job.
A trove of secrets.

We have a non-plan.
All we do is show that we still exist.

*POLICE ON STREET ALONGSIDE GRANDE
BRETAGNE HOTEL, ATHENS*

We are the opposite of blind. We have absolutely nothing
left but our vision.

*CUT TO TELEPRESENCE MEETING,
CORPORATE VIDEO*

Economies liquified.
It seemed as if their material basis dissolved.
Wealth became an airplane routed around the world.
Value became a global architecture of tax havens and
hedge funds.
The name of the perpetrator of this crime is technology,
in the hands of someone.
Politics and technology together create ideology: that
which seems inevitable.
That which is never followed by a question mark.
That which comes first after the blinking cursor.

CUT TO MOLTEN LAVA

"I."

The internet both disintegrated and rejoined the
structures of daily life.
The borders of the world gave in to shapelessness.
The old world began to loosen its structure and a new
world covered it like a second skin.
A network, a set of nodes that are equal.
A simple fact of life.
A new beginning. A public space.
A secret pocket world.

*CUT TO HORSES IN DESERT,
RUNNING BACKWARD*

Together we fall.
Together we fall deeper.

Nothing is to end our ecstatic conquest.
Undoing all that was said and done before we came.
Unseeing everything with our eyes.

We do not live in the same place.
We weren't introduced.
Please don't send us flowers. Send secrets.

*CUT TO WOMAN ON SHORELINE, WAVING
HER RED HAIR WITH DREADLOCKS AND
SWINGING A JAPANESE SWORD*

Once, governments were proud that they had secrets.
Secrets were the preserve of privilege and glamour.
The modern state claims to believe in transparency and
openness.
This obliges the state to hide the fact that it has secrets.
Imagine what a whistleblower experiences, as she exposes
the previously unseen interior of the state.

*CUT TO CHELSEA MANNING,
EDWARD SNOWDEN*

↓
shapeless
horse
↓
housing
problem
↓
murder

Whistleblowers reveal not the excesses and the crimes of the system, even if what is revealed are plainly crimes.

Whistleblowers expose the system's normal operations; the way it works every day, and the way it agrees with itself in doing so.

As they expose the state's interior, leakers are pathologized by the media as narcissistic egomaniacs, seeking attention for themselves.

Informing the public becomes aiding a foreign power.

The world turns around its axis into playback.

CUT TO DATA CENTER—EXTERIOR

Plato's Cave is now classified.

We shine light on the writings on the wall.

Paranoia is historically cast as the out-of-control frame of mind of a madman dictator.

DATA CENTER—INTERIOR

The pathology of an individual authoritarian, imposing his ferocious will on subjects that must continuously be monitored for secret moves.

But paranoia is infrastructure.

It is logistics.

It is software and hardware.

It is uniformed guards.

It is mouse clicks and coffee mugs.

It is the framed photograph of a spouse.

CUT TO COLLATERAL MURDER DETAIL BAGHDAD APACHE AIRSTRIKE

Paranoia is the systematic and robust application of sheer technological possibility, lubricated by a melting empathy.

So that law indeed gets rewritten by those who oppose it. Law in the hands of those who oppose it is just a piece of paper that says something.

A whistleblower in the eyes of those who oppose it is a mere stand-in-the-way of the inevitable.

A traitor.

Enthusiasm for the drone leads to enthusiasm for the drone that takes decisions.

Pattern recognition and algorithms are replacing ethics.

The capacity of our computers to store everything makes us forget the question of whether anything should be stored at all.

CUT TO IDEAL TRANSPARENT FAMILY

The simplest question becomes the most daring vision.

Paranoia prepares its own terrorist plots, which it then prevents.

In scanning the entire internet for who connects to whom, paranoia sweeps up everyone.

Everyone is a suspect, and everyone is in everyone else's social graph.

The internet's cables are compliant with the infrastructure of paranoia.

COLLATERAL MURDER. CIVILIANS WALKING ON STREET IN CROSSHAIRS

The answer, encryption of all communications, will provoke another backlash.

We will hear that those who encrypt are the terrorists.

Paranoia's answer is always the same:

CUT TO YOUNG WOMAN ON HILLTOP UNDRESSING AS GUY SWEEPS IPHONE

"More."

**CUT TO NSA DATA CENTER UNDER
CONSTRUCTION, BLUFFDALE, UTAH**

No government, and no man indeed, was ever seen voluntarily letting go of a technological possibility that was ready and available to him.

CUT TO IPHONE 5 UNBOXING VIDEO

Computers, handheld devices, and information networks keep us company night and day.
Paranoia wants to survive.
Institutions to protect others become institutions to protect themselves.

**CUT TO CHILDREN OF KIM AND MONA
DOTCOM ON THE BEACH IN PIRATE
T-SHIRTS**

When cracks appear, alternatives to the dominant order can gain strength invisibly until they emerge onto the geopolitical stage with no apparent precedent.

CUT TO GLASSWING BUTTERFLY

There is no transparency without enlightenment.
With the industrial revolution came the glass palaces.
Life without secrets found its form in architecture.
Under transparency the state loses the informational privilege that allows it to maintain itself.
Black transparency is involuntary transparency.

**CUT TO SABRE FENCING
MUSIC: "STREETZ TONIGHT,"
ARAABMUZIK, 2011,
ABRUPTLY CUT OFF AFTER A FEW BARS
FENCING CONTINUES**

There is a curfew.
The statues, squares, and monuments are no longer ours.
They are still as images.
All memory has been seized.
Our message is silence, our rage is mute.

**CUT TO DESERT
THERE ARE BEDOUIN TENTS
AND A SATELLITE DISH**

The idea of cyberspace posed a line of separation between the internet and the real world.
Cyberspace would be a separate universe.
Created by people, enabled by technology, and occupied by information.
Geopolitically, it would be like the sea once was.
An unregulated and fluid space where ordinary rules need not apply.
The internet and life are one.
A hot and dry desert wind.
This is our failed state.
All we do is show that we still exist.

END TITLES, CREDITS, AND SOURCES

for Vesper

**BLACK TRANSPARENCY:
THE RIGHT TO KNOW
IN THE AGE OF MASS SURVEILLANCE**

METAHAVEN

Sternberg Press

**METAHAVEN
BLACK TRANSPARENCY:
THE RIGHT TO KNOW IN THE AGE
OF MASS SURVEILLANCE**

PUBLISHED BY

Sternberg Press

TEXT & DESIGN

Metahaven (Daniel van der Velden,
Vinca Kruk)

EDITOR

Niamh Dunphy

PROOFREADING

Max Bach

PRINTING

Nørhaven

Type set in Times Ten and AG Book.

ISBN 978-3-95679-006-5

Published with the financial support of:
Bureau Europa
Creative Industries Fund NL

Sternberg Press

Caroline Schneider

Karl-Marx-Allee 78

D-10243 Berlin

www.sternberg-press.com

© 2015 Metahaven, Sternberg Press
All rights reserved, including the right
of reproduction in whole or in part in
any form.

AFTER THE BEGINNING

1

COUP DE NET

9

**THERE IS NO ORGANIZATION.
THERE'S ONLY YOU.**

23

OPEN GOVERNMENT GLASS CANDY

53

CAPTIVES OF THE CLOUD

75

ALL TOMORROW'S CLOUDS

115

WHEN PIXELS BECOME TERRITORIES

151

NOTES

ACKNOWLEDGMENTS

INDEX

CREDITS

171

Black transparency is a disclosure of secrets that aims to embarrass and destabilize their keeper. Originally an ethical imperative to blow the whistle on abusive government, it is not insensitive to the allures and spectacles of propaganda.

AFTER THE BEGINNING

MUCH HAS BEEN written about political transparency in recent years. Many authors appear to think that the degree of transparency in a system should be measured purely by the amount of information in it that becomes available to outsiders. How that information is released seems to be less important.

This book expresses the view that *method* is of decisive importance to transparency's political impact. To generalize different ways of achieving transparency—and in doing so unifying their various ends and means—is problematic because in practice different means will always lead to different ends. For example, a political system that complies with strict transparency rules may produce thousands, or even millions of documents to answer requests for information, but often the documents produced will be so severely redacted that no real information can be found in them. This is not transparency. “Open government,” as it is called, offers troves of data as entrepreneurial incentives for citizens, but has no actual effect on the way in which government is structured, carried out, shared, or participated in. This is not transparency. More far-reaching forms of democratic change can be effected when transparency gets involuntarily declared over an organization or entity; this is the uninvited, “black” transparency as practiced by organizations like WikiLeaks. The exposed's frantic responses become part of the revelation, making its consequences harder to regulate and contain. A US military strategist once wrote that “the act of playing the game has a way of changing the rules.” Black transparency can be hard to distinguish from anarchism.

Black transparency can be an instrument of genuine political change, but it can also contribute to a historical record against which to set current events. Yet paramount to most if not all political thought about transparency is the idea that information, once disclosed, can cause some

kind of change in a system. Is transparency an add-on, or plug-in, that makes the existing political system better, or government more effective? Some authors have indeed argued as much. Or is transparency, at its most radical and far-reaching, a means to undercut the very concept of government?

Historically the state has always relied on secrecy, meaning an informational privilege enjoyed by those in power. As a political concept, secrecy is much older than transparency; its black box has survived the advent of modern democracy fully intact. It doesn't really care whether a state is democratic, autocratic, green, red, or shaped like an octopus. Under a cloak of secrecy, the executive branch of government coexists with democracy by providing it with a secure platform. The executive branch is an operating system, and democracy is just one among many applications running on it.

Black transparency is a frontal attack on the autonomy of the executive branch. It introduces a haphazard, imperfect, partial, and dicey form of popular democratic involvement with the permanent state of exception that is maintained to nominally protect national security. This frontal attack is also black transparency's Achilles' heel; it may be a very effective way to cause upheaval, but by the same token its ability to negotiate is permanently at risk.

BLACK KNIGHT TO BLACKPHONE

Black transparency unfolds against a backdrop of unprecedented online surveillance by governments. The idea of an independent cyberspace that exists off-limits to the state's territorial power is deeply rooted in the idealism of the early internet. Yet this notion of independence is no longer an accurate way to address the geopolitical architecture of planetary-scale computation—meaning, the changing physical, sociopolitical, economic, and ultimately geographical shape of the world as it becomes overlaid with digital networks. The resurrection of the state in this emerging political geography is not an isolated

phenomenon that results from technological progress in the capacity to spy; rather, it signifies a structural shift in the governance of democratic societies.

The concept of popular sovereignty—where people govern themselves through mutually agreed yet changeable structures of delegative or direct decision making under a rule of law—is contrary to the idea of a sovereign technocracy in which a class of managers, aided by an expansive executive sector, safeguards the continuity of its own operations. "Public space," necessary to openly establish and collectively change the means and ends of government, is replaced by "public order," which structurally regulates and forcefully limits all actors in their ability to effect any changes at all. The preemptive electronic surveillance of potentially every global subject can be thought of as a way for governments to weaponize themselves against the capacity of every person or group in society to change spontaneously—expanding the state's monopoly on violence into precognitive policing of all thought and action. Black transparency is wound up with a state that wants more control, and gets it easily, as popular compliance to technological standards develops along the lines of convenience, not principles.

Sir Walter Scott's fictional Black Knight kept his visor closed at all times to remain unidentified, encrypting his identity in a pre-internet world. Today, every person's capacity to evade surveillance is determined by their position in a feudal matrix of technological and institutional dependencies. Almost all antidotes to this patronizing system of global surveillance go under shades of black.

For example, the Blackphone is a surveillance-proof smartphone; all of its communications are encrypted by default. Dark Wallet is a completely anonymized payment and storage application for the Bitcoin digital cryptocurrency—itsself an anonymous payment standard. The "darknet" or "dark web" is a term commonly used for a shady internet underworld that sports illicit black markets, its traffic encrypted through proxies and decoys.

→ flexible
→ self-organizing network
→ market regulation
"order"

The darknet, governments argue, must be brought into daylight because it engenders terrorist havens, money-laundering freeports, drug trafficking, illegal arms trade, and other such activities. However, the objective condition of technology exists to provide for such things, just as architecture can shield people from the rain, and a face can be hidden behind a veil. Blackphone and Dark Wallet share an equation of encryption and privacy with darkness. The “black” in black transparency is an aesthetic expression of the secret that comes in defense of the public.

#BLACKLIVESMATTER

Not all reverberations of “black” are accounted for at length in this book. “Black” as in black transparency means, more or less, “in darkness” as opposed to “in the light.” This dialectic is consistent with a centuries-old, religiously inspired equation of openness with light and salvation, and secrecy with darkness and doom. For some, personal responsibility and individual sovereignty are to be finally resolved in a network of anonymity and encryption. However, the network’s capacity to erase assumptions about identity, name, skin color, gender, class, finances, residency, and so on, forms only some imagined flip side to the repressive renaissance of real-life policing.

Beginning in 2014 especially, a string of heinous murders of unarmed black civilians by police in the United States led to large public protests. Some of these murders were related to policing as a source of executive branch income, where excessive fines issued for very small misconducts became, in their compound volume, a financial platform for city government.

#BlackLivesMatter pays tribute to the victims of this structural injustice, where racism is fully reducible to the police’s monopoly on the use of arms, and vice versa, and performs a systemic, hyper-violent erasure of the most fundamental rights in tandem with a perverted logic and practice of economic exploitation. As a movement, one of the #BlackLivesMatter demands is that “the federal

government discontinue its supply of military weaponry and equipment to local law enforcement. [...] It remains essential to monitor the demilitarization processes and the corporate sectors that financially benefit from the sale of military tools to police.”

TRANSPARENT CAMOUFLAGE: DESIGNING FOR WIKILEAKS

The burgeoning national security state found its antidote in WikiLeaks—the trigger that made transparency a pop phenomenon, and made dull principles of accountability suddenly hip and trending.

In the spring of 2010, we felt with passionate hope and optimism that the “antisecrecy” platform could use our design to create a different visual presence for itself in the world. Then, before we could start working, the organization was caught in a whirlwind of celebrity.

The products we subsequently designed became a means for WikiLeaks to raise money during an extra-legal embargo, instigated by financial companies under pressure from US government officials. These products included large, patterned silk scarves, and band-inspired T-shirts. The scarves became an alternate means of visibility and identification: a self-proclaimed *favela chic* in which the see-through and the opaque were merged into transparent camouflage.

WikiLeaks had built for itself a system of “uncensorable” web presences around the globe. With this architecture in place, the organization anticipated that censorship would be its main vulnerability. This assumption proved wrong in the long term.

WikiLeaks’ trajectory—from cyber-utopian political practice to major world power to post-empire downfall—says as much about the organization as about the roller-coaster of changes happening at that time. At the height of its fame, aligned with both the hacktivists from Anonymous and LulzSec and the activists from Occupy Wall Street, WikiLeaks seemed in control of global news

cycles, and hoped that the managerial framework of sovereign technocracy would come tumbling down.

After being accused of spying on the UN, WikiLeaks told then US Secretary of State Hillary Clinton to resign (she didn't). A mere threat to release information on a major American bank sent that bank's stocks down. Every day on the front page, the organization started to behave like a world power, and consequently became a player—some would argue, a pawn—in a battle that resembled a new cold war. Putin's Russia chipped in support for a Julian Assange-led talk show and later offered political asylum to WikiLeaks' heir apparent, the whistleblower Edward Snowden.

By this token black transparency became caught up in a political and media constellation central to contemporary Russia: a hallucinatory machinery of fantasy, fiction, antagonism, and glamour, described by Peter Pomerantsev as a permanent spectacle where “nothing is true and everything is possible.”

Where authoritarianism is ostentatiously present, state violence and secrecy are self-evident. As a result, black transparency's fundamental critique of the state no longer applies. That critique is that modern government spends a good deal of its time pretending to be transparent, hiding the fact that it has secrets—the same ones that black transparency reveals. Symbolically, black transparency meets its end in Russia. The internet-based mythmaking machine of contemporary Russian geopolitics presents propaganda as a complex labyrinth, seemingly satisfying our human need for drama, intrigue, and fantasy in full awareness of the deep cynicism that people feel about government. While other truth-seeking organizations in the public interest take over the mission of fact-finding—black transparency becomes trapped in its own subversion. In doing so it doesn't need to transform itself or betray its principles. It already had the pop. And the Black Knight was a fictional character after all.

OPACITY

On February 25, 2014, WikiLeaks™ announced that it will protect and enforce exclusive rights to its global brand through an Icelandic company named WikiLicense. WikiLicense is to produce WikiLeaks- and Assange-themed merchandise after market research has shown that these names have positive connotations for audiences in large parts of the non-Western world. Set to develop products, including underwear, WikiLicense is to use Assange and WikiLeaks in the same manner as the face of Che Guevara—as branded icons of resistance. But while the late Che's likeness and name are free for everyone to use, WikiLicense controls Assange's. Its paywall between the “licensed” and the “fake” runs counter to the ideas that once gave rise to WikiLeaks.

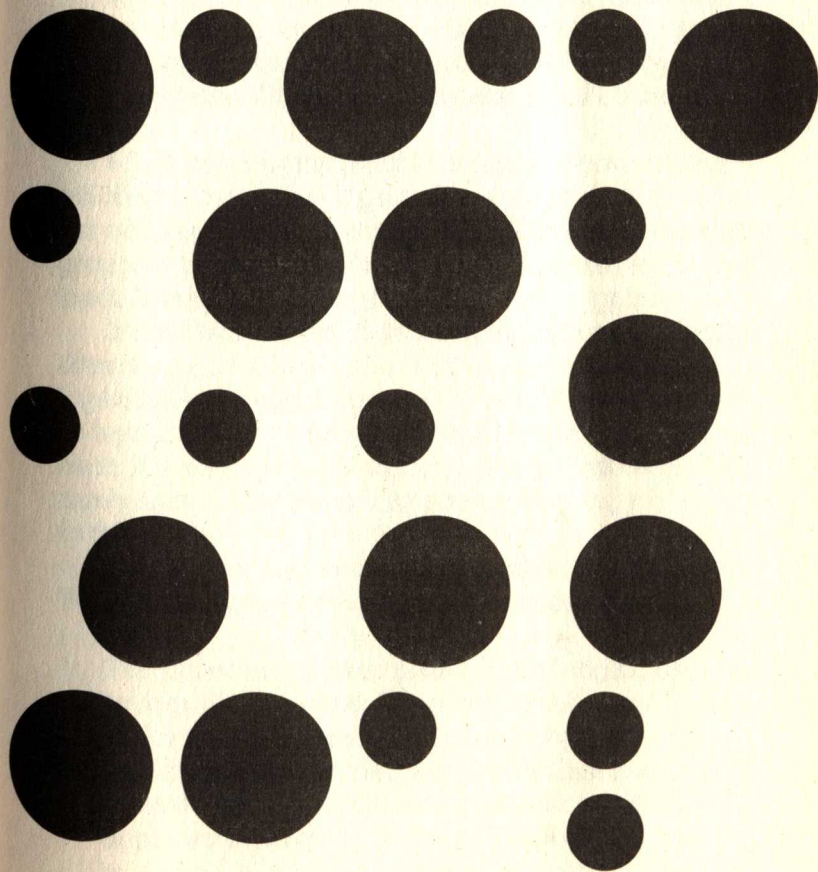
This book is a tribute to the broken glass of the transparency movement. A mere glance at the world today immediately reveals that the transparency we have is partial and unevenly distributed. Sure, the walls of the United States' national security complex are now perforated. But other major powers in the world do not show similar signs of internal destabilization by black transparency. If there are changes, the public will likely play little role in it. The job will be done effectively and quietly behind closed doors.

For all the advocacy for transparency, the world in general never appeared as opaque as now. The most dynamic forces in the world—be they financial, religious, military, or logistic—don't subscribe to a commonly agreed rule of transparency as we know it, changing the rules as part of their game. We seem to be able to have sunshine, yet only incidentally, as part of a quickly changing climate. And that sunshine, like any light, casts its own shadows. In a cloud of data, in the fog of war, we are farther away than ever from the glass cities that promised life without secrets.

Note: References mentioned in this introduction are documented and sourced in the essays that compose this book. The trope of “public space” versus “public order” is explored in the work of the philosopher Nina Power.

secret
ice
head
permeable
transparency
→ Pomerantsev
E 2014
Fluorid
transparency

COUP DE NET



A search for WikiLeaks' single, yet significant, contribution to graphic design: a Surrealist drawing of inadvertent world fame, conceived by an almost completely unknown designer.

THE WIKILEAKS LOGO is a mysterious icon that inserts a good dose of Surrealism into the dull visual brand of contemporary transparency. When we first saw it, it filled us with a mixture of admiration and nausea. A world in the top half of the hourglass melts, like a candle, into another world in the lower half. The continents are visible, and the base of the hourglass contains the word WikiLeaks, typeset in Times New Roman (and sometimes Garamond).

The logo is otherworldly and sinister, but also clumsy and weird. There seems to be a tacit connection between the melting globes in the hourglass and the melting clocks from Salvador Dalí's 1931 painting *The Persistence of Memory*.

While professional graphic designers now sometimes tell clients to avoid having a stable, permanent logo to begin with (and we tried as much with WikiLeaks when we proposed to design for them), the WikiLeaks mark that made history was aiming for the complete opposite.

It tried to squeeze more meaning into an hourglass than any logo could possibly contain. The use of globes in logos is, of course, far from new. But in many cases a world-as-logo is merely a ping-pong ball with graphic shapes on it; it is rarely implied through design, and even more rarely shown, that something strange is going to happen to this world.

Nicolás Mendoza, a media researcher, referred to the WikiLeaks logo as a *coup de net*.¹ Mendoza wrote:

The upper and darker planet is exchanged, drip by drip, for a new one. The power of the image lies in the sense of inexorability it conveys, alluding to earthly absolutes like the flow of time and the force of gravity: a bullish threat that grants the upper world no room for hope. The logo narrates a gradual apocalypse, and by articulating this process of transformation through the image of the leak, WikiLeaks defines itself as the

critical agent in the destruction of the old and the becoming of the new world.²

In November 2011, the organization commented on Mendoza's writing in a tweet: "Finally some gets the WikiLeaks logo."³

Right up until the release of *Collateral Murder* on April 5, 2010, the only press image WikiLeaks offered journalists was the logo.

Who designed it? Asking WikiLeaks directly for this information felt wrong, for a number of reasons. One was that confidentiality and anonymity are strong presumptions in political activism. It's not like going around and asking people for their full names and dates of birth. It also seemed that many people before us had entered into relationships with WikiLeaks with the sole purpose of extracting all kinds of information from it. We did not want to do this. Unless WikiLeaks would voluntarily discuss the logo with us—which they never did other than by saying they treasured it—we decided we wouldn't ask. Besides, it felt more interesting to try and find the designer ourselves, using the internet, which we surmised was hiding the secret of its maker somewhere. No one had taken credit for it. But there were others who were wondering about the logo's origins too.

In 2011, the Bulgarian designer Margarit Ralev wrote a blog post titled "Some Thoughts on the WikiLeaks Logo Design." He posted an intriguing 1963 print advertisement for Braniff International Airways. Braniff was once a prominent US airline, which ceased operations in 1982. In the ad, North and South America were enclosed in an hourglass. Obviously, the hourglass had no implications of deep geopolitical change but suggested that faraway destinations became more accessible for the US traveler. Although the Braniff ad showed that the idea of a territory or continent visually contained in an hourglass was not new, it proved nothing further in regard to the WikiLeaks hourglass.

While Ralev acknowledged that the similarity was probably a coincidence, he surmised that the origin of the WikiLeaks logo was likely to be Europe because that continent was most visible and central on the upper globe.⁴ This musing on Ralev's behalf—one that struck us as almost certainly mistaken—triggered a crucial response. On October 8, 2012, a user named Heronimus added a comment to Ralev's article:

The origin is Australia. Perth to be precise. My friend and artistic collaborator designed it. She went to Uni with Assange in Canberra—and he asked her to make it. So your speculations are for the most part incorrect.⁵

Julian Assange studied physics in Australia at the University of Melbourne and at the University of Canberra between 2002 and 2005. Maybe Heronimus thought he'd been sparse enough with information, but there were plenty of clues here. We were quite sure we could locate the designer.

"PACIFIC PHYSICIST AND ILLUSTRATOR"

In January 2007, the New York-based website Cryptome leaked a set of e-mails exchanged at the time of WikiLeaks' foundation. Some of the (anonymized) messages were about logo design. There was discussion about the hourglass and about an illustration of a mole, which was to be reworked into a "logo-sized icon." On December 9, 2006, the unknown designer of both proposals wrote:

OK, so here are some further modifications: First of all I changed the font on the 2 logos so whatever one you decide to go with, I think this is better. (I am guessing you'll decide amongst yourselves what logo is appropriate.) As to the mole: I disagree about several things. The dark

figures are now looking beyond/above the mole but they should NOT look at one another, as I want no bonding or feeling of togetherness about them. Moles have noses like little hearts (which makes them so cute), whilst seals don't really have a separate nose (it blends in with the skin). I tried a quick change with a drill but I don't like it. Also added a version with a darker mole background, but that takes away from the picture, and I think your eye is no longer drawn to the center. Anyway, I will try to shrink the mole into some kind of logo sized icon over the next few days. Bit busy, cause of Christmas coming up but shall do my best. Hope this is acceptable. Battle on!⁶

An e-mail that WikiLeaks sent to Pentagon Papers whistleblower Daniel Ellsberg that same day included a list of the organization's initial members:

- 1) Retired new york architect and notorious intelligence leak facilitator
- 2) Euro cryptographer/programmer
- 3) Pacific physicist and illustrator
- 4) A pacific author and economic policy lecturer
- 5) Euro, Ex-Cambridge mathematician/ cryptographer/programmer
- 6) Euro businessman and security specialist/ activist
- 7) Author of software that runs 40% of the world's websites
- 8) US pure mathematician with criminal law background
- 9) An infamous US ex-hacker
- 10) Pacific cryptographer/physicist and activist
- 11) US/euro cryptographer and activist/ programmer
- 12) Pacific programmer
- 13) Pacific architect/foreign policy wonk⁷

The third person listed—the “Pacific physicist and illustrator”—seemed the most promising lead. Heronimous claimed that the logo's designer was his female friend and Assange's fellow student. Assange studied physics. But then, who might Heronimous be?

A Google search eventually led to the Facebook page of a certain Heronimous Wang (Hieronymous Wang). An Australian comics wiki website described Heronimous Wang as a “Perth based writer/artist. One half of Ask Dr Wang Productions with Aśka.” Aśka, then, was a “Perth based graphic artist, illustrator and metal head. One half of Ask Dr Wang Productions with Heronimous Wang.”

Their MySpace page has not been updated for years. Topping the friend list is Aśka, whose page links to a portfolio on the DeviantArt network. Indeed the duo's works are scattered across mid-2000s web platforms in various states of disarray. Some of the pages mentioned above have already ceased to exist, and more will.

AŚKA

Aśka sometimes uses the nickname SuperAska. Her bio line reads: “Physics is my Mistress, Art my Mother and Road is my Teacher. Welcome to my world ...” One of her drawings titled *Drunken Manoeuvres*—and dated 2006—depicts a woman with closed eyes throwing the contents of a glass of red wine horizontally into a c-shaped arch so that the splashes and drops reach her closed mouth. The drops look somewhat similar to the leaks in the WikiLeaks hourglass. Most of Aśka's drawings are signed with a signature of her name in the style of a metal-band logo.

On January 28, 2009, Assange announced on the WikiLeaks website the release of “thousands of pages of active insurgency and counterinsurgency doctrine from the US, UK and Indian military.”⁸ The article was accompanied by an illustration attributed to the organization's “cartoonist Aska Doliniska.” The signature at the bottom of the cartoon was exactly the same as the

signature on Aśka's portfolio images, all done in that same heavy-metal style.

We were now certain about the link between Heronimus and Aśka. We were sure that the same Aśka had also worked with WikiLeaks. Only, we hadn't seen anything that looked like the logo in her artwork.

WikiLeaks wasn't mentioned on any of Aśka's on-line portfolios, profiles, or web pages—a remarkable absence given that the logo would be her most famous and widespread work. The closest visual parallel we could find was a 2005 drawing titled *Expired*, which depicts a depressed-looking girl sitting between concert tickets in an aquarium of blue-green hues, similar to the colors of the hourglass. As mysteriously pointless and depressing as the drawing might seem, it brought us closer to the conclusion that Aśka was the person we were looking for.

Aśka didn't seem to make any explicit political or ethical suggestions. Everything political in her work seemed implicit, with an undercurrent of anger and grunge running through it. But that anger seemed as unspecific as a jeans ad about revolution.

However, we found her 2011 video animation adaptation of Guy Debord's *Society of the Spectacle*, posted on YouTube by the user "Azorek79," to contain a crucial bit of information. The video includes a quote by Marshall McLuhan: "All media work us over completely. They are so pervasive in their personal, political, economic, aesthetic, psychological, moral, ethical, and social consequences that they leave no part of us untouched, unaffected, unaltered."

The instance McLuhan's voice says "ethical," the video frame shows a portrait of Assange. Flashing by almost imperceptibly fast, Assange's appearance made us certain that Aśka designed the hourglass. We e-mailed her and requested a short interview.

After a few days, her answer arrived:

Well, I must say it's quite a surprise to hear from anyone regarding the logo. Thanks for your interest and the leads—it's curious to see what people have written about it. What exactly do you mean by an interview? An informal talk with you, in relation to your redevelopment of WikiLeaks branding and such? I am attaching the images for the WikiLeaks logos/images in chronological order to this email. That is really all there ever was.

We spoke with Aška via e-mail. We did not explore her personal background and also withheld her last name on her request.

HOW DID YOUR INVOLVEMENT WITH WIKILEAKS COME ABOUT?

I don't usually design logos, but when friends ask me to, I never refuse. This case was no different. If I remember correctly, a phone number with an African area code called my mobile, and it turned out to be Julian. He wanted me to create some graphics for his ready-to-launch project—more specifically he was after some visuals which people could connect with on, as he put it, “an emotional level.”

HOW DID THE IDEA FOR THE HOURGLASS EMERGE?

I made the logo in 2006, so it's hard for me to remember what I was thinking about at the time I made it. I'm sure it would have been a completely intuitive response to the brief. I can see from my sketches that it was pretty much one of the first things that came to my mind. I was very interested in the idea of transformation that Julian's website was aiming to achieve.

Changing the world may seem like a romantic notion, but it's also exactly what needs to happen for each new generation to supersede the old. So I guess the hourglass is exactly that—a transformation in time. And the best thing about it is that once the last drop falls, you can turn it around and start again.

HOW DID THE SKETCHING AND DECISION MAKING PROCEED TOWARD THE FINAL LOGO?

Julian picked the hourglass sketch from the first few proposals I sent. I followed that with the vector version and apart from the font I don't think anything was altered.

There was an alternative line of thought though. It showed a wall from which bricks were being removed, with looming shadowy figures up above. Soon, however, the idea became really complicated, and included moles and drills. After some back and forth fun, it got scrapped.

WHAT ARE YOUR THOUGHTS ABOUT WHAT HAPPENED SINCE? WIKILEAKS IS NOW EXTREMELY VISIBLE AND WELL KNOWN. DID YOU EXPECT THIS TO HAPPEN?

Yes and no is the short answer. The little I know about Julian is that he is very serious about his undertakings. If he wants to set up a website which uncovers world injustice and government conspiracies then he'll do it. And at that point he already had all the drive, skills, and facilities needed to do that. But of course it was impossible for me to know what that change will feel like before it actually happened. And yeah, it feels ... BIG.

ARE YOU STILL INVOLVED WITH WIKILEAKS, OR DO YOU STILL FEEL RELATED TO WHAT IT IS DOING?

I never felt that I was personally connected to WikiLeaks.

I don't believe a logo has that much bearing at its conception, which is the only stage at which I was ever part of the process. In the end, any image connected with the WikiLeaks' achievements, impact on the world and the monumental work and sacrifice of Julian and the WikiLeaks team, would gain some kind of value, and this is irrespective of the image itself.

Their logo—"the icon"—already has meaning ascribed to it by others—the organization itself, the

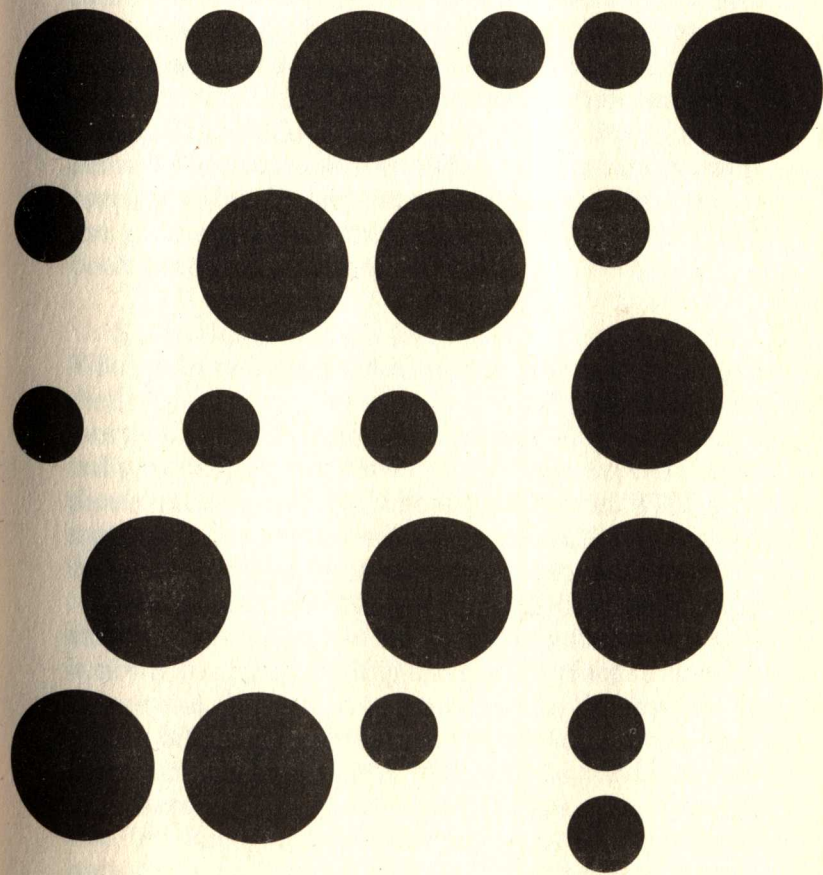
supporters, the media and the aggressors. None of this is connected to me, except incidentally. I am immensely proud of WikiLeaks, but not because I had anything to do with it, but more so on the level of a person eager to see a less hypocritical, a more free and open future on the horizon.

THANK YOU.

The WikiLeaks logo is an important image of political activism in the global age (even though that sounds pretentious having just read a designer's explanation on how it came about).

Its initial strategy of dissemination was critical; it was the organization's only press image. This artificially created visual scarcity helped the mark to become disproportionately well known. The maker doesn't want to be credited. She is a ghostwriter. As someone commented on Facebook: "Whoever invented it, it's history."¹⁰

**THERE IS NO ORGANIZATION.
THERE'S ONLY YOU.**



Hyper-individualism, chaos theory, anarcho-libertarianism, and opportunism coexist non-peacefully in the pop-cultural biosphere of WikiLeaks—the world's first nongovernmental organization dedicated to uninvited, radical transparency. Knowledge is power. Transparency is absolute power. We know the rest.

WIKILEAKS LED TRANSPARENCY into the twenty-first century. It has kicked the door wide open. It has felt the impact of the geopolitical currents that first carried it—then ravaged it. It has been overanalyzed as a curious pathology of resistance against the inevitable, or as an illegitimate deviation from the protocols of open government, or simply, as an ego show.

WikiLeaks has been called a terrorist organization. It has been accused of killing innocent people. We've heard that it put the lives of diplomats, civilians, and military personnel at risk, and that it has hurt the interests of governments and corporations. It has been threatened, cyber-attacked, infiltrated, denounced, boycotted, and exiled. Disorganized and chaotic, WikiLeaks has still defined what we think about when we think about transparency today. It has almost single-handedly created the phenomenon of "black transparency," which this book intends to describe.

STRANGER THAN FICTION

WikiLeaks was geopolitical design: a stateless, faceless shell of an organization built around a drop box to which everyone can post documents. The possibility for relatively ordinary people to conceive of something like WikiLeaks should make us aware of the possibilities ahead. WikiLeaks may be just one out of a series of geopolitical interventions designed to unravel the nature of power today.

Our present reality, when revealed in full, looks stranger than fiction. Our unfolding "speculative present" is slowly but surely putting itself in the place of fiction's former role. (In Don DeLillo's novel *Mao II* the reclusive author Bill Gray believes that terrorism has taken over literature's ability to cause what he calls "raids on consciousness." Gray says, "What terrorists gain, novelists lose.")¹ Indeed, the facts emerging under black transparency are so many and so rich that science-fiction authors ought to fear a coming unemployment; whistleblowers are the ghostwriters of the future. Like anarchism (as

described in the words of the sociologist David Graeber), WikiLeaks feels “less about seizing state power than about exposing, delegitimizing and dismantling mechanisms of rule while winning ever-larger spaces of autonomy from it.”²

WikiLeaks offers no solutions other than exposing more documents. It is the amplifier of the whistleblower’s whispering voice. It has no grand scheme for what should be done, or how we should govern once its revelations have been outed and once the world is in even greater turmoil. This is not your typical nongovernmental organization (NGO) with annual reports, or a public-relations department like a corporate newsroom. It is an antiorganization, a hyperbolic catalyst wielding information as power.

I CASCADES

The saying goes that a butterfly’s wings flapping in Brazil can set off a tornado in Texas. This compelling idea—the subject of a famous 1972 talk by the American mathematician and meteorologist Edward Lorenz—captures the essence of chaos theory: the disproportionate effect a tiny change inside a system can have on the whole.

What Lorenz called a “butterfly effect” also applies to information. At first, a novel piece of information may be circulated intensely in a small network until it “breaks out” and starts infecting neighboring networks, spreading like a disease. Such an occurrence is called an “information cascade.” The network scientist Duncan Watts notes that “cascades of smaller sizes happen all the time. [...] Every shock, in fact, triggers a cascade of some size, even if just the lonely innovator himself. But only global cascades grow in a truly self-perpetuating manner, thus altering the state of entire systems.”³

WikiLeaks was designed to be the butterfly, the amplifier for the unheard voice, the catalyst of the avalanche, the

spreader of the disease. It believes in the idea that information alone can bring powerful shocks, and cause systems to change.⁴

KNITWAR

On June 21, 2010, WikiLeaks founder Julian Assange made a rare public appearance before a European Parliament working group on freedom of expression in Brussels. He was wearing a knit sweater—possibly of Icelandic make. WikiLeaks appeared as an alien at a conference where everyone wore suits and ties. Assange was at once deeply embedded in the involuntary governmental and corporate transparency it championed, while at the same time careless about the visual and political conventions normally respected by his targets.

Prior to WikiLeaks, the geopolitical impact of the internet was often contained and superseded by official political channels. The 2003 invasion of Iraq is a case in point. Fabricated evidence was successfully deployed to bring countries to war with one another without reason, but with great strategic stakes involved for the warmongers.

A subsequent leak of pictures from the Abu Ghraib prison in 2004 affirmed the worst expectations. The leak paid testimony to the omnipresence of records: digital images taken with digital cameras and shared via digital networks. The Abu Ghraib images slipped through the physical and digital walls of the organization that made them, as, some would argue, information is naturally inclined to do. The 2008 US election of Barack Obama was greeted by millions as a break with the Bush administration’s violations of justice, civil liberties, and its abrasive military policies. Obama’s victory was seen as a triumph of internet-driven horizontal democracy over neoconservative war porn. But soon after Obama became president, the participation was over and it became clear that the old habits were to continue unabated. They were part of the system.

states information as freedom embedded by the prevalence of their nature

local global public

NETWORKS AND STREETS

WikiLeaks uses transparency to disrupt the management and control of reality itself. In 2006 Assange wrote a short essay, "Conspiracy as Governance," which argued that power's ability to conspire and organize is destroyed when its communications get exposed and every possibility to coordinate is reduced to zero.⁵ Alternatively, conspiracy can be understood as a form of management. Under an umbrella as seemingly neutral as management, it's much less likely that conspirators will even consider themselves plotters of a particular political outcome. They are basically involved in a kind of maintenance of the status quo; they are no more than caretakers of the structure that takes decisions for them. The term "reality management," coined by the British writer Mark Fisher, describes this status quo as an implicit agreement shared by the political class, the (mainstream) media, and the corporate sector. It is aimed at changing nothing.⁶ As this management also involves limits on the circulation of information and its interpretation, information cascades have the capacity to disrupt it.

As the essayist and filmmaker Hito Steyerl writes: "Remember the Romanian uprising in 1989, when protesters invaded TV studios to make history? At that moment, images changed their function. Broadcasts from occupied TV studios became active catalysts of events—not records or documents. Since then it has become clear that images are not objective or subjective renditions of a preexisting condition, or merely treacherous appearances. They are rather nodes of energy and matter that migrate across different supports, shaping and affecting people, landscapes, politics, and social systems."

WikiLeaks' transformative intervention into the constellation of interests between governments, corporations, and media organizations is of lasting importance—the internet being its platform of choice, with its propensity to spill over into neighboring realities. Steyerl contends:

Data, sounds, and images are now routinely transitioning beyond screens into a different state of matter. They surpass the boundaries of data channels and manifest materially. They incarnate as riots or products, as lens flares, high-rises, or pixelated tanks. Images become unplugged and unhinged and start crowding off-screen space. They invade cities, transforming spaces into sites, and reality into reality. They materialize as junkspace, military invasion, and botched plastic surgery. They spread through and beyond networks, they contract and expand, they stall and stumble, they vie, they vile, they wow and woo.⁷

The sweater worn by Assange is consistent with the transitioning capacity of images. It is a clash of codes. The suits and ties worn by every male official on the planet are a formal means to make reality seem under control. Assange's Icelandic sweater tacitly unlinks his or any appearance from the management of reality: *The importance of what we publish is paramount and speaks for itself. What I am wearing does not affect the code. I could be wearing something else, or nothing at all.*

Just as a Google image search may link seemingly unrelated and possibly trivial artifacts into a compelling visual trope, the sweater links WikiLeaks with modesty and warmth. WikiLeaks is the quintessential political tool of the internet, harnessing heroic intervention, grand geopolitical gestures, and fashionable sloppiness.

All at once.

II ORGANIZATION

In the fall of 2006, originally under the name of w-i-k-i-l-e-a-k-s--o-r-g or simply WL, WikiLeaks was established through a discussion among a group of people on a private mailing list. There were at least thirteen participants.

Assange, known as "Julien," was the most active voice. He asked John Young—a New York architect running the online document archive Cryptome—to volunteer as keeper of WikiLeaks' .org domain. After doing so initially, Young became highly critical of the project. He wrote: "Announcing a \$5 million fund-raising goal by July will kill this effort. It makes WL appear to be a Wall Street scam. This amount could not be needed so soon except for suspect purposes. Soros will kick you out of the office with such over-reaching. Foundations are flooded with big talkers making big requests flaunting famous names and promising spectacular results." Young told Assange that he was going to publish the mailing-list exchanges on Cryptome. Assange asked him not to. Young published them on January 9, 2007.

In December of the previous year, WikiLeaks had already settled on its aqua-colored hourglass logo. In January, as the organization's fame was soaring, someone e-mailed: "The wl.org front page + blurb is seeing many, many quotes and reposts (including of the logo)." The hourglass was the only image used by WikiLeaks for its communication with the press and it would stay like this for the next few years. Its story sounded almost too good to be true. WikiLeaks was founded by "Chinese dissidents, mathematicians and startup company technologists, from the US, Taiwan, Europe, Australia and South Africa"—a sentence that was literally copied or closely paraphrased by almost all newspapers and media reporting on it in 2007.⁸ And the statement continued: "Our advisory board, which is still forming, includes representatives from expatriate Russian and Tibetan refugee communities, reporters, a former US intelligence analyst and cryptographers."

No one has ever seen such a thriving community of huggable liberal pandas and ethical wildcards. In an e-mail to Pentagon Papers whistleblower Daniel Ellsberg, Assange asked for the world's most famous leaker to be part of the organization's "political armor." He surmised: "The more armor we have, particularly in the form of men

and women sanctified by age, history and class, the more we can act like brazen young men and get away with it."

Various political and communicative strategies were debated in that early e-mail exchange. With avid foresight, someone wrote, "Our primary targets are those highly oppressive regimes in China, Russia and Central Eurasia, but we also expect to be of assistance to those in the west who wish to reveal illegal or immoral behavior in their own governments and corporations."

Deceptive, joke-like hyperbole is political armor, more so than a wide-eyed belief in open government. WikiLeaks was designed to confront all government with itself; and to confront liberal democracy with its hypocrisy.

Assange wrote, with cunning:

creation of lexicon

We should be consistent in our use and invention of language. A word or a phrase extracts meaning from its resonance with other usages and our experiences. For instance in the FAQ we sometimes use the phrase "ethical leaking." Should we always use this phrase? "Leak" by itself carries a negative. "Ethical" a strong positive. "Ethical leaking" a positive. But it does isolate "leaks" as being non-ethical unless we stick "ethical" on them. Can we make a movement from this phrase and others? "The ethical leaking movement." Powerful. Can it survive the heat of our vision?

We must find our own "Operation Iraqi Freedom's" blessings and sanctifications that even our most diseased and demonic opponents will find themselves chanting to each other in the night. We need phrases for "leak facilitator," "mail drop volunteer," "ethical leaker," "WL server operator" etc, etc.⁹

THERE IS NO AUTHORITY BUT YOURSELF
It's 2013. In *The Fifth Estate*, a DreamWorks feature film about WikiLeaks, Daniel Brühl shouts to

Benedict Cumberbatch: "There is no organization. There's only you."

Brühl's character is Daniel Domscheit-Berg, a former spokesperson known for his disagreements with Assange. Cumberbatch plays Assange. While intended as a striking *j'accuse* at his interlocutor's oversized ego, Brühl's phrase instead reads like a surprisingly apt interpretation of the current state of human affairs: that all resistance seems atomized to the level of the individual; that traditional political association has ceased to be an effective counterpower. In its 1983 song "Yes Sir, I Will," the radical British punk band Crass stated: "You must learn to live with your own conscience, your own morality, your own decision, your own self. You alone can do it. There is no authority but yourself." Brühl's exclamation updates Crass's lyrics.

In *Here Comes Everybody: The Power of Organizing without Organizations*, the internet guru Clay Shirky argues that we indeed no longer need organizations to get organized. Shirky's argument is that the internet now offers what traditional structures can no longer provide: targeted and efficient action, at close to zero cost for the users, without the need for salaries and pension plans to pay the organizers. However, in many of Shirky's accounts, the potential of the internet to do this leads to the amplification of already existing power relations. The example that leads the way is that of a young white woman in New York City who accidentally forgets her cell phone in a taxi in 2006. The woman, Ivanna, discovers that her phone has ended up "in the hands of a girl in Queens." After some rowdy e-mails back and forth, the phone's new proprietor, Sasha, threatens that she and her boyfriend will hit Evan, Ivanna's fiancé, with the phone if he comes to fetch it. Evan "declined to go, both because he assumed [Sasha's address] was fake (it was) and because of the threatened violence."¹⁰ Instead of confronting Ivanna, he makes a web page where he tells his friends about the story. True magic starts happening: "Evan's friends and their friends forwarded it around the internet, attracting a growing amount of atten-

tion." Then, "Evan's story appeared on Digg. [...] Evan was getting ten emails a minute from people asking about the phone."¹¹ The NYPD got involved, and the story scaled and scaled. At its apotheosis, writes Shirky, "15 members of the NYPD arrested Sasha, a sixteen-year-old from Corona, New York, and recovered the stolen [phone], which they returned to its original owner, Ivanna."¹²

Shirky claims that "one of the themes running through the story is the power of group action, given the right tools."¹³ What though is this really saying? It says that Hispanic teenagers "from Queens" can now be arrested by SWAT teams thanks to the internet. Evan's decision to avoid a head-on confrontation with the thieves and to instead "take the story to the internet" can easily be seen as a consequence of class inequality. The message to Sasha is: the internet will tarnish your name forever and you will be arrested, and I don't even need to mess with you physically to achieve this. Shirky's *Here Comes Everybody* is a bible of atomization, especially when seen through the eyes of the actual victim: Sasha.

We acknowledge that stealing phones is wrong, and it is unfortunate to lose them in cabs, but in this case it is merely punishment that gets scaled. Mass hysteria unfolding around a stolen phone may seem like a butterfly effect, but doesn't lead to any change in the system.

The consequences for Sasha were grave. The *New York Times* and many other news media published her full name—not because of her offence but because of the attention it drew.¹⁴ There was also an age gap: Sasha was sixteen, Evan almost twice her age. He was much more computer savvy than she, and indeed, could use his skills to paint "a bad picture of her for the whole world to see."¹⁵ Parts of *Here Comes Everybody* appear to herald social participation, but on the condition that existing relations of class, power, and gender remain as they were.¹⁶ To be fair, other parts of the book sing the praises of collaborative efforts like Wikipedia. Shirky also explains the concept of information cascades, using 1989 citizen protests

in the city of Leipzig in the German Democratic Republic as an example. He says that these led to a state where the corruption of the regime became common knowledge: "Finally the people in Leipzig could see others acting on the knowledge that the GDR was rotten. [...] This shared awareness is the step necessary for real public action: when the people in the streets of Leipzig knew the same thing as the people watching from their windows."¹⁷

Organization has become the thinnest of membranes—almost an illusion. It no longer provides for future, income, or jobs. Relationships between people and their employers are becoming increasingly temporary and precarious; organization becomes driftwood, floating debris in a sea of insecurity.

Information technologies—including the internet—are permeating the digital walls of organizations. This happens by design, by cyber war, by leaks, and by accident. The infamous Stuxnet trojan virus, for example, was released as early as 2009 and was created by the United States and Israel to target Iran. It spread over the internet. In 2010 it reached the computer that controlled an Iranian nuclear reactor—precisely the one that it was designed to find and sabotage. The last leg of the route—from the network to the reactor's control software—was likely traversed by USB key.

Anonymous and LulzSec hacktivists became specialists at breaking into corporate databases. In 2011, members of Anonymous who posed as employees of the US government defense contractor HBGary Federal, hacked one e-mail address and obtained the password of the entire company's e-mail database from the systems administrator.

The increasingly permeable borders of organizations and the temporary nature of their relationships with employees have added to the power of whistleblowing. Indeed, one striking aspect of the story of Edward Snowden and the enormous information leak he facilitated out of the secretive vaults of the United States' National Security

Agency (NSA), was that Snowden himself was a sort of freelancer, a temporary subcontractor who had no permanent affiliation with the agency; a well-paid information mercenary under neoliberal flex work, whose loyalty to the secrets of imperial policy was safeguarded by lie-detector tests and paychecks.

III CHAOS

In 1992, the American diplomat Steven Mann published an article called "Chaos Theory and Strategic Thought." Mann hoped to inspire US foreign and military policy to learn from chaos. Around the same time, researchers at IBM were busy studying the behavior of sand piles. They added individual grains of sand to a pile to see how many it would take before an avalanche emerged and the pile would collapse, thus seeking to find the magical catalyst—the tiny change causing the disproportional systemic shift. Mann asserted: "On a grand scale, the increasing complexity of foreign affairs cuts against the comfortable assumptions of classical strategy. Can we indeed describe our exquisitely variable international environment in traditional terms of balance of power, polarity, or a shift of tectonic plates?" Further, he argued: "The closer we come to an honest appreciation of the international environment, the more we must confess that it is nonlinear and frustratingly interactive. This complicates analysis tremendously: Nonlinearity means that the act of playing the game has a way of changing the rules."¹⁸

Around the time that Mann wrote his piece on chaos, the first photograph was posted onto the World Wide Web (apparently by the web's godfather Sir Tim Berners-Lee). The web had been launched the previous year. Mosaic, the first browser, was launched in 1993.

Very soon, other entities began to appear in US strategic thinking, filling in for the chaos theory. In a famous study developed during the 1990s and published in 2001, prior

to the 9/11 attacks, RAND Corporation researchers John Arquilla and David Ronfeldt argued that the United States faced new adversaries engaging in *netwar*, “the lower-intensity, societal-level counterpart to our earlier, mostly military concept of cyberwar. Netwar has a dual nature, like the two-faced Roman god Janus, in that it is composed of conflicts waged, on the one hand, by terrorists, criminals, and ethnonationalist extremists; and by civil-society activists on the other.”¹⁹

Since WikiLeaks began leaking US government documents (for example the “Standard Operating Procedures” of the extrajudicial Guantánamo Bay prison in Cuba), two competing interpretations of its activities have prevailed in the response. In one, WikiLeaks is a civil-society activist group. In the other, it’s a band of terrorists.

Under transparency, either voluntarily or by force, more politically and ethically sensitive information is released into the free flow of information.²⁰ In one possible scenario, people would get to make more informed decisions about those who govern them. As Shirky maintains in a piece on WikiLeaks, “citizens of a functioning democracy must be able to know what the state is saying and doing in our name.”²¹ In that scenario, change, if any at all, happens through the established channels and platforms of politics. But this is not what WikiLeaks is about. WikiLeaks is designed to trigger something more energetic; to set information cascades in motion that can’t be controlled by bureaucracy. As Watts asked, “How is it that small initial shocks can cascade to affect or disrupt large systems that have proven stable with respect to similar disturbances in the past?”²²

WikiLeaks has been a catalyst in revolutionary events in recent years. The most notable example of this is the Arab Spring—a series of popular uprisings that began in 2010 in Tunisia, Egypt, and Libya, and sprawled to Bahrain, Yemen, and Syria. Initiating the lead-up to the uprising in Tunisia, WikiLeaks released classified documents in which American diplomats talked frankly

about President Ben Ali and his entourage, affirming objectively and for the whole world the farcical corruption that everyone already knew about. Other events also contributed to the information cascade. The award-winning blog *Nawaat* created a popular YouTube video showing the Tunisian presidential plane flying to Paris, Milan, and Geneva. The plane’s only passenger was president Ben Ali’s wife on a luxury shopping spree. The actual revolution began when Mohamed Bouazizi, a young Tunisian street vendor, set himself on fire after his business had been seized by the government.²³ In 2011 Amnesty International credited WikiLeaks for setting off the revolution in Tunisia.²⁴

A big part of the cascading potential of a leak is not in the content but in its context—not the scoop, but the spin. WikiLeaks has long mastered the art of maximizing a leak’s impact by accompanying it with sharply written (and spoken) discourse. By flavoring its releases with a brand of invincible courage, all its revelations hinted at revolutions.

As Assange remarked in a 2011 interview with Hans Ulrich Obrist:

My political position is that all political philosophies are bankrupt, because they’re not created with a full understanding of how human institutions actually behave. A better question would be: Do I have a political temperament? And I do have a political temperament, which is a combination of libertarianism and the importance of understanding. And what emerges from this temperament is holding power to account through action driven by understanding.²⁵

That political temperament had already reached its zenith with the April 5, 2010, release of a video that WikiLeaks had obtained from Chelsea Manning. The video was recorded through the onboard camera of a US Apache attack helicopter on a mission over New Baghdad in 2007. It

showed civilians, including two Reuters journalists, Saeed Chmagh and Namir Noor-Eldeen, being ruthlessly gunned down by the Apache aircrew. A van that had stopped to aid the wounded was completely blown up, and its driver killed. The children in the van, on their way to school, barely survived the carnage.

WikiLeaks edited and subtitled the video and named it *Collateral Murder*. Its grainy images have traveled the world over and have become symbols of black transparency—the truths that are hidden under the cloak of state secrecy. Consequently WikiLeaks exposed documents about the wars in Afghanistan and Iraq. Widely documented wars, however, have little to no information available to the public about their real consequences and cost, including vast amounts of civilian deaths. By giving the public access to the secret war logs, WikiLeaks enabled everyone to see the facts of imperial policy, rather than public diplomacy and propaganda. This batch of documents culminated in the release of a massive trove of diplomatic messages known as “Cablegate.”

The United States hasn't directly censored WikiLeaks or its partner outlets, but has prosecuted and convicted Manning, and set up a grand jury in anticipation of doing the same with WikiLeaks. The US administration has also been indirectly responsible for an extrajudicial financial embargo against the whistleblower site, carried out by credit-card companies and banks.

IV TRAPPED

WikiLeaks emerged from countries around the Pacific. Its roots were in nomadism, backpacking, couch surfing, statelessness—a group plotted around an ocean, not a continent.

It also had a keen interest in Africa. Some of its earliest releases focused on Somalia, Kenya, and Ivory Coast. One question remaining is if the physical sanctuary of

an African “failed state” would have helped WikiLeaks to stay ahead of its foes. The answer is that, as Steven Mann would have said, the game had changed by playing it. WikiLeaks sought safe havens, but also credibility and infrastructure.

In 2009 and 2010, WikiLeaks became more reliant on European institutions. And nominally at least, Europe loved WikiLeaks in return. The European Parliament's Alliance of Liberals and Democrats (ALDE) invited Assange to its special session on freedom of expression in Brussels (the one where he wore the sweater). The annual Chaos Computer Congress in Berlin was WikiLeaks' home base. Wau Holland, a foundation that handles the organization's finances, is based in Germany. And there is a special connection between WikiLeaks and some of the Nordic countries—Norway, Iceland, and Sweden. Assange appeared at the Oslo Freedom Forum in 2010. *Collateral Murder* was decrypted, edited, and produced in Iceland. WikiLeaks had its data hosted in at least two server locations in Sweden: at the bulletproof hosting firm PRQ and at the boutique James Bond-style Bahnhof data center in central Stockholm. Both hosting companies have ties with the Pirate Bay and the Swedish Pirate Party.

WikiLeaks favored Sweden initially because of its laws on freedom of speech, which were good for hosting data. But this does not mean that the same is true for people. The Pirate Bay was ruthlessly prosecuted in Sweden on behalf of Hollywood, its founders jailed and buried under a multimillion-dollar debt. The Swedish welfare state, a fortress of institutionally guaranteed equality and wealth redistribution, comes with a hefty rule book. Outsiders do not necessarily appreciate Sweden's many written and unwritten protocols, its Pippi Longstocking libertarian past of long-standing popular imagination still stuck in their heads.

In August 2010, two Swedish women who had volunteered for WikiLeaks and subsequently slept with

Assange, reported him to the police. The women said that he had sexually mistreated them. Somewhat ironically, Assange had come to Sweden to apply for citizenship. The Swedish judiciary leaked the allegations against him to a tabloid newspaper. The details of this case, insofar as they are known, have been covered extensively in other places, sometimes in a nuanced manner, but more often as implicit or explicit “proof” that WikiLeaks and Assange are not to be trusted. Regarding himself as a victim, Assange later responded: “Sweden is the Saudi Arabia of feminism. I fell into a hornets’ nest of revolutionary feminism.”²⁶

Before being heard by the police, Assange left Sweden and went to London. This in particular dealt a sensitive blow to WikiLeaks’ credibility and Assange’s reputation as a “cult figure for the European young and leftist.”²⁷ It gave the impression that he was avoiding being held accountable for whatever had happened between him and the two women.

In due course, Interpol issued a Red Notice. Assange offered himself for arrest to the London Metropolitan Police, and pending legal disagreements between him and the Swedish prosecutor, was granted bail. WikiLeaks’ operational headquarters moved to Ellingham Hall, a country estate in Norfolk and two-hour drive east of London, which was rented from WikiLeaks supporter Vaughn Smith, the founder of London’s Frontline Club for journalists. While Assange asserts that Sweden’s extradition request was a proxy for his imminent deportation to the United States, the damage was done. WikiLeaks was no longer faceless, leaderless, or stateless. It had a face: Assange. It had a leader: Assange. And it had a state: the United Kingdom, where Assange was trapped.

COLDER

Under house arrest in Ellingham Hall, Assange was unable to maintain his normal travel schedule. He started a talk show on the Russia-owned television channel

RT, which is the English-language subsidiary of Russian state television.

Critics were quick to dismiss his show, *The World Tomorrow*, arguing that the free-speech advocate was sleeping with the devil. RT is the successor to Russia Today, an unrepentant propaganda machine running shirtless pictures of Vladimir Putin and the like.

But Russia Today’s makeover into RT was indeed a clever one. RT’s founding editor Margarita Simonyan—appointed at the age of twenty-five by Putin himself—sensed that RT should not need to promote Russia at all with so much going wrong in the West, and with there being a large constituency of young people completely disregarded by its establishment-abiding mainstream media. The Kremlin-backed channel set up much of its programming around Western political dissent. The drop in popular support for President Obama, in particular among disappointed young voters, presented a new opportunity for RT. It extensively covered WikiLeaks and Occupy Wall Street, and gave massive (and often quality) airtime to its activists. On YouTube, RT is second to only the BBC in number of views. The channel is already the most-viewed foreign broadcaster in a number of major US cities. “There’s large demand for media that doesn’t just parrot the uniform pulp from the Western press,” Simonyan told *Der Spiegel*.²⁸

SNOWDEN AND RUSSIA

In many ways, Edward Snowden is the heir to WikiLeaks. In July 2013, after leaving the United States, he handed his NSA files over to *Guardian* journalist Glenn Greenwald in a luxury hotel in Hong Kong where he was also interviewed by the documentary filmmaker Laura Poitras. Not long after, he flew to Moscow, initially hoping to leave the Russian capital as soon as he could. But with his US passport revoked, he could not leave Sheremetyevo’s transit zone, which held him hostage like a luxury prison for the stateless. Snowden received asylum offers from Nicaragua and Venezuela, but it was

unclear how he should get to these countries without crossing the airspace of the United States and its allies.

Such concerns weren't all theoretical. The Bolivian president Evo Morales was forced to make an emergency landing in Vienna after taking off from another Moscow airport. France, Spain, Portugal, and Italy blocked it from entering their airspace; they had received information that Snowden was on board. The Austrian police searched the plane and it turned out he wasn't. Morales added, after landing in La Paz, that European countries should liberate themselves from the "imperialism" of the Americans.²⁹ Bolivia then offered Snowden asylum.³⁰

Snowden, a political refugee from the United States, saw each one of his possible flight paths from Moscow arching over Europe. Yet EU countries wouldn't do anything for him despite the NSA's blanket violations of rights that Europe has pledged to guarantee.³¹ The background of European apathy may not even be direct political manipulation by its allies, but rather a deeply engrained fear of acting unilaterally.

It was asylum by Russia that finally saved Snowden. Russia's national Facebook equivalent, VKontakte, offered the whistleblower a job.³² Anna Chapman, Russia's most glamorous spy, sent out a tweet asking Snowden to marry her.³³ And, in a 2014 "town hall meeting" (broadcast by RT, of course), Snowden asked Putin a direct question about Russian internet surveillance. Here is how the *Daily Beast* described that encounter:

Vladimir Putin just trolled President Barack Obama and the entire US intelligence community. He trolled them hard. On live Russian television Edward Snowden, the former NSA contractor who exposed America's dragnet surveillance of call records and Internet traffic, asked the Russian leader whether Moscow does the same: "Does Russia intercept, store or analyze in any way the communications of millions of individuals?"

Not to worry, Putin tells America's most famous intelligence leaker: "We don't have a mass system for such interception and according to our law it cannot exist."³⁴

The Cold War-style faultline that became apparent with Snowden's asylum in Russia was already drafted with the RT-Assange alliance. It's not so much Assange's or Snowden's fault. It's rather Putin's reinvention of Russian gameplay in the world. The Russian leader's favorite thinkers are nineteenth-century religious mysticists like Ivan Ilyin, who dreamed of a great Russian empire.³⁵ In countering the West, Putin merely exploits his opponent's unresolved contradictions, dilemmas, and fears. With focus shifting from the West to the 2014 events in Ukraine and Crimea, however, a different light can be shed on Russia, RT, and its distribution of black propaganda.³⁶

ASSANGE AND ECUADOR

In 2011, Assange made the acquaintance of the Ecuadorian president, Rafael Correa, who appeared as a guest on RT's *The World Tomorrow*. The two men seemed to get along. As the UK Supreme Court ordered Assange's extradition to Sweden in May 2012, Assange immediately applied for political asylum in Ecuador, seeking refuge in its London embassy. His personal connection to Correa played a key role in him being granted the asylum. Assange has now lived on his tiny Latin American postage stamp for more than two years. He can't leave, and is giving press conferences and speeches from the balcony, and interviews and Skype lectures from his room. Assange, like WikiLeaks' data, is stored in a location unreachable to the adversary sovereign, but that place is also his prison cell. Black transparency is exiled to Russia and Ecuador.

SNOWDEN, WIKILEAKS, AND GERMANY

On November 7, 2013, following Snowden's revelations, Germany and Brazil presented a nonbinding resolution

to the UN General Assembly that called to extend internationally guaranteed privacy rights to the internet and to electronic communication. The resolution also called for “independent oversight mechanisms to ensure transparency and accountability of states in regards to their surveillance operations.”³⁷ At the time of writing, it is understood that the US government has paid spies to eavesdrop on the committee that investigates the NSA’s activities in Germany, including bugging Chancellor Angela Merkel’s phone. As a consequence, the CIA’s lead representative in Germany was asked to leave the country in July 2014. While previously unquestioned alliances, like the one between Germany and the United States, showed signs of weakening, the rift is unlikely to widen as the Ukraine crisis forces both countries to collaborate to get Putin under control.

With Assange holed up in London, WikiLeaks co-editor Sarah Harrison, who helped Snowden in Hong Kong and Moscow, now lives in “exile” in Berlin, unable to return to Britain. In a statement on the WikiLeaks site, Harrison wrote: “For the next 39 days I remained with [Snowden] in the transit zone of Moscow’s Sheremetyevo airport, where I assisted in his legal application to 21 countries for asylum, including Germany, successfully securing his asylum in Russia despite substantial pressure by the United States. I then remained with him until our team was confident that he had established himself and was free from the interference of any government.”³⁹

At the 2013 Chaos Computer Congress in Berlin, Harrison made an impromptu appearance. Her refreshing intervention was a reminder of WikiLeaks’ original incarnation, with the difference that WikiLeaks was now the “parent” and Snowden the “heir.” Then, another special guest was unveiled by video link. In a gigantic projection behind Harrison, Assange appeared, addressing the Berlin audience straight from the Ecuadorian embassy in London. He wasn’t wearing an Icelandic sweater.

V POP

We e-mailed WikiLeaks in June 2010, proposing to work on their visual identity. The response did not take long to arrive. It read:

Absolutely. Go for it! We have a shortage of such things ...

J.A.

The WikiLeaks logo—an hourglass containing two worlds, one leaking onto the other—is one of the internet’s best pieces of abstract manga. It can even be considered a digital twenty-first-century Salvador Dalí painting. Yet it is also a very awkward-looking vector illustration. If the logo is a form of digital science fiction, at the same time it feels like it is cut-and-pasted together on a slow PC in an internet cafe in Nairobi. It isn’t an overproduced Hollywood image; more of an insurgent pasteboard. WikiLeaks’ web banners beg its visitors for financial support, sharing a similar feeling of under-designed emergency. The site’s early 2011 visual overhaul demonstrated the intent to appear clean and professional, or as Assange called it, “bathroomsque.”³⁹ This half-hearted attempt at technosterility only emphasized that WikiLeaks is not part of the economic and aesthetic structure of the global media—that it is not a boutique outfit or luxury hotel for “the new news,” but a precarious, man-made observatory of the nature of global power.

WikiLeaks parodies the regimes it criticizes. From its bombastic press conferences, to a “sponsor wall” with PayPal, MasterCard, and VISA logos flipped and turned upside down in protest to their collective boycott of the whistleblower site—all is done to play a trick, to exhaust a repertoire of forms and formats common to the techno-economic superstructure that it reveals and undercuts.

When global-media spotlights were cast on the organization, its logo rose to disproportional fame. Designed to “foment untraceable, unstoppable mass document leaking” in the absence of representative people, their portraits, or other images, the logo functioned as both a credibility statement—“this seems like an organization”—and as a collective anonymizer. Behind its hourglass, WikiLeaks could be everyone and no one in particular. The logo served its traditional purpose. But at the same time, it provided a veil to those running the organization.

Logos are superfluous, boring things. The aesthetic vanguard of architecture and graphic-design professionals has reduced them to black-and-white typographical acronyms, and denounces them completely if possible. But for those less embroiled in the tidal movements of modern design, the logo goes unquestioned. It still provides basic proof that an organization exists.

Yet as soon as WikiLeaks became substantially controversial in the eyes of Western power, a more complex image economy was unleashed, which the logo could neither suppress nor represent. It was an economy of faces. Of Assange. Of Amy Goodman, the *Democracy Now!* anchor. Of Jennifer Robinson, Assange’s lawyer. Of Bradley (now Chelsea) Manning. Of former spokesperson Daniel Domscheit-Berg, and associate Israel Shamir. Of Joe Biden and Hillary Clinton. Of Jemima Khan, Bianca Jagger, and Vivienne Westwood. A seemingly endless succession of avatars began to be attached to the WikiLeaks brand.

We proposed that a new visual identity could be based on this vast array of faces. We also contended that we could work on an identity based on WikiLeaks’ multi-jurisdictional hosting model where servers in different countries would ensure that information can never be taken down. Assange asserted that he didn’t need such an identity—instead, he told us, he needed merchandising products to avert the financial embargo that prevented WikiLeaks from receiving donations. He mentioned T-shirts and cof-

fee mugs as products to work on. We designed a series of T-shirts with the word WikiLeaks stretched and waving in its original, deadpan Times New Roman. The T-shirts commemorated the most famous leaks: each had its own T-shirt.

We designed a series of large silk scarves, with the idea that the secretive WikiLeaks brand harbored a hidden favela chic. The illicit luxury of a fake Louis Vuitton scarf, ripping off the intellectual property and brand value from its original; the knockoff as a geopolitical revenge. Appropriately, the first edition of the scarves was produced in Asia. We were also interested in the notion of “transparent camouflage,” the idea that a scarf provides both opacity and transparency in almost equal measure.

M.I.A.

The World Tomorrow’s theme music was composed by Mathangi “Maya” Arulpragasam, better known as M.I.A. Her career, spanning music and fashion, has been heavily themed around her Sri Lankan descent and affiliation with the Tamil resistance movement. On New Year’s Eve 2010, she released a WikiLeaks-inspired mixtape under the moniker of Vicki Leekx.

M.I.A. is perhaps the mother of radical chic. Her work is often devoid of the specific content of the politics of rebellion that she advocates. This fits with the idea that WikiLeaks, as a global brand, needs fashion ambassadors who translate what the organization does into pop culture, without taking from the site’s core leaking business. But it also shows that a currency of celebrity had gradually taken over from WikiLeaks’ initial cult of invisibility.

M.I.A. opened one of her November 2013 tour concerts in New York with a live Skype statement by Assange. He called her “the world’s loudest and finest rapping and dancing megaphone for the truth.”⁴⁰ She said:

For me, it was just about having information. [...] With what’s going on in the press and in

America—in New York, especially—it's such an eclectic and diverse place [and] has been a cultural hub, but now I think information is a little bit harder to get from the outside. So it was really amazing to expose my fans to a live feed in the Ecuador embassy and give them that moment where they can actually get direct information, not through news or media outlets, but just get something right there that no one else knew. That's why I didn't even tweet it.⁴¹

The only information given is the fact that a connection was made with Assange through a Skype call. Nothing of what had been said was mentioned.

In the past, WikiLeaks wanted sophisticated whistleblowers, Dalai Lamas, ethical goddesses and gods to be its political armor. What once was an “intelligence agency of the people” gradually became transparency's shipwreck. The accusation of persistent egomania is never far away, and in such a bleak universe, when there are almost no new leaks to be shared, celebrity is a way to stay visible. In celebrity, existence is content.

LADY GAGA

In October 2012, the global pop phenomenon Lady Gaga was snapped by paparazzi leaving the Ecuadorian embassy.⁴² There had been two prior pop-cultural conjunctions between Gaga and the WikiLeaks megabrand. The first one occurred when Manning, while stationed in Iraq in 2010, had gathered military files on a rewritable CD marked “Lady Gaga.” The second conjunction was the rumor of a close friendship between Gaga and Slavoj Žižek, the Lacanian philosopher, which went viral in the United Kingdom at the end of 2010 thanks to some cleverly crafted “Žižek quotes” of questionable veracity cited on the pages of *Vogue* and the *New York Post*.⁴³ During Žižek's high-profile debate with Assange in London in

2011, the story became attached to WikiLeaks because of the philosopher's denial of the acquaintance.

When Manning got sentenced the next year, Lady Gaga tweeted: “The news of Bradley Manning's sentencing is devastating. If our own can't speak up about injustice who will? How will we ever move forward?”⁴⁴

VI

THE PERSONAL IS GEOPOLITICAL

The *Economist* noted in 2010: “Liberalism was once a radical, revolutionary philosophy, but it has become hard to believe it. What is most intriguing about the WikiLeaks saga is not the pathology of hacker culture [...], but the possibility that Julian Assange and his confederates have made dull liberal principles seem once again sexily subversive by exposing power's reactionary panic when a few people with a practical bent actually bother to take them seriously.”⁴⁵

WikiLeaks' geopolitics were personal. Cunning, game-like dissidence informed the group's every move under the gaze of its spellbinding logo. Some elements of its geopolitics have since become universally available goods, such as anonymous drop boxes. No longer the property or asset of a single organization, now anyone can set up such a drop box with open-source software.⁴⁶

Had it continued in its 2006 mold of anonymity, WikiLeaks perhaps would have remained an underground phenomenon, an alternative media outlet. It can only really outperform adversaries who are below a certain size and scope. In other words, a head-on confrontation with the US government—such as the one WikiLeaks had the courage to seek—is only under very exceptional circumstances a gambit to be won.

Many have argued that there were design flaws in the original WikiLeaks model that, had they been identified and worked on, could have been overcome and could have resulted in a better or “grown-up” version of

universal → open source
guides individual (for public)
action



WikiLeaks. Such arguments are made by people like Domscheit-Berg who felt frustrated with WikiLeaks' lack of internal structure and accountability, and offended by Assange's ways of asserting centralized, yet in their view unaccountable leadership.

But possibly, WikiLeaks—the tiny butterfly—was simply always meant to be swept up by the geopolitical tornados it triggered. The “evidence” it produces is not just in the leaks but also in power's response.

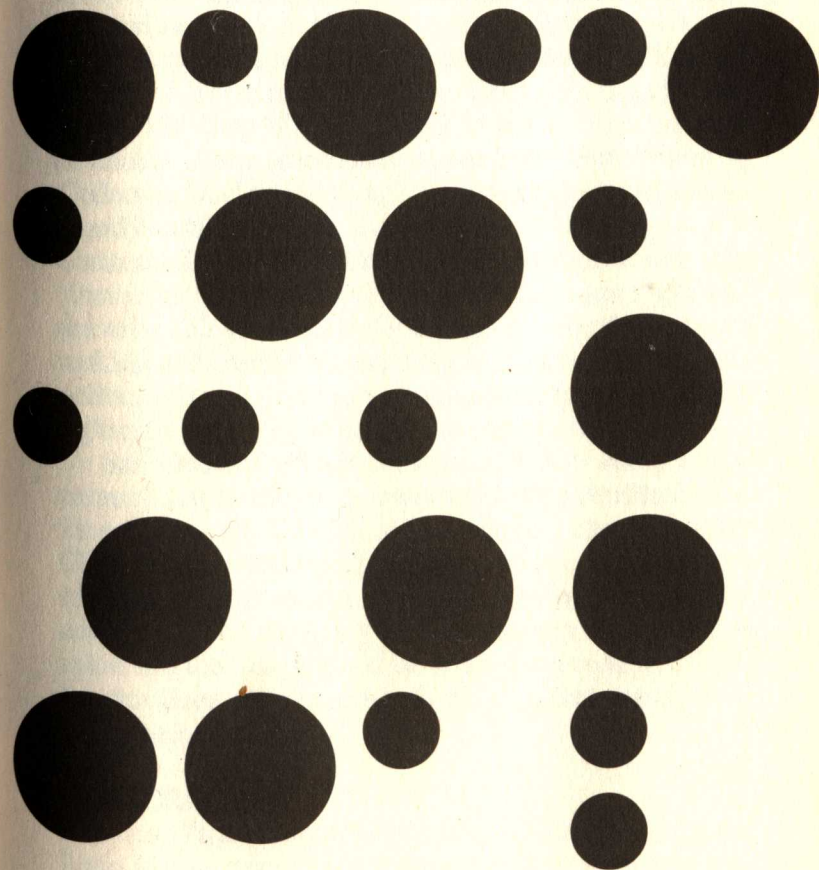
As Saroj Giri stated:

WikiLeaks clearly embodies a radical rupture in US imperialism's normal functioning and also from the normal channels of dissent and “citizen activism” set up by imperialism. As it stands, Wikileaks cannot be contained and even understood as part of an impeccably liberal idea of an active citizenry, transparency, accountability and so on. WikiLeaks is not just demanding the right of citizens to know about the decisions and actions of those in power but is challenging the very legitimacy of that power. “Knowing the truth” through Amnesty or Reporters Sans Frontières that are established groups engaging with states through established procedures and legal battles is one thing. Knowing, in terms and conditions that are themselves illegitimate from the standpoint of power, is however another thing—it radicalizes the very meaning and significance of the “right to know.” WikiLeaks' action is therefore at one level a purely formal gesture, the audacity of the act, which stands on its own irrespective of how damning the actual contents of the leaks have been for the US and other governments, irrespective of the diplomatic fall-out and embarrassment caused. At least in the way it was received by large majority of people in the world, its action seems to carry an insurrectionary force,

highly dissonant and subversive for the “established order.”⁴⁷

WikiLeaks has lost much of its political armor, even as it regained a capacity to receive and publish documents. It continues to unravel the circuitry of modern state power: Where does this end, and does it ever end? Probably not. This the rupture: What is an organization in the afterlife of imperial intervention? A masthead on a website. A logo drawn by an Australian student. A name known to the public—yet no longer the Transparency International of the big What. The NO-NGO. After WikiLeaks began wheeling and dealing real power—real power being the catalyst of the cascade, a totalitarian super-brand, or the stranded remains of a pirate galleon that once sailed the oceans—there was no more organization. There was only you.

OPEN GOVERNMENT GLASS CANDY



Can we still take transparency seriously? Of more recent coinage than its older antonym, secrecy, transparency is sometimes practiced genuinely, but ever so often only an instrument to make a government appear "open" to "civic engagement," leaving the state's core of secrecy intact. Worse, transparency can be used as a tool to make dictatorship seem okay. A takedown of the long political slumber led to transparency's awakening in the twentieth and twenty-first centuries.

Everything is "civic" today: media, tech, engagement, Honda cars. "Civic" is the "political" that has been tamed & co-opted by donors & VCs.

—Evgeny Morozov¹

SAIF QADDAFI WAS groomed (and doomed) to be the heir to his father, Muammar, the late dictator, until the Arab Spring came and swept away Libya's ruling dynasty. Deep links between the despot and his Western allies became exposed. A playboy on the international scene, Qaddafi received a PhD in philosophy from the London School of Economics (LSE) in 2008. His dissertation, titled "The Role of Civil Society in the Democratization of Global Governance Institutions: From 'Soft Power' to Collective Decision Making?," was cowritten by a Boston-based consultancy firm that was paid by the Libyan government. In his dissertation, Saif Qaddafi wrote that "increased transparency is of vital importance if citizens are to be able to successfully engage in collective decision making and consent through voting—two of the cosmopolitan principles that are necessary to ensure a just and legitimate system of international governance."²

Saif Qaddafi's thesis demonstrates how easily transparency may be used as a decoy for anything but itself, and for purposes wholly opposed to its ends. The researcher Clare Birchall notes that while we do not live in an age of transparency, we do live in an age of *transparency advocacy*.³ The advocacy of transparency as a political value and tool may indeed be at an unprecedented high, but this does not mean that there is, in fact, transparent government around.

SECRECY

The word "transparent," which comes from the Medieval Latin word *transparentem*, describes the visual property of translucence. The word first appeared in the early fifteenth century. Its usage as a figurative, phenomenal

expression for “easily seen through” dates from the late sixteenth century.⁴ The antonym of transparent is “opaque.” In its contemporary usage, transparency is contrasted with “secrecy” so often that Google autofills the phrases “transparency vs.” and “secrecy vs.” with their respective antonyms. The political secret, by comparison, is much older than transparency. In 109 AD, the Roman historian Tacitus coined the term *arcana imperii*—the “secrets of imperial policy.” These were the crown jewels of political rule.⁵ This archaic configuration of power, built around secrecy, has survived in modern times. Eva Horn emphasizes: “Modern power fundamentally hinges on a vast range of secrets and secrecy. However, unlike pre-modern regimes that viewed their *arcana imperii* as a legitimate part of governance, modern governments tend to make a secret of their dependence on secrets.”⁶

The WikiLeaks and Edward Snowden episodes have laid bare how nominally open systems build an elaborate architecture of legal and administrative barriers to obscure their reliance on secrecy. Bringing this architecture into the open by removing the barrier frustrates the very mechanics of geopolitical gameplay. Henry Farrell and Martha Finnemore argue that leakers “undermine Washington’s ability to act hypocritically and get away with it.” Hypocrisy, then, is “central to Washington’s soft power—its ability to get other countries to accept the legitimacy of its actions.” Indeed, “secrecy can be defended in a democracy. Blatant hypocrisy is a tougher sell.”⁷ If transparency advocacy and dictatorship can live together happily, then what is transparency but pseudo-liberal gibberish, only useful to open doors to the upper echelons of power—and then, once doors are opened and positions taken, to be laughed at, joked about, ditched, and killed? Was transparency ever something more than a noble lie? Was legitimacy ever something other than *our ignorance*?

Time and again the extralegal character of sovereign power reveals itself: the same decision makers who

obscure the legal rationale behind their secret actions also proclaim to be advocates of open government and a free internet.⁸ In the 1920s, the German jurist Carl Schmitt suggested that no one can predict, and thus legally codify, the unexpected; it is the sovereign alone who decides on the state of exception that results from its occurrence. This unpredictable threat, Schmitt said, is “a case of extreme peril, a danger to the existence of the state, or the like. But it cannot be circumscribed factually and made to conform to a preformed law.”⁹ What Schmitt still saw as a perilous glitch demanding instantaneous action, has with today’s national security policies become an all-encompassing domain of preemptive militarization, surveillance, and secrecy. Judicial and executive power are forming strange new hybrids. For example, Foreign Intelligence Surveillance Act (FISA) courts, deliberating in complete secrecy, routinely renew the NSA’s blanket surveillance mandate. Though it is alive and well today, it is not so much the sole prerogative of the heads of state anymore to decide on the exception. Rather, exceptionalism has become a property of the entire executive branch. A vast crypto-industrial complex depends on and caters to its addictions. WikiLeaks and Snowden have helped expose a tip of the iceberg of this public-private cohort—this new Holy Alliance that binds old-style *arcana imperii* to the latest cloud technology. So while the world recedes into neo-feudal rule by tech overlords and extralegal sovereigns, at the same time it appears overjoyed with the idea of transparency. How did this paradox come about?

GLASS REVOLUTION

In the nineteenth and twentieth centuries, glass became endowed with political, social, and aesthetic idealism. In the Great Exhibition of 1851, London opened its newly built Crystal Palace—an enormous edifice made out of glass sheets and cast iron. The Crystal Palace in its organizational principle was still Neoclassicist, symmetrical,

if transparent object casts shadow
what does it say about secrecy?

hierarchical. The revolution lay in its material translucency. The concealment that had always been essential to architecture was replaced by revelation.

Glass would make it impossible for anyone to harbor secrets, and caused intellectuals and revolutionaries to predict how it would incapacitate the ancien régime. Paul Scheerbart's 1914 manifesto *Glass Architecture* is a shining example of glass advocacy. He took the liberating potential of the translucent material quite literally, and conceded: "We live for the most part within enclosed spaces. These form the environment from which our culture grows. Our culture is in a sense a product of our architecture. If we wish to raise our culture to a higher level, we are forced for better or worse to transform our architecture. And this will be possible only if we remove the enclosed quality from the spaces within which we live."¹⁰ There was a wish for full transparency without surprises; a glass world without promises, vagueness, or mysteries. Visions of clarity, based on the glass metaphor, spread across design, art, and architecture. In 1932, the writer Beatrice Warde likened her ideal of the printed page to a crystal goblet, and saw this as pertaining to a state of invisibility where a container only exists to fully reveal its contents—be it the written word or wine.¹¹ Warde's belief in typography as a transparent container hints at a more stealthy idea: a design that is invisible and thus concealing itself by transparency. Detlef Mertins notes that, for the philosopher Walter Benjamin writing a year after Warde, "glass architecture assumes the characteristics of a revolutionary surface for a new subjectivity—an austere and slick surface on which it is hard to leave traces, accumulate commodities or form habits."¹² Benjamin advocated "a kind of 'traceless' living in a technologised environment that had realised itself fully, that is transparently, its physiognomy no longer deformed to harbour secrets."¹³

Benjamin's *The Arcades Project* was an ambitious endeavor, in part dedicated to the analysis of glass-roofed shopping arcades in Europe. The following fragment from

The Arcades Project can be read as a premonition to transparency as an image of collective desire—an image into which a society tries to project a better version of itself:

Corresponding to the form of the new means of production, which in the beginning is still ruled by the form of the old [...] are images in the collective consciousness in which the new is permeated with the old. These images are wish images: in them the collective seeks to both overcome and to transfigure the immaturity of the social product and the inadequacies in the social organization of production. At the same time, what emerges in these wish images is the resolute effort to distance oneself from all that is antiquated—which includes, however, the recent past.¹⁴

However, the opposite could also be true: imposed transparency would allow the government to spy on everyone. Yevgeny Zamyatin's 1923 dystopian science-fiction novel *We* is set in a see-through city of glass, called the One-State. In this totalitarian panopticon, where all political and most social life is forced to take place under complete transparency, Zamyatin offers an amazing reading of the opacity of fog. The novel's protagonist, a government worker, falls in love with a spellbinding female resistance leader, "I-330" (all inhabitants of the One-State are referred to by numbers). She asks him if he will follow her everywhere, no matter what. And this is something he wants, but also fears. They walk through the fog together—which, of course, obscures their movements from the all-seeing gaze of the OneState. I-330 asks, "You like the fog?" He answers, "I hate the fog. I'm afraid of the fog." I-330 responds: "That means you love it. You're afraid of it because it's stronger than you, you hate it because you're afraid of it, you love it because you can't master it. You can only love something that refuses to be mastered."¹⁵

Glass has not, of course, lived up to its revolutionary dreams. Banks and financial firms have hijacked the glass facade and made it the ultimate expression of corporate value. As the processes of finance capital became invisible, intangible, and abstract, they required a new paradigm for their representation in architecture.¹⁶ That representational paradigm was transparency. Sky-lit atria and glass facades disclose precisely nothing about the reality of modern finance: data transfers, high-speed trading, and other digital processes taking place in data centers and custom-built fiberoptic highways. Mertins, however, reminds us that with the “significant changes that have taken place in technology and culture, it can be said that glass is still glass because it was never just glass.”¹⁷

“AN INHERENT QUALITY OF ORGANIZATION”

In a famous 1964 essay titled simply “Transparency,” architects Colin Rowe and Robert Slutzky noted that transparency is “dignified with far from disagreeable moral overtones.” They stated: “[It is] the result of an intellectual imperative, of our inherent demand for that which should be easily detected, perfectly evident, and free of dissimulation.” Rather than just considering material translucence (or, more precisely, glass), they defined it as a “broader spatial order,” pertaining to the “simultaneous perception of different spatial locations”—“an inherent quality of organization.”¹⁸ The authors illustrated their ideas with Le Corbusier’s unrealized 1927 design for a League of Nations campus in Geneva. On this campus, the observer would be able to identify and understand the different elements that made up the building complex, as well as the relationships between them. Rowe and Slutzky, however, did not make an obvious next step, which would have taken them from Le Corbusier to an *even broader* spatial order: the League of Nations itself.

Indeed, the idea of “phenomenal transparency,” which Rowe and Slutzky introduced to contrast with the

“literal transparency” of glass, is not merely a quality of organization. It *is* organization.

The League of Nations was an intergovernmental organization intended to become a forum for transparent world affairs. It was originally proposed by US president Woodrow Wilson to avert another world war, establishing accountable international law putting limits on interstate conflict. But the League, founded in 1919 and dissolved in 1946, was incapable of containing Italy, Spain, and Germany—three hostile powers who were nonetheless among its members. When Italy invaded Ethiopia in 1935, killing tribal warriors with machine guns and mustard gas, the other members of the League stood by and watched the onslaught as if it were a soccer match. World War Two signed the League’s fate as a design fiction, armed only with the best intentions.

What didn’t work on the transnational scene did work, to some extent, on the national scale. The United States took the lead in policy experiments with government transparency. In 1913, Louis Brandeis wrote that “sunlight is the best of disinfectants.”¹⁹ Brandeis was a brilliant lawyer with close ties to Wilson; he owed his appointment at the US Supreme Court to the president. A pragmatic visionary, Brandeis wanted the age of fast industrial development to become equally progressive on matters of policy. As America’s industrial power was on the rise, Brandeis fought for minimum wages for female workers and for government and business accountability. President Wilson stated: “Government ought to be all outside and no inside. I, for my part, believe there ought to be no place where anything can be done that everybody does not know about. [...] Secrecy means impropriety.” As Birchall reminds us, “Wilson’s *Fourteen points* (1918), which informed the flavour of Armistice and became the basis of the League of Nations, began with an insistence upon transparent diplomacy: point 1 calls for: ‘Open covenants of peace, openly arrived at, after which there shall be no private international understandings of

any kind but diplomacy shall proceed always frankly and in the public view.”²⁰

Transparency set on a path toward institutionalization. Harold L. Cross’s 1953 book *The People’s Right to Know: Legal Access to Public Records and Proceedings* laid the groundwork for the United States Freedom of Information Act (FOIA), which was signed into law in 1966 by President Lyndon B. Johnson. The terms “freedom of information” and “the right to know” have become common parlance since. One of the act’s most outspoken advocates was Donald Rumsfeld—the same politician who later approved secret torture at the Abu Ghraib prison in Iraq.

WHISTLEBLOWERS

In 1972, Ralph Nader coined the term “whistleblower” in his book of the same name. Whistleblowers expose an organization’s wrongdoing by releasing secret documents into the public realm under an ethical imperative. The world’s most famous whistleblower was Daniel Ellsberg, who in 1971 leaked the Pentagon Papers to the *New York Times* hoping to expose the true nature of the Vietnam War to the American public. In 1996, the *New York Times* concluded that the Johnson administration, which had introduced FOIA, had “systematically lied, not only to the public but also to Congress.”²¹ According to the public-policy scholar Ann Florini, transparency “refers to the degree to which information is available to outsiders that enables them to have an informed voice in decisions and/or to assess the decisions made by insiders.”²² Florini does not distinguish between the suppliers of information. It may be an organization, a dissenting insider, or an outsider who has acquired access to such information. The differences between these types and methods of disclosure matter greatly—they do so ethically, politically, and legally. Involuntary disclosure, or black transparency, reveals three things at once. First, the secret itself. Second, the secret’s keepers and their panic once the secret is released into the world. Third, the framing or “spin” of

the disclosure, which matters to its political impact. Accordingly, black transparency can never be “only” about the information that is released.

Ellsberg photocopied the Pentagon Papers by hand. The act of leaking depended as much on physical labor as it did on its delivery in a proverbial brown envelope; and the entire process finally relied on the willingness and capability of journalists to interpret and release the information. And in turn, this hinges on a newspaper’s courage to oppose the government and practice—what Glenn Greenwald calls “adversarial journalism.”

Once WikiLeaks enabled whistleblowers to upload documents digitally, protecting their anonymity, the distinction between source and publisher became fuzzy. With its anonymous drop box and its uncensorable publishing platform, WikiLeaks was “an intelligence agency of the people, casting pearls before swine.”²³ Everyone in the crowded, filthy, and chaotic city square awaits the spectacle that is WikiLeaks’ guillotine of information. This story is as old as Robin Hood.

349 GIGABYTES OF POSSIBLE NOTHINGNESS

WikiLeaks’ black transparency demonstrates deep links between transparency and secrecy. The most bizarre WikiLeaks releases are its so-called insurance files. The organization describes these as “encrypted versions of upcoming publication data.” These informational black holes are released “from time to time to nullify attempts at prior restraint.”²⁴ The first insurance file was posted in July 2010 as a supplement to the Afghan War Logs.²⁵ The largest one to date, posted on August 17, 2013, is a 349-gigabyte-sized document.²⁶ However, the files can only be unlocked once their passwords are published, and none has been so far. It is impossible to know if the files contain intelligible information at all. The cryptographer Bruce Schneier called them “random data bluffing.”²⁷ These black blocs invoke enigma and information mystique.

There has been some speculation about what the cryptic archives may contain. Maybe, as some have suggested, the largest release is nothing other than the entire trove of information that Snowden took from the NSA, equivalent to a Holy Grail of twenty-first-century leaks.

Eva Horn argues that the concealed secret constitutes a “form of looming latency or potentiality that is more powerful than its actual content.”²⁸ The distinction between form and content matters because the importance of a leak is often assumed to be based on its content alone. The insurance files show the importance of the *form* of the leak, devoid of any content. Since we don’t know what is inside and to whom the information, if any, originally belonged, we are free to speculate. Insurance files shadow-box, and play air guitar, against unidentified adversaries.

Edgar Allan Poe’s short story “The Purloined Letter” (1845) unfolds around a compromising letter that was stolen from the French queen; the contents of the letter remain unknown, and irrelevant, throughout the story. All that matters is the form—the envelope: “‘It is clear,’ said I, ‘as you observe, that the letter is still in possession of the minister; since it is this possession, and not any employment of the letter, which bestows the power. With the employment the power departs.’”²⁹

DATA PURLOINED LETTERS

In an interview with *Computer World* in October 2009, Assange said, “At the moment [...] we are sitting on 5 GB from Bank of America, one of the executive’s hard drives.” The remark caught little attention at the time. But on November 29, 2010, *Forbes* reported that WikiLeaks’ next target would be a “major American bank.” Assange affirmed in an interview that the documents WikiLeaks held “could take down a bank or two. [...] Yes, a big US Bank.” Assange stated:

It will give a true and representative insight into how banks behave at the executive level

in a way that will stimulate investigations and reforms, I presume. Usually when you get leaks at this level, it’s about one particular case or one particular violation. For this, there’s only one similar example. It’s like the Enron emails. Why were these so valuable? When Enron collapsed, through court processes, thousands and thousands of emails came out that were internal, and it provided a window into how the whole company was managed. It was all the little decisions that supported the flagrant violations. This will be like that. Yes, there will be some flagrant violations, unethical practices that will be revealed, but it will also be all the supporting decision-making structures and the internal executive ethos that came out, and that’s tremendously valuable. Like the Iraq War Logs, yes there were mass casualty incidents that were very newsworthy, but the great value is seeing the full spectrum of the war. You could call it the ecosystem of corruption. But it’s also all the regular decision making that turns a blind eye to and supports unethical practices: the oversight that’s not done, the priorities of executives, how they think they’re fulfilling their own self-interest. The way they talk about it.³⁰

Technically, this leak was a purloined letter. After the interview, coinciding with Cablegate, Bank of America shares fell by 3 percent.³¹ On December 18, the bank stopped processing WikiLeaks payments, joining an embargo by companies such as VISA, MasterCard, and PayPal. The *New York Times* reported that Bank of America had assembled a crisis team. It bought up potentially defamating internet domain names, and hired a consulting firm to deal with its impending reputation crisis.³²

The law firm Hunton & Williams, on behalf of Bank of America, secretly invited three cybersecurity firms with close ties to the US government. The firms were to

come up with strategies to counter WikiLeaks. The three firms named their collaborative effort Team Themis, after the ancient Greek deity for "divine order." The team consisted of Palantir Technologies, Berico, and HBGary Federal. A PowerPoint presentation that sketched out its plans was coincidentally retrieved by hacktivists that were part of Anonymous. This happened between February 5 and 6, 2011, after they had gained access to HBGary's e-mail server.³³

On February 9, *Reuters* reported that Assange had retracted his statements on the imminent release on Bank of America; he "privately acknowledged the material was not self-explanatory and that he personally was unable to make much sense of it. Assange indicated it would require a substantial amount of effort by financial experts to determine whether any of the material was newsworthy, according to the sources."³⁴ In July 2011, Assange said that WikiLeaks was "under a kind of blackmail in relation to those documents that will be dealt with over time."³⁵ Daniel Domscheit-Berg, a former WikiLeaks spokesperson, added to the confusion a month later. He said he had personally destroyed some of the Bank of America data "in the interest of the security of sources."³⁶ Domscheit-Berg claimed that the Bank of America files were given to WikiLeaks between January and September 2010, which is after Assange's 2009 *Computer World* interview. And obviously, Assange's and Domscheit-Berg's statements on the issue can't both be true.

NEO(CON)LIBERAL TRANSPARENCY

Open government is often seen as an ethical imperative. Yet Birchall, in an analysis of "transparency as a neoliberal tool," points out how for many policymakers open data is an entrepreneurial incentive for citizens who turn from political subjects into "economic nomads."³⁷ Open government champion Neelie Kroes, in her address at Open Government Data Camp 2011 in Warsaw, announced skyrocketing profits from transparency:

Opening up public data will foster the participation of citizens in political and social life, increase the transparency of public administration, and improve public decision making. These will help us address the challenges we face in areas such as transport, energy and health. They will make our lives easier. And they represent important new opportunities for innovative businesses. The overall economic gain could amount to tens of billions of euros, every year.³⁸

Transparent government is usually advocated by simply contrasting it with secretive or corrupt government, making the choice for the first seem easy on ethical grounds. There are plenty of authoritarian states and corrupt leaders to pick from, and the case for transparency seems to become naturally evident. However, there is frequent mention of a government's "performance" or "effectiveness"—notions that have no real ethical resonance, and seem to fall in line with Birchall's description of transparency as a neoliberal trope, or tool. Even if, in this version, transparency is merely a technical feature, a government wielding it can still pride itself on the moral and ethical overtones that come with the concept.

As William D. Eggers writes in *Government 2.0: Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy*, "It's a fairly simple formula: transparency generates accountability, which in turn generates pressure for improved performance, which in turn generates, well, performance."³⁹ Eggers describes what he considers a success story of transparency—the redesign of the state government of Florida:

For years, Donna Arduin, in her capacity as deputy budget director for New York governor George Pataki, was a key player in New York's secretive budget process. [...] When she became Florida's

budget director, she couldn't have faced a more different environment. Florida's far-reaching "sunshine laws" made it renowned for open government. And Arduin's new boss, Jeb Bush, was committed to making Florida government more transparent and performance-based. [...] The combination of Florida's penchant for open government and Bush's penchant for performance management resulted in the first American state budget specifically formatted and designed for the web—what Bush dubbed his "e-budget."⁴⁰

Jeb Bush is George W. Bush's brother. He was, along with Paul Wolfowitz, Donald Rumsfeld, and others, a signatory of the Statement of Principles of the Project for a New American Century (PNAC), a neoconservative think tank at the heart of Bush's redefinition of America's imperial role. Bush, the transparency advocate, was also an adviser to the Lehman Brothers' private equity group before it declared bankruptcy in 2008.⁴¹

Eggers claims that transparency keeps "government accountable to citizens who know what, how and why their government is doing what it's doing." In a disclaimer, he adds: "But just making vital information publicly available doesn't mean much if we have to go to great investigative lengths to find it and by the time we find it, it's already out of date. We shouldn't need a lobbyist to navigate our way around government. We shouldn't be forced to file a Freedom of Information Act request to find out how our government agencies are performing."⁴²

There are some who see transparency as an instrument to question, expose, or even abolish government. But others see it merely as a type of increased managerial efficiency. The coalition between these two groups is bound to dissolve sooner rather than later. In her 2009 treatise, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*, Beth Simone Noveck—who would later

become Obama's deputy chief technology officer for open government—agrees with Eggers: "When the public cannot see how decisions are arrived at, it cannot identify problems and criticize mistakes. Accountability declines and so does government effectiveness."⁴³ However, Noveck recognizes the importance of nongovernmental actors maintaining a check on state power: "Civic groups are also taking advantage of new technologies to shine the light of greater transparency on government from afar. These third-party brokers of transparency are helping to do what government is not doing enough of for itself." Yet, she writes, "these purely civic programs are disconnected from the practices and priorities of government."⁴⁴

Since FOIA exempts areas of government where it would make the biggest difference—the secrets of imperial policy—"open government" is mostly eye candy for the citizen-entrepreneurial policymaker and has no real political implications. Yet among transparency advocates this distinction is not conventionally made; there are ongoing attempts to glue different, incongruous types of transparency together and make it seem as if they all mean the same "sunlight as disinfectant."

Involuntary transparency is something fundamentally different than "open government." The logics of both methods of disclosure are opposed, something transparency advocates often prefer to ignore. Micah Sifry's book *WikiLeaks and the Age of Transparency* is an example of the resulting confusion, as the author simultaneously tries to keep both sides happy. Sifry codirects the Personal Democracy Forum and is a frequent recipient of US government financial help for conferences and "civil society boot camps." He writes:

No one American official has been more eloquent in her expressions of support for the power of the internet than US Secretary of State Hillary Clinton. [...] Under her leadership, the State Department has expanded its use of social

media, developed initiatives to support the use of mobile phones for raising money to aid victims of natural disasters in Pakistan and Haiti, launched a "Virtual Student Foreign Service" to involve college students in online public diplomacy, and organized several visible technology delegations and training workshops to foster greater use of modern tools to strengthen civil society organizations."⁴⁵

But simultaneously, Sifry likes WikiLeaks, and mocks Clinton's bitter condemnations of them. He writes that after Cablegate, she "fell back on a much older way of seeing the world."⁴⁶ Clinton's dislike of WikiLeaks has a much simpler explanation: she is angry. How can a secretary of state be forced to appreciate the exposure of her own government documents that she had hoped to keep secret? Clinton's is not so much an older way of seeing the world; it is the way most governments continue to see the world. Sifry, always on the fence, came to the defense of WikiLeaks once more after Sir Tim Berners-Lee, "a leading advocate for open government and open data," stated that the Cablegate data was "stolen" and that transparency did not apply to state or military secrets. Sifry responded: "With all due respect for Berners-Lee and his pioneering and ongoing contributions to an open society, he is wrong. Government transparency cannot be defined as only the information that governments deign to share with the public."⁴⁷

QADDAFI GOES CIVIC

The musings on transparency and civil society in Saif Qaddafi's PhD dissertation were designed to be liked by Western leaders, policymakers, academics, entrepreneurs, and social-media gurus. The effort was substantial and well under way. For example, Clay Shirky has admitted to consulting with Libya "about using social software to improve citizen engagement in coastal

towns." Shirky wrote: "What we believed at the time was that Libya's planned devolution of political power to individual towns was real; what we learned was that it wasn't. I'm sorry I wasn't able to help expand representative government in Libya, but I'm not sorry I tried."⁴⁸ Saif Qaddafi, in his dissertation, thanked Joseph Nye, the Harvard professor who coined the concept of "soft power." Nye, Saif Qaddafi claimed, had been helping him with his thesis writing on soft power. Like Shirky, Nye visited Libya on the invitation of Monitor, the consulting firm that orchestrated Libya's reputation in the West, and even prepared a monumental tome of Muammar Qaddafi's political writings, adorned with praise from Western academics. Nye reported about his trip in the *New Republic*, shedding favorable sunlight on the despot:

[Muammar] Qaddafi has long been seen as a bad boy in the West. Yet, in recent years, Qaddafi has appeared to be changing. He still wants to project Libyan power, but he is going about it differently than in decades past. Where once he had tried to bully and even overthrow governments to his south, now he is hosting peace talks on Darfur. Where once he sought weapons of mass destruction, now he has abandoned his nuclear program. These moves have paid off: A decade ago Libya was subject to U.N. Security Council sanctions; recently, the United States raised no objection to Libya being seated on the Security Council. Qaddafi, in other words, seems to have become interested in soft power—the art of projecting influence through attraction rather than coercion.⁴⁹

Note the echo chamber here: the architect of soft power gets paid to write that the Libyan dictator has discovered soft power.⁵⁰ Four years later, when it had become

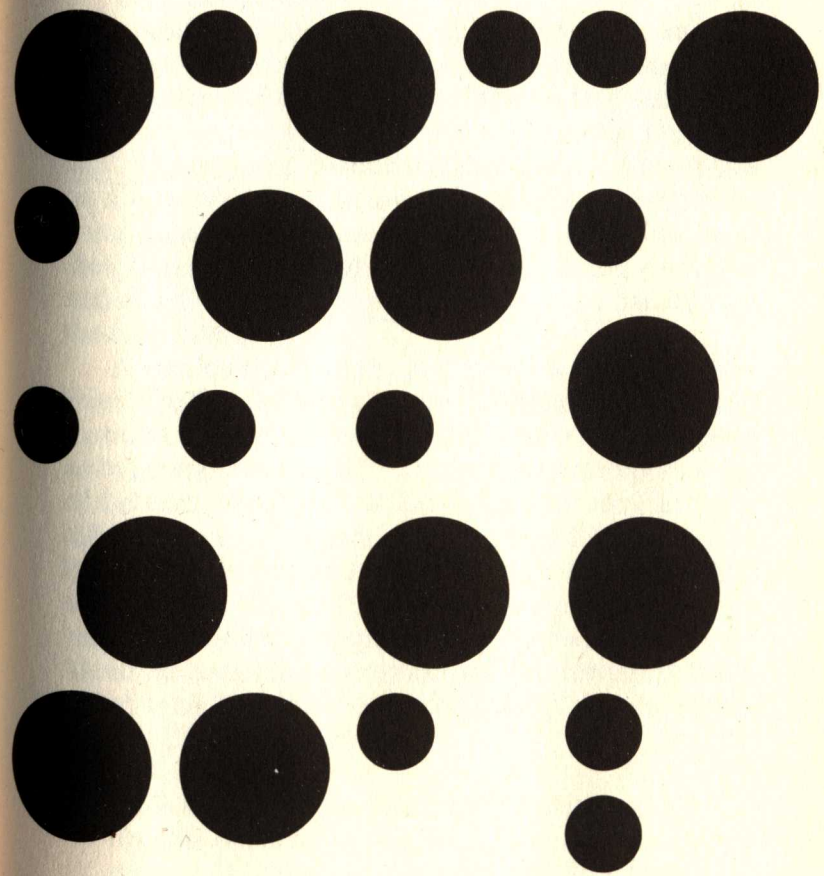
apparent to Nye that "Qaddafi's departure is the only change that will work in Libya," he posthumously belittled his role in the dissertation. Nye propounds that "At the request of a friend, I read one chapter that referred to soft power, something I have done for many who have written about that topic. Otherwise, I was not involved in his thesis and know nothing about the controversy about it that the London School of Economics is now investigating."⁵¹ Saif Qaddafi, however, contends that he met with Nye in person and that the Harvard scholar provided him with extensive advice and direction. He writes: "I would also like to acknowledge the benefit I received from comments on early drafts of the thesis from a number of experts with whom I met and who consented to read portions of the manuscript and provide advice and direction, especially Professor Joseph Nye." Indeed, soft power is discussed in two chapters and spans over one-third of the thesis. Qaddafi's dissertation claims that "the improved human rights record in Libya is in part due to the campaign by the Qaddafi Foundation and other international human rights NGOs."⁵² The snake bites its own tail again: the Qaddafi Foundation was Saif Qaddafi's charity organization, and a boutique outfit for the Libyan regime. The foundation later became a sponsor of the LSE.

The leftist vanguard journal *Kittens*, in a piece criticizing WikiLeaks, wrote the following about transparency:

WikiLeaks proposes that transparency leads to good governance, to a better life for the subjects. However, if a government truthfully reports that the current debt crisis requires large scale cuts to social services, this is transparency; if the US government openly declares its enmity to WikiLeaks, this is transparency; if the law informs someone that his material needs count only insofar they are effective demand, this is transparency; if a state mobilises its population

to militarily defeat the mobilised population of another state, this is transparency. Transparency in itself does not prevent harm: rather, most of the misery is wrought in the open.⁵³

CAPTIVES OF THE CLOUD



The “cloud”—the seemingly intangible conglomerate of deterritorialized servers that keeps our data afloat 24/7—holds almost every single event on the face of the earth in some digital file.

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

I

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

THE COMING

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

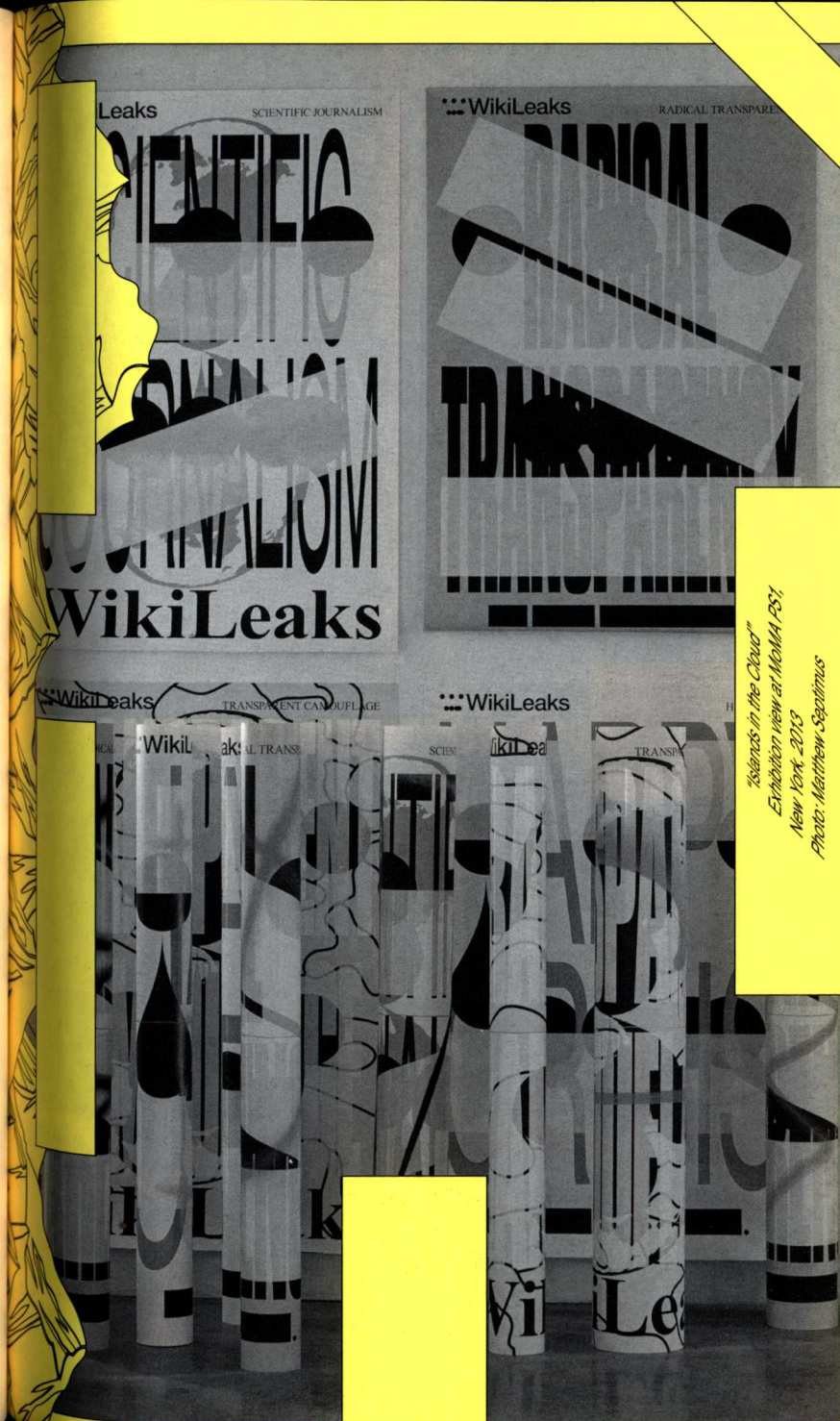
A nondescript diagram in a 1996 MIT research paper titled “The Self-Governing Internet: Coordination by Design,” showed a cloud of networks situated between routers, linked up by Internet Protocol (IP).³ This was the first reported use of the term “cloud” in relation to the internet. The paper talked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

I don’t think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing—they should be in a “cloud” somewhere. And that

if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you—or new devices still to be developed—you can get access to the cloud. There are a number of companies that have benefited from that. Obviously, Google, Yahoo!, eBay, Amazon come to mind. The computation and the data and so forth are in the servers.⁵

The internet can be compared to a patchwork of city-states or an archipelago of islands. User data and content materials are dispersed over different servers, domains, and jurisdictions (i.e., different sovereign countries). The cloud is more like Bismarck's unification of Germany, sweeping up formerly distinct elements, bringing them together under a central government. With the cloud, the user no longer needs to understand how a software program works or where his or her data really is.

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



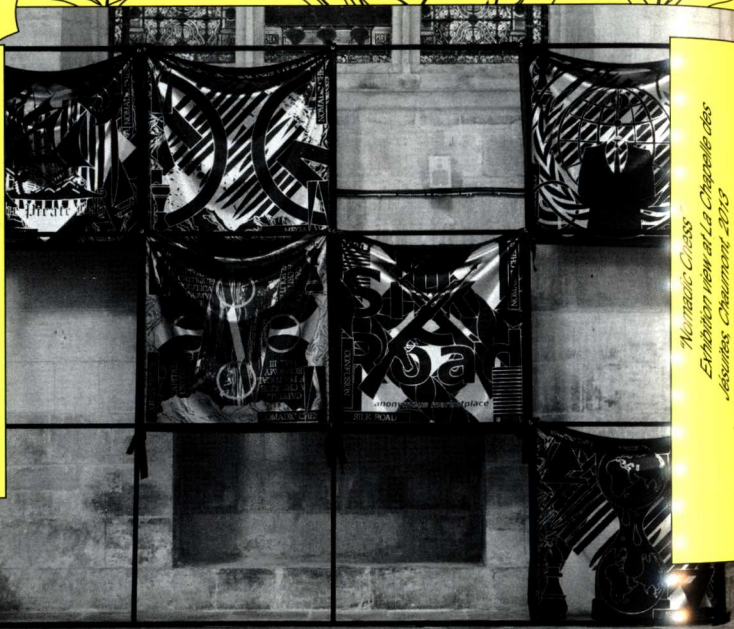
*"Islands in the Cloud"
Exhibition view at MoMA PS1,
New York, 2013
Photo: Matthew Segowitz*

the cloud's central model of data storage and management, which is handled and owned by a handful of corporations.

The coming of the cloud is best described by Aaron Levie, the founder and CEO of Box, one of Silicon Valley's fastest growing cloud storage providers. As Levie states, the biggest driver of the cloud is the ever-expanding spectrum of mobile devices—iPhones, iPads, Androids, and so forth—that enable users to tap into the cloud: “If you think about the market that we’re in, and more broadly just the enterprise software market, the kind of transition that’s happening now from legacy systems to the cloud is literally, by definition, a once-in-a-lifetime opportunity. This is probably going to happen at a larger scale than any other technology transition we’ve seen in the enterprise. Larger than client servers. Larger than mainframes.”⁸ Google, one of the world’s seven largest cloud companies, has recently compared itself to a bank.⁹ That comparison is apt. If data in the cloud is like money in the bank, what happens to that data while it resides in the cloud?

THE UNITED STATES CLOUD AND THE PATRIOT ACT

The amount of access and control over online data is partially determined by who has registered the site, and where it is hosted. For example, all data stored by US companies (or their subsidiaries) in non-US data centers falls under the jurisdiction of the USA Patriot Act, an antiterrorism law introduced in 2001.¹⁰ This emphatically includes the entire US cloud—Facebook, Apple, Twitter, Dropbox, Google, Amazon, Rackspace, Box, Microsoft, and many others. Jeffrey Rosen, a law professor at George Washington University, has established that the Patriot Act, rather than investigating potential terrorists, is mostly used to spy on innocent Americans.¹¹ But the people being watched are not necessarily Americans. Via the cloud, people across the world are subject to the same Patriot Act powers, which are often misused by authorities. Matthew Waxman of the Council on Foreign Relations outlines the situation:



*Monadic Chess
Exhibition view at La Chapelle des
Associés, Charenton-le-Pont, 2013
Photo: Sébastien Allié*



*Fasting phase for "Monadic Chess"
in Amsterdam, 2013
Photo: Mienhaaren*

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

Saskia Sassen, a sociologist, adds to this perspective:

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

Microsoft was the first cloud company to publicly confirm that the Patriot Act gave the government access to its data stored outside the United States.¹⁴ In August 2011, Google also confirmed that its data stored overseas is subject to “lawful access” by the US government.¹⁵ A 2012 white paper, released by the law firm Hogan Lovells, examined these findings and concluded that while the Patriot Act does give the US government access to the cloud, many other governments enjoy similar forms of access under

their own laws—and further, that using the “location” of a cloud server to determine legal protection was a mistaken idea altogether.¹⁶ The paper noted the widespread use of so-called Mutual Legal Assistance Treaties (MLATs), which streamline the exchange between countries of data needed for investigative purposes. Apart from treaty-backed requests, “informal relationships between law enforcement agencies [...] allow for governmental access to data in the ‘possession, custody, or control’ of cloud service providers over whom the requesting country does not otherwise have jurisdiction.” The legality of such informal relationships was not examined by the study. It did not backlog any recorded abuses of the Patriot Act, or discuss reports by two US senators about a “secret interpretation” of the law, which would give the Federal Bureau of Investigation (FBI) far-reaching extra surveillance powers that the public is unaware of.¹⁷

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

SUPER-JURISDICTION

In Egypt during the Arab Spring, Facebook and Twitter played the role of subversive, uncensored, alternative media—in part because the servers and other infrastructure of these popular services were beyond the reach of local authorities. Indeed, former Egyptian president Hosni Mubarak's best bet to fend off the power of the internet was to switch it off entirely. To do so, "just a few phone calls probably sufficed."¹⁹ While Mubarak's ultima ratio was to wall the country off the network, the violent crudeness of this act demonstrated the dictator's much more substantial *lack of power* over the network's larger infrastructure. Sovereign control over the cloud, in contrast to authoritarian power mongering, is a sophisticated affair. One might draw a very different map here: the global spread of the US cloud, for example, results in a kind of "super-jurisdiction" enjoyed by its host country. In 2012, the United States Department of Justice (DOJ) seized the website Megaupload.com. Megaupload Limited was a Hong Kong-based internet enterprise paying loving tribute to all kinds of Hollywood films (to say it politely). According to the company, the site offered "no-registration upload and sharing of files up to 1 gigabyte." It was seized by the DOJ and the FBI in January 2012, backed by film-industry copyright claimants. Megaupload stands accused of generating "more than \$175 million in criminal proceeds" and causing "more than half a billion dollars in harm to copyright owners."²⁰

The site's founder, the then thirty-seven-year-old millionaire entrepreneur Kim Dotcom, and three of his associates were brought to a New Zealand court to face extradition to the United States. They'd been living like self-styled oligarchs. In a gesture toward transparency, they said they had "nothing to hide."²¹ In particular, Dotcom himself embodies the absurd saga of a contemporary, self-parodying internet hooligan—a legal black hole turned persona, unprepared in every way to be "famous" yet accepting the challenge wholeheartedly. Megaupload.com

was, at least in its own imagination, nothing more than a technical conduit between those who upload and those who download—its indiscriminate policies exemplifying a hedonistic brand of laissez-faire anarcho-capitalism. The US government's prosecution of the site remains highly debated, because the DOJ regarded the site's global user base as willing conspirators who were trying to break US law. As Jennifer Granick at Stanford Law School notes, the DOJ referenced "unknown parties" (i.e., the users of Megaupload) as members of a conspiracy to commit copyright infringement in the United States. Granick notes that such users "were located all over the world, and may or may not have acted willfully." Indeed, with Megaupload.com, the government alleges that there was "an agreement to violate a US civil law, including by many people who are not subject to US rules." She then asks, "Does the United States have jurisdiction over anyone who uses a hosting provider in the Eastern District of Virginia? What about over any company that uses PayPal?"²² Indeed, these are the sorts of questions prompted by super-jurisdiction.

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

Michael Geist, an internet law professor at the University of Ottawa, observes that, indeed, "All Your Internets

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

CLOUD SURVEILLANCE

The various technical components that enable global communication—the server, network, and client—all lend themselves to surveillance. *Access Controlled*, an MIT Press handbook on internet surveillance and censorship, states that “the quest for information control is now beyond denial.”²⁵ The book describes the so-called security-first attitude toward internet governance, driven by a fear of terrorist threats and concerns over child pornography on the internet. This allows the state to police the internet without any restrictions. As the authors assert in their conclusion: “The security-first norm around Internet governance can be seen, therefore, as but another manifestation of these wider developments. Internet censorship and surveillance—once largely confined to authoritarian regimes—is now fast becoming the global norm.”²⁶ Indeed, if the lawsuit brought by the Electronic Frontier Foundation (EFF) against the telecommunications corporation AT&T is any indication, the US government seems determined to expand its access to electronic communication. The EFF’s star witness in the case was Mark Klein, a former AT&T technician who claimed in 2002 to have seen the creation and ongoing use of a private room where the National Security Agency (NSA) had “set up a system that vacuumed up Internet and phone-call data from ordinary Americans with the cooperation of AT&T.”²⁷ Klein said the system allowed the government full surveillance of not only the AT&T customer base, but that of sixteen other companies as well.²⁸ The US government dismissed the case against

the telecommunications provider, asserting the state-secrets privilege rule. The government also dismissed cases against itself and other telecom companies that assisted with similar endeavors including Sprint, Nextel, and Verizon.²⁹ If the allegations are true, according to *Access Controlled*, “they show that the United States maintains the most sophisticated Internet surveillance regime.”³⁰

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

Journalists regularly criticize (or praise) the US government for its ability to spy on “Americans.” But something essential is not mentioned here: the US government’s ability to spy on everybody else. The impact of US surveillance is potentially as vast as the impact of the cloud itself. An FBI representative told CNET about the gap the agency perceives between the phone network and advanced cloud communications. The representative described the FBI at risk of “going dark,” and mentioned national security to show how badly it needed cloud wiretapping,

revealing that the state-secrets privilege—once a democratic anomaly, now a routine invocation—will likely be used to shield such extensive surveillance powers from public scrutiny.

Users' concerns about internet surveillance increased with the proposed Stop Online Piracy Act (SOPA), which was introduced into the US House of Representatives in late 2011. How the government would police SOPA became a real worry, with suspicions that the enforcement method of choice would be standardized Deep Packet Inspections (DPI) deployed through users' internet service providers—a process by which the “packets” of data in the network are unpacked and inspected.³³ Through DPI, law enforcement would detect and identify illegal downloads. In 2010, before SOPA was even on the table, the Obama administration sought to enact federal laws that would force communications providers offering encryption (including e-mail and instant messaging) to provide law enforcement with access to unencrypted data.³⁴ However, it is worth noting that encryption is still protected as “free speech” by the First Amendment of the US Constitution—further complicating, but not likely deterring, attempts to break the code. One way of doing so consists of surrounding encryption with the insinuation of illegality. In 2012, the FBI distributed flyers to internet-cafe business owners requesting them to be wary of “suspicious behavior” by guests, including the “use of anonymizers, portals or other means to shield IP address” and “encryption or use of software to hide encrypted data.” In small print, the FBI added that each of these “indicators” by themselves, however, constituted lawful conduct.³⁵

COERCIVE PATERNALISM

Real-name requirements by cloud-based social networking platforms such as Facebook and Google+ explicitly attack anonymity and pseudonymity online, affecting the fundamental rights of political speech; not even freedom of speech, but the premise of the act of speech. Real-name

directives require users to register with a service using the name that is in their passport. The reasons given by cloud services for this are vague—perhaps for fear of sounding too openly authoritarian. The preferred route, instead, sounds like fatherly advice. Facebook claims that it has a real-name policy “so that you always know who you’re connecting with,” while Google wants to make sure “that the people you want to connect with can find you.”³⁶ These explanations gesture toward an idea of normative social arrangements, requiring that you use the same name that you’d use among your friends, family, or coworkers. Alexis Madrigal points out a certain irony in the Google+ real-name requirement: “The kind of naming policy that Facebook and Google Plus have is actually a radical departure from the way identity and speech interact in the real world. They attach identity more strongly to every act of online speech than almost any real world situation does.”³⁷

Cloud providers such as Amazon use real-name registration as a mechanism for accountability. Though Amazon still allows users to use a “pen name,” the use of a trademarked “real name” is advertised as having the ability to “potentially increase your reputation in the community” as a retailer, seller, or reviewer.³⁸ Some see the real-name badge as a step toward “fixing their flawed [and] exploitable review system” for book reviews. These reviews are notoriously dominated by biased “anonymous” users, often thought to be (and sometimes proven to be) adversary authors, family members, or publishers.³⁹ Though Amazon’s reason for promoting real names is more explicit than that of Facebook and Google+, one can imagine the marketing benefits of a synchronized real-name system between social media and retail websites, and the connection that such a synchronicity might have with the government. Such requirements can be seen as aligned with plans by the US to introduce a universal “trusted identity” or “Internet ID” system for US citizens, a commission that the White House granted to the US Commerce Department in 2011. According to US Cybersecurity Coordinator

Howard Schmidt, the effort entails creating an “identity ecosystem” for the internet.⁴⁰

Cass Sunstein, the Obama administration’s former chief adviser, has argued for government policy against the spread of online “rumors.” One of the most persistent rumors was that President Obama had been born in Kenya and therefore holds his presidency illegally.⁴¹ This rumor was also one of the most virulently effective political weapons of the Republican Right, if only, as the architectural theorist Keller Easterling has argued, because rebuttal required repetition of the original rumor. Sunstein believes that certain properties of the internet are geared toward the uninformed circulation of rumors and conspiracy theories. With so-called echo chambers and cybercascades, one-sided opinions can often spread rapidly across the network without encountering meaningful opposition. Supposedly reliable reporting by professional journalists now has to compete with—and often gets surpassed by—blog posts, Facebook updates, or tweets. The effortless ability for all internet users to live on a “Daily Me”—a news diet catered to fit and maintain an individual’s already established set of beliefs—would result in a fragmentation of the general public into factions that no longer expose themselves to views held by others. Sunstein claims that under such fragmentation, “diverse speech communities” are created “whose members talk and listen mostly to one another.” He states:

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

Sunstein is concerned that rumors may impair the effectiveness of government and that they may undermine its legitimacy. In early 2008, he and a coauthor published a

paper on conspiracy theories based on the 9/11 attacks. Sunstein suggested that “government agents (and their allies) might enter chat rooms, online social networks, or even real-space groups and attempt to undermine percolating conspiracy theories by raising doubts about their factual premises, causal logic or implications for political action.”⁴³

Nowhere is a government’s coercive stance toward the spread of online rumors as clear as in China. In Beijing, regulations were put forth that required users to register on social media sites with their “real name identities” by March 2012—such regulations are comparable to the policies already embraced by Facebook and Google. Sites including Sina Weibo, one of the country’s largest microblogging websites, began implementing these regulations, and users were forbidden from making statements against the state’s honor, or statements that might disrupt civil obedience.⁴⁴ Around the same time, social media sites across the country flared up against the ouster of political leader Bo Xilai from the Communist Party. The Chinese police swiftly detained six people and shut down sixteen websites over “rumors” surrounding the incident, including claims that military vehicles were entering Beijing.⁴⁵

CLOUD AS A POLITICAL SPACE

The increasing prominence that cloud-based internet services, social media, and VoIP technologies now enjoy over legacy tools of communication is apparent in how they enable new, virtually cost-free forms of organization. For social movements relying on collective action, this factor has proven to be key. Unsurprisingly, when social media platforms are suddenly “switched off,” their ability to organize can be severely affected. Facebook, in the wake of nationwide anti-austerity protests in the United Kingdom in February 2011, deleted profiles of dozens of political groups that were preparing to take part in further protests. By doing so, the company effectively disabled political activism that had, for obvious reasons, moved its

coordination to the cloud. The reason for Facebook's actions is still not known and likely never will be. All the social networking behemoth could utter to justify its behavior was cryptic technospeak; a Facebook spokeswoman said that profiles had "not been registered correctly."⁴⁶ In 2010, UK Prime Minister David Cameron and other conservative politicians met in London with Facebook founder Mark Zuckerberg. Their admiration was mutual.⁴⁷

Rebecca MacKinnon, a former CNN reporter and cofounder of the citizen media network Global Voices, asserts in her book *Consent of the Networked* that "we cannot understand how the internet is used unless we first understand the ways in which the internet itself has become a highly contested political space."⁴⁸ This not only applies to the internet, but also to the cloud. The rights to a free flow of information, freedom of expression, and freedom from censorship have been described as a compound right to "internet freedom." Indeed, Wael Ghonim, the Google executive referenced at the start of this chapter, said that unhindered access to the internet will liberate a society. The problem with Ghonim's statement is that he didn't really mean the internet but the cloud. He meant Google, YouTube, Facebook, and Twitter; platforms hosted in the United States—not grassroots or distributed mesh networks. The US-based cloud certainly provides useful, free tools for protesters to organize and coordinate. It can help make worldwide oppression and conflict visible. But Facebook and Google are not the content and substance of these political struggles, they are, at best, a few tools.

On January 21, 2010, then US Secretary of State Hillary Clinton gave a widely cited speech on foreign policy and freedom. In it, she proclaimed something quite implausible for a US official: "As I speak to you today, government censors are working furiously to erase my words from the records of history."⁴⁹ Indeed, the speech singled out authoritarian regimes as the single biggest threat to the internet and the path of human progress that leads from it. Evgeny Morozov commented on Clinton's

"anachronistic view of authoritarianism." As Morozov explained, "I didn't hear anything about the evolving nature of Internet control (e.g., that controlling the Internet now includes many other activities—propaganda, DDoS attacks, physical intimidation of selected critics/activists). If we keep framing this discussion only as a censorship issue, we are unlikely to solve it." He went on to criticize the double standard the State Department advertised with regard to online anonymity:

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

Still, the definition of internet freedom remains relatively opaque. One example of this ambiguity is provided by the Global Internet Freedom Consortium (internetfreedom.org) that aims to "inform, connect, and empower the people in closed societies with information on a free Internet."⁵¹ A campaign by Free Press called "Save the Internet" (savetheinternet.com) divides internet freedom into three clearly defined categories: net neutrality (wired and wireless); strong protections for mobile phone users; and public use of the public airwaves and universal access to high-speed internet.⁵² Net neutrality is the principle that all data on the network is to be treated equally by governments or by network service providers. Coined by the legal scholar Tim Wu in 2003, network neutrality was meant as a benchmark for the open nature of the internet—an "end-to-end" infrastructure unbiased toward its content and

thus enabling transparent innovation. The internet, then, is “a platform for a competition among application developers. Email, the web, and streaming applications are in a battle for the attention and interest of end-users. It is therefore important that the platform be neutral to ensure the competition remains meritocratic.”⁵³

Network neutrality applies to a decentralized architecture, with clearly divided roles between ISPs, broadband service providers, content providers, and services and applications on the network. It constitutes a de facto gentlemen’s agreement through a joint, economic (thus depoliticized) interest in innovation and fair competition. Indeed, political speech can, in this view, also be considered part of a competition—one of ideas. Venture capitalist Joi Ito expressed this view in 2003 when he wrote that such a competition of ideas “requires freedom of speech and the ability to criticize those in power without fear of retribution.”⁵⁴

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

The terms of service of any cloud-based provider are a far cry from a binding agreement to net neutrality; they allow plenty of space for “cloudy bias.”

For example, in August 2012, Apple banned Drones+ from its App Store. This app, developed by New York University student Josh Begley, provides aggregated news

about US drone strikes in Pakistan, Yemen, and Somalia, and it includes a Google map on which the strikes are marked. The app also notifies the user whenever a new drone strike has occurred and says how many casualties it had produced. Crucially, the information collected by the app is already public and freely available through various other sources including the *Guardian’s* iPhone app. Apple demonstrated its cloudy parody of network neutrality in the ever-changing reasons it gave for rejecting Drones+. Apple had a problem with the Google logo appearing on the Google map. In July, the company stated in an e-mail, “The features and/or content of your app were not useful or entertaining enough, or your app did not appeal to a broad enough audience.” By August, Apple changed its mind. The app contained “content that many audiences would find objectionable, which is not in compliance with the App Store Review Guidelines.” Indeed, the company eventually concluded that Drones+, which does not show users any images of actual drone-related bloodshed, was “objectionable and crude.”⁵⁶ The *New York Times* wondered how on earth it could be that “the material Apple deemed objectionable from Mr. Begley was nearly identical to the material available through the *Guardian’s* iPhone app. It’s unclear whether Apple is treating the two parties differently because the *Guardian* is a well-known media organization and Mr. Begley is not, or whether the problem is that Mr. Begley chose to focus his app only on drone strikes.”⁵⁷

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

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

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

The political, legal, and jurisdictional consequences of the cloud are slowly becoming apparent—right at the moment we are most unlikely to withdraw from it. The cloud is just too good. We won't stop using our iPhones, iPads, Androids, and Kindles. PayPal is still our frenemy. Happily captives of the cloud, we will tweet our criticisms of it, and Facebook-broadcast our outrage over its government backdoors. But the story is not over yet. Will the anarcho-libertarian roots of the internet kick back at the cloud's centralized architecture, or are they forever over-

run by it? Has the cloud assumed its final form, or is there still a time and place for surprises?

II

Is the future of the world the future of the internet?
—Julian Assange⁶⁰

The cloud is the informational equivalent to the container terminal. It has a higher degree of standardization than earlier forms of 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. The internet was like a wholesaler for all types of information and media formats. As Milton Mueller notes in his book *Networks and States*, all media that “used to be delivered through separate technologies governed by separate legal and regulatory regimes, have converged on the Internet protocols.”⁶¹ In the cloud, such “digital convergence” goes even further: data becomes more effectively and thoroughly harvested, analyzed, validated, monetized, looked into, and centrally controlled than on the open internet.

SPACE OF FLOWS

In the last twenty years, we have been able to describe borderless information society in terms of its physical territories and infrastructures. These are also the places where people live, where resources are finite, and where climate, energy, food, and many other conditions determine what the world looks like. 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.”⁶²

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.”⁶³ As legal scholars Jack Goldsmith and Tim Wu note in their book *Who Controls the Internet?*, beneath “formless cyberspace” rests “an ugly physical transport infrastructure: copper wires, fiber-optic cables, and the specialized routers and switches that direct information from place to place.”⁶⁴ James Gleick describes the network’s data center, the cables, and the switches as “wheel-works,” and the cloud as its “avatar.”⁶⁵ The cloud presupposes a piece of land where data centers can be built. It presupposes an environment stable enough for its server farms to run securely, 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, it is precisely for this reason that the infrastructure safeguarding its permanent availability is monstrous in size and scope. According to research carried out in 2012, the cloud uses about thirty billion watts of electricity worldwide—roughly equivalent to the output of thirty nuclear power plants. About one-quarter to one-third of this energy is consumed by data centers in the United States. *New York Times* journalist James Gland says that “a single data center can take more power than a medium-size town.”⁶⁶

A data center is a building that houses computer servers. The servers are powered by electricity and cooled by water. Usually a data center looks like a large, flat, windowless box: a Walmart without a logo. To its users,

the cloud seems transparent—always available, hanging in the air, on screens, in waves, appearing and disappearing; a “shapeless cyberspace.” Yet at the core of this ghost dance is pure materiality; a steel and concrete building dependent on electricity, water, and people. If the enormous, energy-slurping data factories are the cloud’s true form, then the “space of flows” recalls the medieval castle, the treasure chest, or the military base. It recalls political and military conflicts that have occurred on the territory 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.⁶⁷

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 that “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.”⁶⁸

A RENAISSANCE OF THE STATE

The early internet, in the hearts and minds of idealists, was something of an anarchic, dreamlike place. John Perry Barlow, cofounder of the EFF, prefigured the cyber-utopian position in his 1996 manifesto, "A Declaration of the Independence of Cyberspace." In it, Barlow asserts that the network and its inhabitants are independent from the old-fashioned rules and regulations of territorial states:

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.⁶⁹

Barlow's cyberspace was a commons, a "world that all may enter without privilege or prejudice," and one where "anyone, anywhere may express his or her beliefs"—a world beyond authority. His ideas have resonated. The independence of the internet from central control remains a strong driving force for many of its users, engineers, and for civil rights activists. Saskia Sassen says 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."⁷⁰ 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."⁷¹

One place where the rhetoric of borderless freedom of information is most pervasive is in the cloud. The world's most powerful information companies have inserted strands of cyber-utopianism into their mission statements. These tech giants talk about themselves as heartwarming charities. Every billionaire CEO is his own private Dalai Lama. Pseudo-liberal gibberish of assumed universal validity permeates the junkspace of mission statements, annual reports, and TED (Technology, Entertainment, Design) talks especially when it comes to the cloud. Microsoft wants to help everyone around the world "realize their full potential." Facebook aims to give "people the power to share and make the world more open and connected." Skype makes it "simple to share experiences with the people that matter to you, wherever they are." And Instagram, bought by Facebook, envisions "a world more connected through photos."⁷²

Cyber-utopianism may have never been fully realized. But online anonymity, cryptography, Peer-to-Peer (P2P) file sharing, TOR (The Onion Router) bridges, Bitcoin cryptocurrencies, offshore data havens, public key privacy, bullet-proof hosting, and other such phenomena, would not exist without it. 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."⁷³ 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."⁷⁴ The data haven is a spatial form that, at least in theory, enables the evasion of sovereign power, while establishing an enclosed territory on the face of the earth. The data haven was once 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, during the early 2000s dot-com boom, home to the servers of HavenCo, a startup providing offshore data hosting beyond the reach of any jurisdiction.⁷⁵ One of HavenCo's early-day angel investors is the current MIT Media Lab director Joi Ito, who declared himself "a great fan of the concept," still in 2002.⁷⁶ Sealand's fragile, 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, who is currently a professor of law at the University of Maryland, feels skeptical about Sealand and HavenCo: "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."⁷⁷

Grimmelmann also questions HavenCo's effectiveness as "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." As he rhetorically asks, "In an age of YouTube, BitTorrent, and the darknet, who needs HavenCo?"⁷⁸ Yet Sealand was also a flagship for the internet's anarcho-libertarian movement. After the ailing principality had put itself up for sale on eBay, the P2P BitTorrent site the Pirate Bay tried to buy it, proclaiming to offer citizenship as a serious escape strategy.⁷⁹

Froomkin, in a lecture at the Oxford Internet Institute in June 2012, sketched an arresting and slightly dystopian diagram for the internet's future. Froomkin thinks the vision of a deterritorialized internet outside of anyone's control was believed by governments around the world, including but not limited to dictators and authoritarians. His diagram presents a dialectic between two opposing visions.⁸⁰ On one side, there is the "Cyberpunk Dream." Most of the cyber-utopian (Barlow-style) outlook is listed

on this side. On the other side, there is "Data's Empire," which has most of the cloud's standardization and control. Two cloud-based services, YouTube and Twitter, still remain part of the Cyberpunk Dream, presumably because of the pivotal role both services play in online activism. Froomkin describes Data's Empire as a "renaissance of the state"—a reemergence of state power over the network. Froomkin suggests that this renaissance happened in an unwitting response to the mirage of cyber-utopianism; the anarchic internet, after all, existed mostly in the imagination of its advocates.

The end of the first dot-com era coincided with the 9/11 attacks, where the state encountered a new, borderless enemy: al-Qaeda. Subsequently the United States redefined its own national security as a global, all-encompassing surveillance paradigm with European governments following meekly in its wake. The internet has turned out a victim of this move.

THE LEGAL VOID OF "LIKE" VS. "LAW"

Cyber-utopians, in hopes of evading the state's grasp, assumed that its coercive powers would be constrained by jurisdictional and constitutional limits. As Grimmelmann concisely put it, "HavenCo simultaneously thumbed its nose at national law and relied on international law to protect Sealand."⁸¹ The possibility for states to evade the law, of going rogue, or extrajudicially handling 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 essay "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."⁸² 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."⁸³

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."⁸⁴

And indeed, it isn't. A mere thirteen years after Boyle's "Foucault in Cyberspace," the controversial whistleblowing website WikiLeaks found itself to be the living proof of this when it became embargoed by US companies.

WikiLeaks began in 2006 as a web platform for the release of leaked documents. It is practically uncensorable since its hosting was set up in multiple countries, its data thus protected by laws in 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 Iceland's bankrupt Kaupthing Bank, the site ran a discouraging note for its adversaries demonstrating 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."⁸⁵

On receiving a complaint from Kaupthing, a Reykjavík court silenced Iceland's national broadcaster, RÚV. RÚV was planning to break the story on television. So instead of airing the story, the TV host pointed viewers to the WikiLeaks website where they could see the docu-

ments for themselves—to great social and political effects in Iceland. WikiLeaks evaded the gag order by hosting its information offshore. 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 released 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 that are processed by the Wau Holland Foundation based in Kassel, Germany. Wau Holland reportedly 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.⁸⁶ The crowdfunding went through conventional payment channels: PayPal, an online payment system owned by eBay, Western Union, VISA, and MasterCard (the latter two corporations virtually dominate the credit card market). One could say that the WikiLeaks donations relied on a private cloud of intermediary, US-based companies. WikiLeaks claims that funding after the release of the first cables peaked at an all-time high of eight hundred thousand individual donations in a single month.⁸⁷

After the release of Cablegate, WikiLeaks' Sweden-based servers were hit by a vast DDoS attack. The attack compelled the organization to hire cloud hosting with Amazon Web Services (AWS) in the United States. On December 1, 2010, a day after this move, AWS kicked WikiLeaks from its servers, marking the effective beginning of a pan-industrial, state-corporate embargo.⁸⁸ Amazon's decision was prompted by an aggressive call to arms from Joe Lieberman, a US Senator for Connecticut and chairman of the Senate Committee on Homeland Security. Lieberman urged American enterprises to stop providing services to the whistleblowing site, even though he had no legal authority to enforce

this.⁸⁹ His words amounted to nothing more than a personal view. Lieberman took the position of both accuser and judge, stating, "It sure looks to me that Assange and WikiLeaks have violated the Espionage Act."⁹⁰ The result was that WikiLeaks' vital infrastructure fell through as key companies withdrew themselves. EveryDNS, a California-based domain name registry, stopped providing access to the wikileaks.org domain name server so that the site could only be accessed if a user entered its IP address into a web browser. MasterCard, PayPal, VISA, and Western Union ceased to process WikiLeaks donations. Apple removed a WikiLeaks iPhone app from its store. Together, all of these actions amounted to an extra-legal embargo for which the organization was unprepared. Yochai Benkler, a professor of law at Harvard University, examined the embargo in detail in a 2011 article. Benkler asserted that though the embargo came from multiple sources, it was issued 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."⁹¹

Boyle asserts 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."⁹² The distinction is significant. It captures 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 (believably suggesting to be) capable of triggering a potentially devastating set of cascading effects in case his friendly suggestions are not followed up. Power then is to personally govern

the pressing of LIKE buttons, deciding on life or death, just like the Romans decided the fate of the gladiators; Facebook's original LIKE symbol—a thumbs up—has its roots in ancient Rome. Arguably, Lieberman clicked the DISLIKE button (thumbs down) on WikiLeaks, causing a wave of consequences resulting from his private, social, and network power, backed by his position of senator. 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 an actor within a nexus of sovereign, economic, and social power, leveraging some of those in service of his goals."⁹³

The financial embargo against WikiLeaks 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."⁹⁴ It remains, however, questionable as to whether the order against Valitor will actually restore funding to the site. 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."⁹⁵ Sveinn Andri Sveinsson, a lawyer for DataCell, is less pessimistic. Sveinsson was quoted calling the victory a "good day for the freedom of expression."⁹⁶ Still, the case was decided as a matter of contractual rather than constitutional law.⁹⁷

The situation for WikiLeaks became worse when Assange was accused of (but not charged for) sexual misconduct in Sweden. Interpol issued a Red Notice for his arrest. A two-year standoff between Assange and UK prosecutors ensued. After he lost his appeal against his extradition to Sweden at the Supreme Court in May 2012, Assange escaped to the Ecuadorian embassy in London where he applied for (and received) political asylum. Assange claims he did not want to evade Swedish accusations but rather a possible extradition to the United States on presumed charges of espionage.⁹⁸

The way Assange's legal team fought his extradition, followed by his move into the Ecuadorian embassy, are remarkably consistent with WikiLeaks' multi-jurisdictional hosting model. The case brought forward deep ambiguities in the treaties regulating extraditions, prompting Tiina Pajuste to argue in the *Cambridge Journal of International and Comparative Law* that the UK Supreme Court's decision displayed "a fundamental mistake" in its judgment.⁹⁹ At the embassy, Assange's life appears to have become fully equivalent to that of WikiLeaks' data. The Ecuadorian outpost is like an offshore internet server, beyond the grasp of Western powers. Indeed, there was widespread anger when Britain briefly threatened Ecuador to annul the status of its embassy's premises.¹⁰⁰

Assange himself frequently deploys chessboard metaphors when talking about jurisdiction in a multipolar world. As he 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."¹⁰¹

If WikiLeaks and Assange make one thing clear, it is that the jurisprudential assumptions of cyber-utopianism 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 being 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 conceptions like network neutrality, internet freedom, and freedom of expression—despite their key democratic value—do not 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.

THE DISSENT OF THE NETWORKED

In early 2011, Birgitta Jónsdóttir, an Icelandic Member of Parliament, found out that the US DOJ had subpoenaed Twitter for her account information. Jónsdóttir was in the DOJ's crosshairs for her alleged involvement in the making of *Collateral Murder*, edited and produced by WikiLeaks in Iceland in 2010.¹⁰² The video documents the shooting of unarmed civilians in Baghdad by a US Apache helicopter crew. All Twitter Inc. user information is stored on servers in the United States. They are accessible to US law enforcement with or without a court order. The DOJ's subpoena was issued to Twitter in regard to Jónsdóttir and the computer experts Jacob Appelbaum and Rop Gonggrijp. It came with a gag order: Twitter was forbidden to talk about it with anyone. However, Twitter's lawyer challenged the gag order with a judge and successfully lifted it. 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."¹⁰³ Her message was retweeted over one hundred times.

The problem is that in the cloud, there is no equivalent to a "home." Cloud computing may sometimes seem

to mimic or emulate elementary privacy concerns.¹⁰⁴ Amazon Web Services—the same company that extrajudicially boycotted WikiLeaks—boasts that it errs on the side of “protecting customer privacy,” and is “vigilant in determining which law enforcement requests we must comply with.” It heroically says: “AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis.”¹⁰⁵ 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. And the possibility of revolving-door interests between business and government can’t be ruled out either. Amazon’s current, Washington, DC-based Deputy Chief Information Security Officer is reported to possess a “distinguished career in federal government security and law enforcement.”¹⁰⁶ A cloud service provider’s own security staff may in various ways—socially, geographically, and through expertise—already be intimately connected to the very law enforcement agencies whose requests it is supposed to scrutinize.

As journalist 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.¹⁰⁷

This, then, reflects an outdated idea of a third party’s role in a subpoena. At the time when the law was 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.”¹⁰⁸ 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, and 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.”¹⁰⁹

Jónsdóttir, Appelbaum, and Gonggrijp tried to find out if companies other than Twitter 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.¹¹⁰ 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."¹¹¹

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 as 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 United States to silence the truth as a means of maintaining power. She wrote that the DOJ's subpoena constituted a "hack by legal means."¹¹²

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, #d0xcak3.¹¹³ 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 with the hacktivist collective Anonymous at a given point in time. WikiLeaks tweeted that it was now time for Twitter to move its servers offshore.¹¹⁴ 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."¹¹⁵

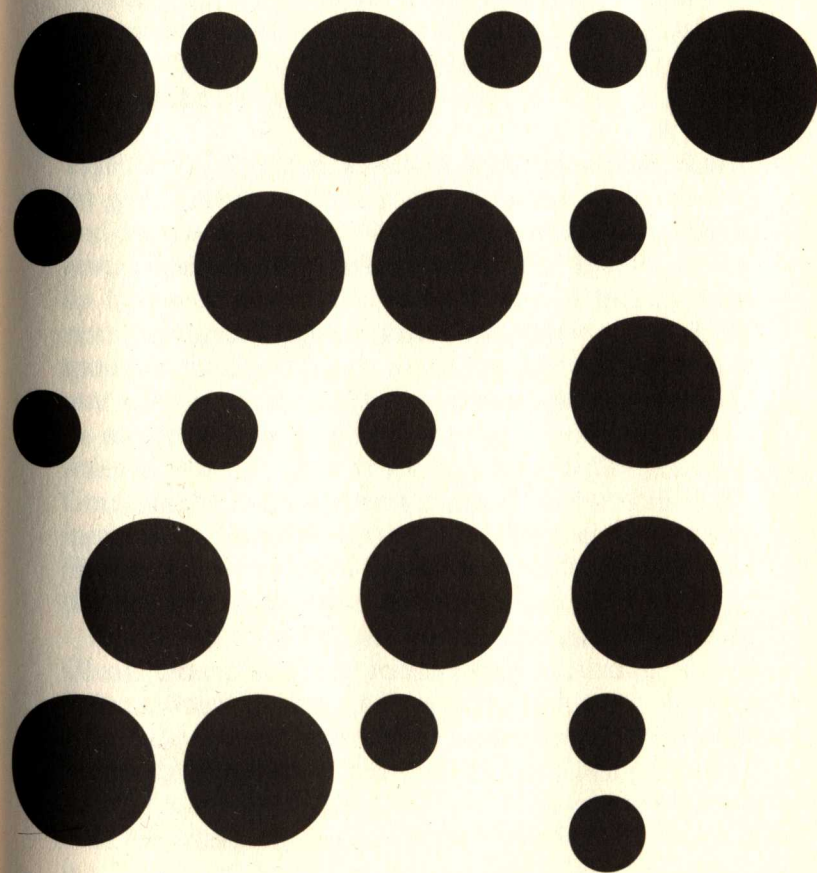
Groys's "future power" over the network is unlikely to pose direct, legal limits on free speech. Instead, like in the WikiLeaks embargo, it directly affects the material basis of those who speak. One is tempted to think of the ways in which the FBI pursued hacker collectives Anonymous and LulzSec after their DDoS attacks on MasterCard and VISA. The FBI fully exploited the real-world frailties and vulnerabilities of the hackers, who presented themselves as superheroes online. But they were not in reality. The authorities made no qualms about the question of whether or not Anonymous and LulzSec's actions entailed a form of "civil disobedience." They were treated as criminals, 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.¹¹⁶ One of the group's most prominent members, who used the pseudonym of Sabu, was apprehended by the FBI and turned into an informant. *New York Magazine* wrote: "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."¹¹⁷

Ars Technica added, "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."¹¹⁸ The *Guardian* completed this story: "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."¹¹⁹

The space of flows is anti-smooth. It looks like a data center and the coal plant that powers it. It looks like 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 crash landing from the digital into the real world is hard. It comes with a cruelty and intensity we have not even begun to understand. Along these lines, we might grasp an emerging political geography of information, resources, and infrastructure. 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."¹²⁰ Indeed, the world is lumpy and nondigital enough for us not to easily draw conclusions. This story is not over yet. Tomorrow's clouds are forming.

ALL TOMORROW'S CLOUDS



The quest is on for a relocalized internet that we all can understand as our own. An internet, or a cloud, that is able to resist surveillance because it is collectively governed by its citizens.

This design question is not without problems. It comes down to reimagining our social contract with each other, with the state, with corporations, and with democracy itself.

A Massive, Expanding Surveillance State With Unlimited Power And No Accountability Will Secure Our Freedom by Hans Christian Andersen.
—pourmecoffee, Twitter post¹

Violence arms itself with the inventions of Art and Science in order to contend against violence.
—Carl von Clausewitz²

Basically, infrastructure is the technology that determines whether we live or die. Your infrastructure will kill you—if it fails, you fail.
—Smári McCarthy³

THE INTERNET BEGAN as a place too complicated for governments to understand. It ended up, in the second decade of the twenty-first century, as a place that *only* governments seem to understand. At least, they think they do. US spy agencies sift through the cloud to find out if the next Osama bin Laden is posting cat videos online. In response to the obvious lack of privacy every global internet user now enjoys, some European countries try to cash in on secure web hosting and watertight e-mail—ironically referred to by one security researcher as “bullshit made in Germany.”⁴ Vladimir Putin fortifies Russia’s digital walls, incarcerates (then “pardons”) Pussy Riot, nationalizes its Facebook alternative, VKontakte, and offers asylum to the NSA whistleblower Edward Snowden.

Aided in no small part by the courage of journalist Glenn Greenwald and documentary filmmaker Laura Poitras, Snowden has single-handedly changed the way we see the internet by merely revealing how the NSA sees it: as a structure whose full-on infiltration and militarization is the agency’s only goal. The NSA’s coercive power over the internet is not so much a nuclear weapon as it is a bioweapon. Snowden’s files—released after an earlier episode of groundbreaking disclosures spearheaded by Chelsea Manning and WikiLeaks—are sparking East-

West divides that are starting to resemble a new Cold War fault line. For some years, Ecuador has hosted Julian Assange in its London embassy as a political refugee, while it is rebranding itself as a “haven for internet freedom.”⁵

These and other ripple effects can be viewed as part and parcel of what Benjamin Bratton calls a “geopolitics of the cloud.”⁶ Unsurprisingly, there is a deep divide between the perspectives of various national governments, often claiming or (erroneously) believing to be able to restore national (e.g., “your”) sovereignty over data space, and the transnational, borderless character of the network itself. The central political design question, however, is not about whether these structures are national or transnational in scope. It is simply about how they are decided upon; how they are governed.

CONNECTING THE DOTS

Before becoming director of the NSA, Keith Alexander was heading the US Army Intelligence and Security Command. In this position, he commissioned an architecture firm to model his office, the so-called Information Dominance Center, after the control room of the Starship Enterprise. Referencing *Star Trek* proved crucial to Alexander’s political advocacy for surveillance. *Foreign Policy* notes that “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.”⁷

Alexander has currently stepped down from his position at the NSA. It was a taxing year at the helm of the spy boat. Before Snowden gave thousands of top-secret documents to the press, Alexander used to publicly appear in the full attire of a four-star general. He alternated his uniformed appearance with other outfits. For example, he wore an Electronic Frontier Foundation (EFF) T-shirt at Def Con, an industry-sponsored hacking conference. In his talk Alexander urged digital troublemakers to join the ranks of the NSA. The cynicism of his seemingly trivial

dress code is that the EFF is a US-based, nonprofit organization that scrutinizes government surveillance and advocates civil rights—the violation of which is Alexander’s day job. Nevertheless Alexander pleaded that his agency operated lawfully and transparently. “We are overseen by everybody,” he said.⁸ But that was in 2012. Then came the revelations. Alexander changed his public relations tactics accordingly. From then on he appeared as an obedient bureaucrat, serving the nation to avoid the next 9/11. At Def Con 2013, he presented the NSA’s mission as “connecting the dots.” This means collecting and analyzing everyone’s data, everywhere, up to three degrees of separation away from a suspected terrorist.⁹ Typically, someone who has fifty friends on Facebook has about 1,334,978 friends of friends of friends.¹⁰ Columbia University law professor Eben Moglen calls it plainly, “spying on humanity.”¹¹ The NSA boasted that its surveillance had thwarted fifty-four terrorist attacks; however, that claim lacked any factual evidence, according to research by the independent online journal *ProPublica*.¹²

Simultaneously entrepreneurial and totalitarian, the NSA exerts a strange form of digital parenthood over the internet. A Platonic necessary evil, protecting an abstracted version of freedom and democracy from an abstracted version of terrorism. Alexander—who plotted to ruin the reputation of Islamic radicalizers by publicly revealing their porn-site visits¹³—is, after all, a pseudo-amicable human incarnation of neo-Stalinism. The agency uses corruption with martial agility. “Overseen” by secret FISA courts, it has built a giant, data-slurping behemoth facility in Utah—a Walmart holding everyone’s indeterminate digital past. When asked by Congress if the NSA collected data on millions of Americans, 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

The NSA also wielded its power to influence and alter the technical and security standards on which the internet

itself relies, including the pseudo-random number generators used by the microchips of our computers. These generators create strings of numbers needed to encrypt information. By having them put out a lesser variety of numbers, decryption becomes easier, especially for someone in the know about just how much less varied the output is. Yochai Benkler asserts that 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, while it, in the president’s own awe-inspiring legalese, 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 International Monetary Fund (IMF) and the World Bank.²⁰

I POWER

What type of power is at work in the NSA’s military infiltration of the internet and its users, and to what and to whose end does it work?

In 1957, Robert A. Dahl succinctly defined the concept of power as follows: “A has power over B to the extent that he can get B to do something that B would not otherwise do.” This bare-bones definition does not specify *how*, indeed, a “probable pattern of future events” as Dahl called it, will be established.

The most direct manifestation of power is coercive force or “hard power.” The sword of the sovereign. A police batallion threatening a group of demonstrators to withdraw. Imprisonment. A gun pointed at you, or even the knowledge or fear that your opponent *has* a gun. A bribe. Blackmail. Situations where you, B, face the direct, negative consequences from your possible noncompliance with A. “Soft power,” by contrast, lets B do what A wants because B deems it attractive (thus beneficial) to be like A. This is the power of seduction, persuasion, image, and brand. The outcome of soft power is a change of behavior of B under the influence of A, where no act or threat of force was necessary.

At the end of the 1980s, consumer brands like Coca Cola, McDonalds, and Levi’s had become signposts of America’s imminent victory over the Soviet Union, symbolizing the defeat of Communism; the military hard power that drove the nuclear arms race and the Cold War had been replaced by the lure of American brands. It was not fear of a deadly strike but image, celebrity, music, movies, and consumer products—*desire*—that finally toppled the Union of Soviet Socialist Republics.

REVOLUTIONS

Fast-forward about twenty years: free webmail, chat, and social networking are seen by many as the Coke and McDonalds of the internet age—signposts of freedom in zones of authoritarianism. Tools of free communication, promises of connection, friendship, and more: symbols of a new order. Hillary Clinton’s calls for an open internet and for freedom of information in 2010 and 2011 are promotional phrases for the US cloud that facilitate these

freedoms in exchange for data. Clinton stated: "Refusal to support politically-motivated censorship will become a trademark characteristic of American technology companies. It should be part of our national brand. I'm confident that consumers worldwide will reward firms that respect these principles."²¹

The target of the cloud's liberating potential isn't any particular regime or empire, but simply any place under "authoritarianism."²² Identification of the US social media cloud with protests against authoritarianism indeed amounts to a brand-name-dropping exercise. For example, the general term "Twitter revolution" applies to no less than five successive periods of political disruption: the 2009 unrest in Moldova following the elections, the 2009 and 2010 protests in Iran around the elections, the Tunisian Revolution of 2010 and 2011, the Egyptian Revolution of 2011, and the Euromaidan Revolution in Ukraine starting in 2013. Three of these Twitter revolutions—Iran, Tunisia, and Egypt—double as "Facebook revolutions."

Indeed, "internet-enabled social mobilization" has become a lame excuse for commentators, journalists, and technology prophets to foreground the digital technology used in political protests over their content and subject matter. As one Egyptian protester tweeted, "We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world."²³ This is more than enough information for those who lack any real interest in, and understanding of, the difficult histories and political intricacies of places and their inhabitants; they can simply focus on the social media.

In April 2014, the Open Society Foundation—George Soros's vehicle for benevolent geopolitical change—sent out a tweet: "It started with a Facebook message." The tweet linked to an article by the Ukraine-based journalist Mustafa Nayem. Nayem claimed that the 2013 events on Maidan Square in Kiev were triggered by a post he had written on Facebook. Maidan, crucially, triggered not just a "revolution" but also a potentially disastrous imperialist

response by Russia. Yet Nayem wrote that the ousted, Kremlin-backed president Viktor Yanukovich is too old and doesn't understand Facebook.²⁴

Such "analysis" of protests in authoritarian countries, written sometimes by and more often *for* tired Western liberals, is supposed to contain a deeply reassuring subtext: that despite the all-out crisis of Western influence and/or relevance in the various regions where conflict or unrest is at play, all is well because they are still using *our* tools, *our* technology, *our* standards of communication.

All of this would be pure soft power for the US cloud if it weren't for the fact that the network connection alone, even when provided for by US companies, has nothing to do with the United States. David Singh Grewal calls the power inherent to communication standards "network power." As he explains:

For instance, consider international sentiment about the United States. You can think of something like, "people having good feelings about the United States." A certain kind of positive branding is there—and that is at the heart of American "soft power"—but it may suffer major reversals very quickly, as we have seen in the last eight years with the Bush administration. What is interesting, by contrast, about network power, is that the world can end up deciding that it hates the American model, and America can effectively suffer a complete bankruptcy in its soft power account, and yet, the world is still poised in significant parts to emulate the United States—because our standards are becoming the platform on which people can connect on a global level, independent of whether they have decided to like us. [...] I think a great many of the forms of globalization are driven by something other than direct political control of foreign territory, and can better be understood on a network power, not a soft power, model.²⁵

For Clinton, the fact that the world is using US social media adds to the country's soft power account: it brings about a greater appreciation and legitimacy of the United States. For Grewal, there is no such connection, because things people say on the communication platforms that the cloud provides may have nothing to do with what they think of the United States.

At the same time, the US cloud is quickly expanding beyond social media into all areas where big data—large-scale information collection and analysis—is critical. The data being gathered is not about people's opinions; it is their behavior that is being mined. Alexander tried to convince the public that through gathering massive amounts of "hard" metadata, the NSA will figure out where the "soft" changes are located; changes on the level of content, people's opinions, their subjectivity. But massive metadata collection far exceeds the relatively quaint category of content as a power base. Stewart Baker, a former general counsel of the NSA, has asserted that "metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content. [...] It's] sort of embarrassing how predictable we are as human beings."²⁶ General Michael Hayden, Alexander's predecessor at the NSA, went even further: "We kill people based on metadata."²⁷ The NSA's power is thus about the military infiltration and exploitation of the world's behavioral patterns.

Google is a protagonist in the business side of this endeavor. Once a refreshingly nerdy search engine, it is now an infrastructural empire adorned with geopolitical soft power jewels and tons of cash, and a radar to predict flu epidemics. Google sees itself with appropriate grandeur. In 2012, its vice president for marketing announced that Google's emotional value was now key: "If we don't make you cry, we fail."²⁸ Top executives Eric Schmidt and Jared Cohen subsequently published *The New Digital Age*, a geopolitical manifesto on making life easier. Cohen, who directs Google Ideas, is also a fellow at the

Council for Foreign Relations and a former adviser to Clinton and Condoleezza Rice. He and Schmidt believe that a succession of technological revolutions will change life on Earth forever. As Evgeny Morozov cynically comments in his (hilarious) review of *The New Digital Age*: "First, a 'smart-phone revolution,' a 'mobile health revolution,' and a 'data revolution' (not to be confused with the 'new information revolution') are upon us. Second, 'game-changers' and 'turbulent developments' will greet us at every turn. Your hair, for example, will never be the same: 'haircuts will finally be automated and machine-precise.'"²⁹ In his own review of the tome, written for the *New York Times*, WikiLeaks' Julian Assange finds that in this book-length TED talk, "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."³⁰

Indeed, every transaction on a Google server is an event under American jurisdiction, making a joke of soft power. The United States can subpoena most information that in some way exists inside or passes through its network infrastructure. As discussed previously, a form of "super-jurisdiction" has emerged with the US-instigated shutdown of Hong Kong-based Megaupload.com and a plethora of other websites, and with the DOJ's subpoena of Twitter (and other social media) accounts belonging to WikiLeaks supporters. In fact, the small print of Clinton's 2010 internet freedom speech spells out bad news for some disruptive actors: "Those who use the internet to [...] distribute stolen intellectual property cannot divorce their online actions from their real world identities. [...] Our ability to bank online, use electronic commerce, and safeguard billions of dollars in intellectual property are all at stake if we cannot rely on the security

of information networks. Disruptions in these systems demand a coordinated response by governments, the private sector, and the international community.”³¹

In addition, it has been suggested that the DOJ’s subpoena of WikiLeaks-related Twitter users was a case of so-called parallel construction, meaning that information that *had already been obtained* through surveillance—using the secret Section 215 of the Patriot Act, which authorizes bulk collection—was retroactively “legally” retrieved to become admissible in court, while leaving the laws and sections that enabled the spying unexposed. The glitches that suggest such parallel construction are hard to dismiss.³²

Without a doubt, the United States’ global communication standards have network power. Yet, the territorial bases of these standards bind global subjects to key aspects of US hard power—predominantly, its judicial regime and its pervasive surveillance, by which the United States can effectively seek to control events on foreign soil, effecting, as A, a change in the behavior of B.

US martial law, with all of its cleverly designed back doors and gray areas, permits the government to create a dragnet around the cloud and the internet. The network power of standardization is a key enabler of the “hard power” surveillance state and its metadata-based alternative world map, where targets are IP (network) addresses. Morozov is only half-ironic when he predicts the ultimate consequence of every other object in the world, previously dumb and now smart, becoming chained up into an “internet of things” with surveillance back doors everywhere. He writes, “Now that Google has acquired Nest, the manufacturer of smart objects for the home, NSA might access your bedroom as easily [as] it can currently access your inbox.”³³

II ABSTRACTION

The Slovenian philosopher Slavoj Žižek argued in 2011

that the era of cloud computing spells out a “tation of the ‘general intellect.’” Žižek wrote:

Users today access programs and software maintained far away in climate-controlled rooms housing thousands of computers. To quote from a propaganda-text on cloud computing: “Details are abstracted from consumers, who no longer have need for expertise in, or control over, the technology infrastructure ‘in the cloud’ that supports them.”

There are two tell-tale words here: abstraction and control. In order to manage a cloud, there needs to be a monitoring system that controls its functioning, a system that is by definition hidden from the end-user. The paradox is thus that, as the new gadget (smartphone or tiny portable) I hold in my hand becomes increasingly personalized, easy to use, “transparent” in its functioning, the more the entire set-up has to rely on the work being done elsewhere, on the vast circuit of machines which coordinate the user’s experience. In other words, for the user experience to become more personalized or non-alienated, it has to be regulated and controlled by an alienated network.³⁴

Any technological process involves a degree of abstraction. In the cloud, this abstraction does not merely consist of a user not understanding the details of a program’s technical functioning. The abstraction implies a relationship where the compliance of the user with this abstraction benefits the provider to the point where A gets B to do something it wouldn’t otherwise do—which was Dahl’s definition of power. While transparency used to be about revealing the component parts of a system and their relationships, nowadays we think of “transparent design” as merely a simple, minimalist container. Rather than enabling transparency, it is an aesthetic that to some extent works as a legitimizer, perhaps similar to what the New York-based trend

forecasting agency K-HOLE has coined as “normcore”—a deliberately chosen nonidentity, or, according to Microsoft researcher and MIT visiting professor Kate Crawford, fashion’s answer to big data. Normcore’s solution is to no longer be obliged to differ.³⁵ As K-HOLE tweeted in early 2014, “Normcore finds liberation in being nothing special, and realizes that adaptability leads to belonging.” According to others, it amounts to “mock turtlenecks with Texas and Patagonia windbreakers; Uniqlo khakis with New Balance sneakers or Crocs and souvenir-stand baseball caps.” Stylist Jeremy Lewis has called it the “exhaustingly plain” look of people like Steve Jobs and Jerry Seinfeld.³⁶

Whereas transparent, minimalist abstraction legitimizes the cloud’s hidden control mechanisms, and while today’s digital nomads camouflage themselves as transparent physical nobodies under normcore right at the middle of the Gauss curve where we find the average tourist in midtown Manhattan, abstraction is also a power relationship working through and over distance. Indeed, a distinct way of looking at power bypasses the more common distinction between hard and soft, and instead runs along a binary of proximity and distance. Hannah Arendt reasoned that out of the barrel of a gun comes violence, not power. As soon as the gun is removed, everyone will continue their activities. Not physical force itself but its mere threat is often enough to force B into compliance with A.

Power, then, can increase with a greater distance between A and B. For example, the sound of military aerial drones communicates the potential of hard power; and the aerial dread of a hovering “cloud” seems to be not entirely coincidental as the human relationship with the skies overhead is one of subjugation and abstraction at the same time. Drones are a cloud but in a purely negative form. What in cloud computing is thought of as a *user* and in surveillance as a *suspect*, is considered a *target* by the drone operator. Apart from their strikes, the mere presence of drones overhead can cause people to develop mental illnesses, as the report *Living Under Drones* has testified.³⁷ A drone’s

power is a looming latency, subordinating the longevity of human experience to long-lasting abstraction, and control.

This is true also from the perspective of the drone’s eye view. As a pilot flies his Reaper over Waziristan from the comfort of an air-conditioned shipping container in Nevada, that pilot’s power increases incrementally through a distance to the target. The one who pulls the technological strings here has a higher price tag attached to his life. He is guaranteed to physically survive the strike, which indeed makes a drone pilot the opposite of a kamikaze pilot or a suicide bomber.

Arendt relates the principle of abstract power to the Greek mathematician and physician Archimedes, who hoped to establish a point of observation that would be impartial to the observed, like a cloud. As she wrote:

Without as yet actually occupying the point where Archimedes had wished to stand, we have found a way to act on the earth as though we disposed of terrestrial nature from outside, from the point of Einstein’s “observer freely poised in space.” If we look down from this point upon what is going on on earth and upon the various activities of men, that is, if we apply the Archimedean point to ourselves, then these activities will indeed appear to ourselves as no more than “overt behavior,” which we study with the same methods we use to study the behavior of rats.³⁸

In 2002, following the footsteps of Arendt, the researcher Diana Saco wrote that “technology has provoked a reorientation of our way of thinking that is itself premised on a new kind of spatial practice: on taking up a standpoint that is abstracted from our interactions with others in a shared, public space.” As Saco explains, “This shift in spatial position and perspective has a number of significant consequences. First, it implies an intersection between knowledge and power (actually, force) that, on Arendt’s

URBAN
PLANNING
HIGH
RISE

reading, lay at the heart of Archimedes' philosophy: drawing from the simple mechanical properties of levers, Archimedes inferred that 'our power over things grows in proportion to our distance from them.' What he proposed, then, was a form of abstract knowledge, about things at a distance, that would enable a form of abstract power: the ability to act on bodies at a distance."³⁹

The internet has become so vastly essential to life itself that it is eligible to be a platform for almost anything; from all of our daily needs, to our innermost feelings and relationships to others, to physical desire, culture, literature, music, art, and various kinds of geopolitical force fields including hard power, soft power, network power, and abstract power. The writer Brian Kuan Wood argues that the obsession some have developed with the physicality of the internet—its cables, data centers, and other architectural and tangible shapes—is merely a decoy that distracts us from the internet's essential transformation of our affective and emotional lives.⁴⁰ The geopolitics of the cloud are not limited to the territorial traces of an intangible universe of information, like the remnants of armored vehicles in a war zone; the transformation of economies, of livelihoods, of forms of human cooperation, and the far-reaching breakdown of any and all structure that preceded the internet, is part of this too.

Out of any process of fundamental transformation of the man-made world evolves a settlement where some govern and others don't. The question as to who governs the internet—the cloud, the giant abstraction that carries our information—is a question worth asking in the full knowledge that the answer *isn't* "the King."

THE SOLUTION IS THE PROBLEM

Evgeny Morozov identifies the attitude by which many technologists approach the problems of society as "solutionism."⁴¹ Solutionism, says Morozov, hides the political dimension of the questions that confront society by readily disguising them as technological problems.

Consequently it brings them under the control of programmers, systems managers, software entrepreneurs, and hordes of policymakers volunteering to help. As a result, political, social, and civil issues eventually tend to all become questions of big data.

There are, however, problems for which no iPhone app can find an answer, and one of them is: Who governs the app?

Who rules the internet on whose behalf, as ridiculously archaic as the question may sound, is a political and legal issue of foremost importance to everyone who uses it. It is no longer about net neutrality. According to Milton Mueller one of the problems with internet governance is whether it is "the people interacting via the Internet or the territorial states constructed by earlier populations in complete ignorance of the capabilities of networked computers" who should be "sovereign."⁴² 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."⁴³

The network grapples with the opposite of scarcity. It bathes in an overabundance of apps and services that thrive on the deterritorialization, expropriation, and extortion of life and data. Benjamin Bratton calls this "microeconomic compliance."⁴⁴ It is probably the most convenient model of exploitation that ever existed.

People who use the internet live in territories; they have citizenship. But this feedback loop doesn't activate their political agency. What, after all, really is the connection between both? Is it perhaps the "indifference, weariness and exhaustion from the lies, treachery and deceit of the political class," as Russell Brand aptly called it?⁴⁵ On the other hand, Snapchat, Instagram, and other multi-billion-dollar-valued apps are vehicles of affective lure—or of "ghostmodernity," as the artist Jesse Darling described

concept of perfect security

↓
is it's not its own type of solutionism?

it.⁴⁶ They are endlessly more attractive and performative than our everyday complicity with the machinery of representative politics. No one talks about revolution—only about Twitter or Facebook revolutions because they make good headlines and relate to our smartphones. We have an exhausted political machine on the one hand—“citizenship” gets molded into tiresome, backward rituals of participation. On the other hand, we have the splendor and immediacy of affect and connection via our digital tools, which are built on microeconomic and geopolitical compliance. It seems an easy win for the latter. But we have no collective governance. People have not considered the internet as a democratically governable structure and are completely fine with it. Yet the working model of self-government that we do have—parliamentary representative politics—is, at best, an ailing patient. And aren’t the two somehow related? Isn’t a *structural lack* of democratic governance over the internet somehow mirroring the *democratic deficit*—the fundamental shortcomings and bore-doms of parliamentary democracy?

Carne Ross, a former British diplomat and founder of the diplomatic advisory group Independent Diplomat, argues for a social contract for the internet. “The balance between the individual and state needs to be more fundamentally altered,” writes 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.”⁴⁷ Ross’s proposal is neither technical nor bureaucratic. It is political in the most personal sense. Its problem is that it draws on decision making and on enforcement structures that don’t exist yet. As stated in Ross’s book *The Leaderless Revolution*, which promotes benign anarchism, people may be able to work out their own polity better than any government can. Indeed, it is unclear how a social contract for the internet 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. It is equally unclear how to achieve such a balance without a voluntary (and extremely unlikely) retreat of the powers that be.

A version of a social contract between citizens versus governments and corporations was demonstrated in 2012 when internet users across the world successfully prevented the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) from coming into effect.⁴⁸ “Social contract” here means the basic possibility for people to bargain against the powerful and to prevent adversarial measures that threaten a common resource.

A social contract for the internet requires governments and corporations to accept its political inconveniences. It requires them to radically cut back on surveillance. It requires them to legalize leaks, cyber protests, and online civil disobedience as legitimate political expressions. As noted previously, UK- and US-based hacktivists in 2010 and 2011 used DDoS attacks to target private corporations that held up a corporate embargo against WikiLeaks. Those responsible were hunted down and tried as criminals; the analogy between hacktivism and nonviolent civil disobedience was lost on the system, its politicians, and its judges. Digital equivalents to strikes and blockades are framed as crimes against property and profit. Cyberprotests, and the state’s response to them, express the complete *absence* of any verifiable and binding social contract between the internet and its users. The nonexistence of structural agreement or a form of collective governance leads to a giant puzzle of partial solutions.

SCARCITY AS A POLITICIZER

There are different routes than the social contract. The activist group Nullify NSA has taken on the task of disabling the NSA by shutting off the water supply to its data centers. The fascinating proposition is, at minimum, a stark reminder that the ability to spy and store data ultimately depends on local conditions, including the

availability of electricity and cooling. Thus, any internet operation depends upon and interacts with the living environment—the territory and its resources. Michael Boldin, the executive director of the Tenth Amendment Center and a Nullify NSA representative, explains: “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.”⁴⁹

Nullify NSA is on the libertarian-conservative Far Right. Its ideas are, as Boldin says, “backed up by the advice of James Madison.” He continues: “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.” Nullify NSA has all of the Right’s typical rigor and determination even while it seeks to be “transpartisan” in its efforts. Boldin emphasizes this: “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.”

The group observes the interdependency between the digital and the physical domains plainly and accurately. 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.” He

goes on to analyze the data center distribution of the NSA 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.

After all, the NSA’s weak point may be its insatiable appetite for electricity rather than its breaches of the constitution. This leads us to the under-investigated relationship between data centers and their territories.⁵⁰

III THE POSSIBILITY OF AN ICELAND

The recently coined term “data sovereignty” describes two distinct trends in hosting models. The first is an increasing tendency of nation-states to make networks fit within their national border. The only advantage of these national networks is that they are not directly under the auspices of the NSA—though it is unlikely that serious spying can or will be stopped. “Boutique” data sovereignty is an economic strategy in the wake of global surveillance. “E-mail made in Germany” is now hot—user data is protected by the supposedly watertight German privacy laws.⁵¹ Swisscom, Switzerland’s telecommunications company—majority-owned by the government—is creating a secure Swiss cloud, aspiring to levels of security and privacy US companies can’t guarantee.⁵² Luxembourg’s and

Switzerland's wealth freeports for property in transit—mostly expensive art—now also offer data storage.⁵³

② The second definition of data sovereignty is more personal. Every internet user should own all of their online data. Jonathan Obar criticizes the idea but largely for the wrong reasons. He claims that personal data sovereignty is fallible because we have big data now: giant, algorithmic pools of personal information, connections, locations, and behavioral patterns that determine, for example, what ads are targeted to a user or which connections are offered to him or her by the system. Obar says:

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.⁵⁴

The saying goes that if your only tool is a hammer, all problems look like nails. Data may well 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—the credit default swaps of the cloud are as unsustainable as the subprime mortgages that triggered the 2008 financial collapse. The NSA participates in the corporate feeding frenzy of big

data as much as cloud providers do. There is, in this light, nothing strange about wanting more personal control over one's information. A clear model for it is still missing, but a 2011 paper by US Naval Postgraduate School students suggests 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."⁵⁵ First of all, to break down the abstraction of the cloud, the internet needs to be more localized.⁵⁶

A recent case in point where the boundaries between a politics of locality and a politics of the network are being traversed is Iceland—a sparsely populated island in the North Atlantic that has come to look like one of the places in the West where political alternatives get a chance, if rarely. On July 5, 2008, John Perry Barlow, the EFF's founder, gave a speech at the Reykjavik Digital Freedoms Conference. The talk was titled "The Right to Know."⁵⁷ Barlow took his audience on a journey beginning at the wordless prehistory of Homo sapiens; he ended by venturing a somewhat unexpected update of the data haven. Iceland, Barlow said, could become a "Switzerland of Bits"—a sanctuary for digital freedom, a safe harbor for transparency, a fortress for the Enlightenment. Cyberspace, for Barlow, was both global and local: "The more local it becomes, the more global it becomes."

A mere three months after Barlow's talk, all of Iceland's banks collapsed. Relative to its size and population, it was the largest banking crisis ever suffered by a country.⁵⁸ Iceland's recovery from the financial crisis became a case of national democratic and ethical reform. A twenty-five-strong Constitutional Assembly rewrote the constitution, together with a crowdsourcing effort that introduced thousands of comments and hundreds of concrete proposals from citizens directly into the legislative process.⁵⁹ On June 16, 2010, Iceland's parliament cast a unanimous vote for IMMI, the Icelandic Modern Media Initiative. IMMI packaged the best freedom of speech, source protection,

and libel protection laws as they existed in various countries.⁶⁰ And while the idea for the Switzerland of Bits came from Barlow, WikiLeaks had a crucial influence on IMMI's legal architecture as the whistleblowing platform ran hosting agreements with ISPs in the various countries where such laws already existed separately. IMMI compiled the laws from these countries and introduced them to Iceland.

The 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.⁶¹ At the same time, McCarthy is involved in the development of MailPile, a secure, cloud-based e-mail application designed to be an effective competitor to Gmail and a collective decision-making software in the political lineage of "liquid democracy"—a form of delegative democracy used by Pirate parties. As a founding member of the Icelandic Pirate Party, much of McCarthy's work takes place on the razor edge between 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."⁶²

James Grimmelmann 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."⁶³

In Iceland, the data haven has evolved to a more advanced plane that includes policy, software, coding, and advocacy, removing itself from the anarcho-libertarian free-for-all. The internet, here, is an experiment with democracy as much as with the environment; many of Iceland's data centers are climate-neutral, running on geothermal energy. Then, the development of online tools for communication, coordination, and democratic decision making falls within IMMI's scope. The programmer and consultant Eleanor Saitta, who is the organization's technical director, explains:

The Internet is a \$11 trillion US 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.⁶⁴

A networked politics of locality springs from a space of exception created both within the context of Iceland as a community and a geography and from the internet as a human construction:

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.

The design agenda for the future of the internet seems straightforward: become a post-institutional, non-state

actor and start with political reform right where you live. The idea of a localized internet anticipates increasing overlaps between digital and physical social structures. Saitta states:

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.

SERVERS IN THE CLOUDS

The possibility for a network—centralized, decentralized, or distributed—to override jurisdiction and state power is an early dream of the internet, shaped and inspired by cypherpunk science fiction. What was once thought to be “the internet,” a deterritorialized space among a world of nation-states, is saturated today with the spatial implications of borders, jurisdictions, and sovereignty. Increasingly, new approaches to guarantee internet freedom are

based on eluding these spatial implications of a (perhaps always) reterritorialized internet.

In recent years, the Pirate Bay, a famous Sweden-based P2P BitTorrent sharing service, had access to its service blocked in various countries. Its three founders were sentenced on charges of enabling the violation of intellectual property by facilitating illegal downloads. At the time of writing the case has been brought to the Swedish Supreme Court, but the final sentences are still pending. Apart from being a file-sharing site, the Pirate Bay is also a kind of living manifesto for the cyber-anarchic. It has issued various viral memes, had planned to buy the Principality of Sealand, and in March 2012 made an unexpected announcement. The Pirate Bay announced it would start hosting content from airborne drones to evade law enforcement and copyright claims.⁶⁵ Their 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" that has built a set of wireless, connected drones operating like a mobile darknet.⁶⁶ 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."⁶⁷

Though some of the Pirate Bay's servers reportedly now operate out of a secret mountain lair,⁶⁸ its Low Orbit Server Stations (LOSS) are a drone concept acting like a satellite and redirecting traffic to a secret location. Though the plan is, conceptually, a call for a deterritorialized internet space, it seems somewhat oblivious to the legal implications of the localized server that would still

remain. The Electronic Countermeasures project, on the other hand, is based equally on deterritoriality as well as locality. The architect Liam Young, a 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.⁶⁹

critical theory internet!

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 than that.

THE TYPO-SQUATTING STATE

An island can be made to exist either by carving out law or by not legislating at all. State power works both ways. Negatively, some jurisdictions lack effective control over their borders and a centrally administered rule of law—they are "lawless" zones in various states of anarchy, poverty, decay and crime."⁷⁰ In international relations it has become customary to apply a set of benchmarks to measure statehood. For example, a state needs to be able to control its

MAINTAINED DETOUR
BY WESTERN IDEAS → A TYPE OF CONTROL

borders, have a centrally administered rule of law (even if that entails dictatorship), and to a considerable extent a state needs to comply with customary practices in "international society" in order to fit in. 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 indicate a state authority that is not substantially fulfilling these criteria. Since the introduction of the term in the 1990s, various failed states have emerged, many of them in Africa—Somalia, Yemen, Sudan, and Mali are a few examples. The designation of "failure" seems legitimate when applied to the raging civil wars and violent conflicts that have terrorized the continent, even when taking into account that many of these are the by-products of colonialism and ruthless exploitation. But the term "failure" also points back to the political process, ideology, or entity that hands out the designation. In other words: one man's failure is, potentially, another man's mode of governance. 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."⁷¹

Failed states have their own political model; a "failure" to produce outcomes compliant with accepted norms can be regarded 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 law. They are outside of the international system and of world politics. Insofar as they are still partially inside that system,

IS THIS
"CONSTRUCTIVE" → IN A (RE)BUILDING SENSE?

ALT

inherent, really?
by being on earth?

they may present new opportunities for internet practice, new sovereignties for network hosting, and new areas for nomadic infrastructure. Grimmelmann asserts 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.⁷²

A country like Cameroon represents a borderline case. There is digital infrastructure in the country, but its statehood appears to descend into failure anyway. In 2008, Ozong Agborsangaya-Fiteu, a senior program manager for Africa at Freedom House, 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."⁷³ About a year later, internet-security firm McAfee unveiled that Cameroonian websites were the most dangerous in the world for users—even more so than ones from Hong Kong. Cameroon boasts an 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 by one character from the ubiquitous ".com," the top-level domain extension—hence Cameroon's success in building popular Potemkin website destinations of misspelled URLs. Apparently Facebook.cm has led users to a highly

offensive porn ad.⁷⁴ Is this boom in scam internet destinations some sort of data-haven by-product? Grimmelmann comments: "Yes, you could put it that way: I'm reminded of the Eastern European virus-writing 'industry.'"⁷⁵

IV PEOPLE BEFORE CLOUDS

In *The Truman Show*, Jim Carrey plays Truman Burbank, the unwitting protagonist of a real-life sitcom. After he discovers that the world he inhabits is a stage, Christof, the show's director or "creator" played by Ed Harris, makes an emotional appeal to convince Truman that the reality *out there* is no better or more real than the 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, 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 the former/previous NSA director, Keith Alexander, as similarly semi-comforting as the creator's view? Alexander begins almost every other sentence with the phrase, "from my perspective." He doesn't really 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 him, countless potential "cyber" threats. Alexander's NSA is about "connecting the dots" and "saving lives." It's like a virtual ambulance rushing to the rescue of the digitally wounded. He brags about his agency's "tremendous capabilities" as if he were a middle-aged computer-systems manager boasting about his Windows server. How do we escape the custody of this virtual father figure and those waiting to take over once he steps down? How do you effectively liberate a society that has the internet? To begin with we need to get rid of the deceptive gibberish of technocracy. We have become 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 internet are right, but they shouldn't forget that we also need the right politics to use them. Technology's spectacle needs to be unleashed to further the ends of those who wish for a way of their own, rather than to help those who merely wish to 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 encrypt all of 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. On the other hand, the very argument for total encryption is the flipside of solutionism; it asks technology to solve a political problem. Encryption alone can't heal the internet. Apart from these two strands is a third possibility: a localized internet that wields the double-edged sword of political and technological reform, and one that saves the network from being a looming abstraction manipulated by four-star generals, politicians, and 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 technomanagerial matrix and look each other in the eye.

New politics, new technologies, and new imaginations are needed—all three of them, in abundance. Democracy

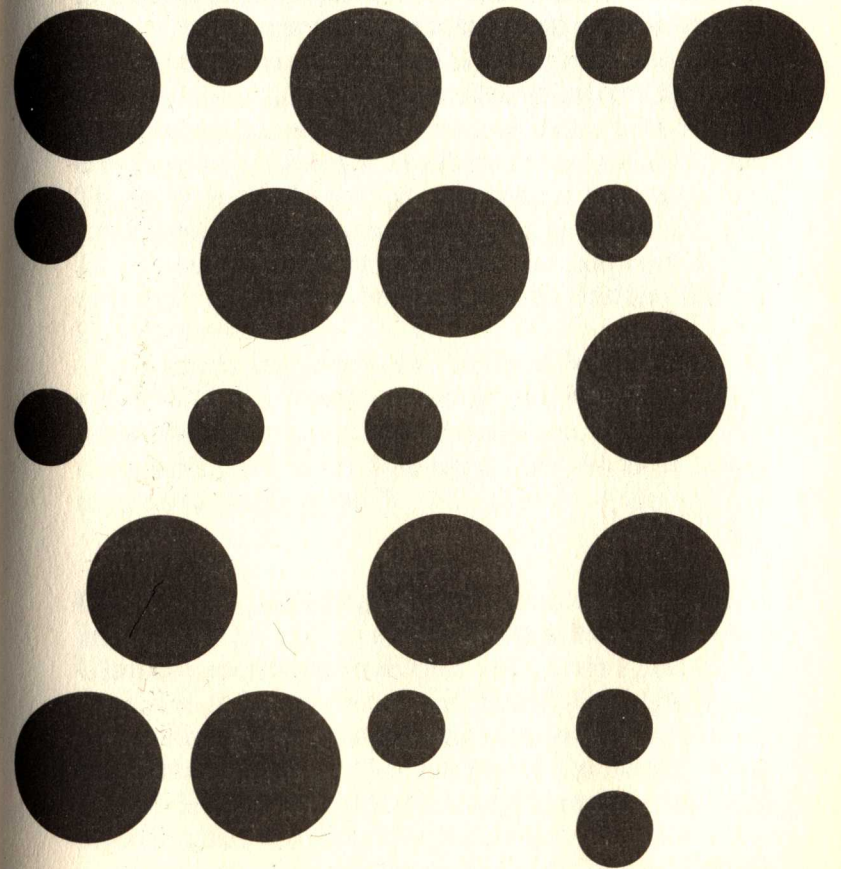
potential /
epitaphical

actual /
concrete

except
we have
lost a
sense
of
"perfect
security"

and people need to come before clouds. Drinking water needs to always be prioritized over spying. Life itself is the enemy of surveillance.

WHEN PIXELS BECOME TERRITORIES



Black transparency holds Western governments that claim to be transparent accountable. So what about Russia? All that is glamorous, absurd, and surreal shines in Vladimir Putin's geopolitical endgame; his postmodern absolutism is immune to the criticisms of black transparency because it doesn't attempt any claim to transparency. In spite of this, some of the fantastical elements in Russian power and dissidence may provide future activism with the radiant hues that the clinical neutrality of mainstream transparency is dearly missing.

IT'S JULY 17, 2014.

Malaysian Airlines flight 17 from Amsterdam en route to Kuala Lumpur is shot down over eastern Ukraine by Moscow-backed rebels of the self-proclaimed Donetsk People's Republic. All 298 passengers die in the crash. An emotional letter from a Dutch father who lost his daughter goes viral on the internet. It begins with the words, "Thank you, Mr. Putin."¹

The victims' bodies are flown to the Netherlands. The military ceremony that awaits the bodies at Eindhoven air base is solemn, and staged. Its message is that though these were civilian deaths, this is no civilian crash. But as Russia's largest trading partner, second only to China, the Dutch government does not want to damage its delicate economic ties, leaving it to others to make accusations. The interventionist French philosopher Bernard-Henri Lévy, happy to volunteer for the job, writes in the *New York Times* that Vladimir Putin is the perpetrator, and condemns France for building aircraft carriers for the Russian navy.

Sanctions on Russia are imposed by the West. In winter 2014, the Russian economy dips into a crisis. The ruble crashes. In an address to the nation, Putin cites the Czarist-era philosopher Ivan Ilyin: "He who loves Russia should wish her freedom."²

PROXIES

Ukraine is a geostrategically vital zone. Pipelines carrying Russian gas and oil stretch through its vast territory. Ukraine depends on these fossil fuels, as do a host of EU countries. A former part of the Soviet Union, Ukraine is the world's third-largest grain exporter and has a substantial military force. At the breakup of the Soviet Union it inherited the world's third-largest nuclear weapons arsenal, which was dismantled in 1996.

The Ukraine conflict is a geopolitical deadfall. On one side stand the Ukrainian government and its army, supported by Europe and the United States. Ukraine's 2004

Orange Revolution, which successfully overturned the crooked election of Russian vassal Viktor Yanukovich, was reinforced by a host of Western NGOs and governments, including the United States. The 2013 Maidan protests, named after Kiev's central square, erupted after a fraudulently reelected Yanukovich backed out of talks with the European Union, instead seeking closer ties to Moscow. Following Yanukovich's final exit, a democratically elected pro-Western government was installed in Kiev.

Putin resorted to brute force and invaded the Crimean Peninsula, a Ukrainian territory, under the pretense of protecting the area's Russian-speaking population. The takeover led to the separation of Crimea from Ukraine, and the formation of the Republic of Crimea, a federal subject of Russia. Since the annexation, Russia has militarily intervened in the eastern part of Ukraine as well, though in a more covert manner. In and around the eastern Ukrainian cities of Donetsk and Lugansk, backed by a large Russian-speaking population, new sovereign territories have been declared by rebels under the command of seasoned Russian war veterans. These rebels, whom the Ukrainian government calls "the terrorists," hope to establish Novorossiia (New Russia), a Czarist-era land division that includes eastern Ukraine. In Russia, belief in these operations is emboldened by unrelenting anti-Western propaganda. Moscow has previously intervened in a similar manner in post-Soviet border areas such as Abkhazia and Transnistria, the difference being that this time, high strategic interests are at stake for the West. Ukraine becomes a proxy conflict reminiscent of the Cold War—yet different from that era in a few important ways.

The idea that states can exert "natural rights" over other territories on the basis of some revered historical past has been around as long as nations themselves have existed.

As Benedict Anderson reminds us: "Romanovs discovered they were Great Russians, Hanoverians that they

were English, Hohenzollerns that they were Germans—and with rather more difficulty their cousins turned Romanian, Greek, and so forth. On the one hand, these new identifications shored up legitimacies which, in an age of capitalism, scepticism, and science, could less and less safely rest on putative sacrality and sheer antiquity."³

In the conflict between Ukraine and Russia, something other than sheer antiquity is at work. While the war comes at the cost of many civilian casualties, the destruction of cities, and the displacement of refugees, a key part of it is fought on an entirely different territory than Ukraine or Crimea: on internet server farms, many of which are located in the United States. The entire conflict is energized, recreated, and postproduced through social media, image manipulation, fiction writing, and role playing. The seemingly local nature of the conflict is supplemented by a permanent overlay of cloud-based social platforms, such as Facebook, Twitter, Wikipedia, and VKontakte. A greater Russia is made out of the pixels of YouTube videos and anti-Obama memes, which then gets projected back onto the territory.

What distinguishes the 2014 Ukraine crisis from earlier cases of Russian imperial intervention is precisely that this one has a detailed visual surface. That so much of it seems to happen in the open, and that every video, every image, every social media account is a trap door.

Planetary-scale computation, to cite a phrase coined by the design theorist Benjamin Bratton, is transforming geopolitics in ways we are yet to understand, and so it may be that cloud computing lifts the entire Ukraine conflict out of the simple binaries in which it gets served to the world, changing parts of its political geography.⁴

As Bratton explains:

The geopolitical architectures that we have inherited from the Treaty of Westphalia, the Mountbatten Plan, Bretton Woods, etc. were, first of all, "design" decisions and were based on

particular political, discursive, even topological understandings of the world. To recognize them as such, it becomes obvious that the “alter-globalization” we imagine for the years to come must take different forms and formats than those through which we currently govern. In time, those forms may be based upon rather different relations to whatever becomes of things like sovereignty, nation, narrativity, geography, polity. These are the material design problems of the next century. [...]

Planetary-scale computation has both deformed and distorted traditionally modern geometries of jurisdiction. It is also producing new territories of jurisdiction in its own image. Unusual and as-yet-unnamed networked patterns of informational and urban subjectivity are already shifting the geopolitical landscape.⁵

HIROSIMA NAGASAKIEVA

After the Crimean annexation, Russia appointed thirty-three-year-old Ukrainian chief prosecutor Natalia Poklonskaya to handle the “Nazis”—basically, Moscow’s Ukrainian opponents. The Russian English-language television and internet channel RT made the young and beautiful Poklonskaya central to its broadcasting under the tagline, “She annexes your heart.”⁶ In one awkward news program where the hosts were visibly uncomfortable with their autocue, RT announced that Poklonskaya, the bombshell “prosecutie,” had spontaneously risen to internet fame in Japan.⁷ Allegedly without any form of central coordination, anime artists were drawing her portrait after a video went viral on the YouTube channel YouTubi News on March 13, 2014.⁸

YouTubi News appeared out of nowhere days before the Poklonskaya video was released, raising the question where the first few of its hundreds of thousands of viewers came from. How exactly did the video become an infor-

mation cascade if YouTubi News had no other videos and no subscribers?

The most widely distributed and well-known example of the anime prosecuties is a drawing by “Itachj,” or Itachi Kanade, a Vietnamese amateur illustrator using a fake Japanese name.⁹ Itachj calls the piece “Quick draw Natalia Poklonskaya (Наталья Поклонская).”¹⁰ It is the only drawing in the entire portfolio with a political resonance, and with the specific addition of Cyrillic characters in the caption. All other drawings seem like generic anime characters.

On March 19, after the “eruption” of the meme, Itachj writes in the comments below the drawing: “It’s just a quick drawing when I was bored, I dont think it become popular.”¹¹ However, the drawing doesn’t look like a hasty sketch. It turns out that Itachj can produce such characters on commission:

Please send a note to me here or you can add my

Yahoo account: wp_93@yahoo.com.vn

Payment throught PayPal only!

Email: huunganpham@yahoo.com.vn

I draw only anime style about:

— Anime girl

— Fanart

— OC

Hentai, Ecchi is OK ^_^

About Price:

— Only character (full body): 20 USD/PIC

— Only character (half body): 15 USD/PIC

— Character + Background : 25~30 USD (it base on the difficult) ^_^¹²

Itachj includes a link to a YouTube video of Poklonskaya, posted on a user account awash with videos of the Ukrainian conflict, Crimea, Putin, and the Russian military. The channel’s name is “Hirosima Nagasakiava.” Its profile picture is a photo of Japanese pop singer Ayumi

Hamasaki. Indeed it takes a certain sense of morbid humor to forge Russia and Japan together by making the bombed cities Hiroshima and Nagasaki sound like a Russian female name. There is a sense of honesty here too, however: Hiroshima Nagasaki—*the bizarre identitarian construct of a fictional Russian-Japanese YouTube pop icon—wasn't meant to be seen, let alone approved of, by the liberal viewers RT tries to court. Its full-on dark humor and fantasy reveal a geopolitics of fate that could only emerge from Russia.* They announce a deceptive world after transparency, which is fully aware of its own misery. RT's "Japanese viral meme," which is based on the Hiroshima Nagasaki video that resulted in the first anime drawing of Poklonskaya, becomes pure astroturf. Quasi-grassroots inventions were meticulously crafted and prepared to appear spontaneous, when in fact some if not all of the anime drawings may have been commissioned. The Vietnamese illustrator may have innocuously included the YouTube link below his post, while asserting that the drawing was just a quick sketch.

In late July 2014, Itachj announces his retreat from anime drawing.¹³

NYASH MYASH

On April 15, 2014, "Nyash Myash," a fanatically nationalist music video featuring Poklonskaya, is posted on YouTube. At close to thirteen million views in early August 2014, it is by far the most popular of all prosecutive clips. The video is a self-made music track lip-synched to Poklonskaya, intertwined with fragments of anime that show her fighting demons. The chilling chorus goes, "Power blood, Nyash Myash, blood power, Crimea is ours."¹⁴

RT broadcast the video as part of its ongoing Poklonskaya coverage:

The internet fame of Crimea's chief prosecutor, Natalya Poklonskaya, rages on. A patchy music clip made from Poklonskaya's videos has scored

millions of views on YouTube, with a celebrity opposition figure calling the attorney a "sex symbol of Russia."

Footage of Poklonskaya's emotional speech on the *coup d'état* and "chaos" in Ukraine has been making rounds on the internet since March, but this is the first time it has been set to music. The chorus of the music mix, compiled by an anonymous internet DJ known only by his alias "Enjoykin," could certainly be described as simplistic. [...] The "nyash-myash" bit was apparently taken out from Poklonskaya's own reaction to her becoming an anime star and receiving a Russian nickname of Nyasha—to which she replied that she would prefer to be perceived as a prosecutor and will not allow any "nyash" or "myash" while at her post. On a more serious note, the rest of the clip offers cuts from Poklonskaya's solemn statement which said that "the anti-constitutional mayhem has led to a massive bloodshed [...] we have no moral right to step aside from our people [...] our task is to get the work of the prosecutor's office back on track in this country."¹⁵

Cleverly, RT tells viewers first how "the internet" keeps loving and amplifying the Crimea prosecutor. Though seemingly innocuous as an assertion, the subtext of this message is designed to appeal to the same liberal instincts that love Facebook revolutions—in other words, if it's grassroots, on the internet (and especially, shared through social media), while spontaneously amplifying itself to global fame, apparently without central command, then it just *has* to be good. Second, RT distances itself slightly from the violent content by saying the video "could be described as simplistic." After having thus nominally satisfied its liberal viewers' main concerns, the rest of the story glorifies Poklonskaya as a higher authority who has personally intervened to save Crimea from Hobbesian

chaos and “anti-constitutional mayhem.” Words like “emotional” and “solemn” extend further credibility to the prosecutive’s proxy body politic, a stand-in Leviathan for legitimacy, a political fairy tale.

HIGHER FORMS OF PHOTOSHOP

At the St. Petersburg-based Internet Research Agency, workers are paid to each handle a large set of parallel Twitter and Facebook accounts, and to post thousands of pro-Russian comments on Western media articles. The agency, allegedly managed by Putin’s personal chef, is a private company. It is the geopolitical version of a “click farm”—meaning a sweatshop-like facility where underpaid workers “like” things on Facebook to produce social capital for companies.

The Internet Research Agency recycles an unofficial yet sanctioned jargon around the conflict. Journalist Alexandra Garmazhapova writes that “every day, thousands of comments are posted about the ‘Junta’ which has taken power in Kyiv, and the necessity for Russian forces to enter eastern Ukraine. These bloggers have, supposedly, ‘liberated Crimea, and will liberate Novorossiya’ (referring to eastern Ukraine). Supporters of Putin consider Ukraine an ‘artificially created state which does not really exist.’”¹⁶

The Spanish word *junta* means military dictatorship. Some Western news media used to refer to US-backed military governments in Latin America using the same word. After CIA director John Brennan visited Kiev in April 2014, Moscow demanded an explanation for what it regarded as proof of a direct US intervention of that kind in Ukraine. The White House asserted that visits like Brennan’s “are a standard means of fostering mutually beneficial security cooperation.”¹⁷ Reading between the lines of this statement may prove that Moscow had a point; what, after all, does such a visit mean if it takes place during the very nonstandard circumstance of a de facto war between Ukraine and Russia?

In May 2014, the *Guardian* reported a landslide of forty thousand comments a day to its Russia and Ukraine-related articles, believing it was dealing with “an orchestrated pro-Kremlin campaign.”¹⁸ Leaked internal documents from the Internet Research Agency revealed its plans to create a viral video in which Alexei Navalny, a Russian opposition figure and transparency activist, would be compared with Adolf Hitler. Such a video surfaced on YouTube in early 2012.¹⁹ The *New York Times* noted that it went viral mainly because Navalny posted it on his blog.²⁰ The video was created by the Moscow-based design outfit Butovo, which specializes in anti-Navalny artwork.

Russia’s internet-based psychological warfare can be seen as a landscape of crude, absurdist jokes. An enigmatic surface of information supplements the shells of statehood—territorial fictions such as the Donetsk People’s Republic, the Lugansk People’s Republic, and the Federal State of Novorossiya, into which both republics have merged. Novorossiya has its own state flag and YouTube channel where it posts smartphone-recorded videos of tank battles. The term is also used frequently by Putin to extend Russia’s historical claim over Ukraine, though the Russian leader ceases to speak of Novorossiya when he is focusing on the dire state of the economy.

Top leadership positions at the Donetsk People’s Republic are occupied by “political technologists.” Leadership is rotating. As the republic’s now-former prime minister, Alexander Borodai, stated: “Let me remind you, I myself am from Moscow. I am Russian. A citizen of Russia, and a resident of the city of Moscow. I am not from the Donbas, not at all. I came here as a volunteer. It just so happened that, instead of sitting in a trench with a rifle or a machine-gun, I’m now in the prime minister’s chair. Well ... that’s fate.”²¹ A former director of the Russian state security service FSB, Borodai denied having any official ties with Moscow. Indeed he claimed that the civil war in Ukraine, as well as the breakaway states,

are volunteer efforts—the same firewall that clears the Russian state from any official involvement.

Borodai also denied the rebels' possession of the surface-to-air missile launcher that brought down flight MH17, alleging that pictures and videos of such a launcher taken at various locations in eastern Ukraine have been produced using "not Photoshop, but maybe some kind of more advanced programme." Borodai's deputy, his fellow Moscovite Vladimir Antyufeyev, was Transnistria's former Head of the Ministry of State Security before acquiring his new role in Donetsk.²²

"Official nationalisms" and Czarist Russification, explains Benedict Anderson, "can be best understood as a means for combining naturalization with retention of dynastic power, in particular over the huge polyglot domains accumulated since the Middle Ages, or, to put it another way, for stretching the short tight, skin of the nation over the gigantic body of the empire."²³

That skin is now a screen—a surface.

THE SURFACE

The MH17 crash is undisputed by either side in the Ukraine conflict. For a brief moment in time, it cracks open the proxy war. However, the Russian media, including RT, float "alternative explanations" around the crash. Sara Firth, one of RT's reporters, quit her job over the channel's persistence in promoting such theories in the face of overwhelming evidence pointing at the pro-Russian rebels. As Firth explains, after the MH17 incident the channel ran

an eye-witness account that made an accusation against Ukraine and we had a correspondent in the studio who was asked to produce something about a plane that had been shot down at some point in the past and had been the fault of Ukraine. I've been in that position myself before, where you're asked to bring up some piece of

obscure information that implies something that fits with the RT agenda. And you think well, it's not outright lying but it has no relation to what's happening and shouldn't be run at a time when a story of that size is breaking. A news story that is so sensitive. It's abhorrent and indefensible.²⁴

WikiLeaks retweets one of many "alternative explanations" of the MH17 incident. The theory, floated without accompanying evidence, asserts that about a month prior to the crash, a Ukrainian warplane, while attacking rebel-held positions, had tried to use a commercial airliner as its shield, provoking rebel forces to shoot it down.²⁵

WikiLeaks' retweet of this conspiracy theory is just one example of how black transparency's adversarial relationship with the general concept of Western power—in particular the governments of the United States, the United Kingdom, and Sweden—has brought it into alignment with other opponents of that same power.

Still, in November 2010, WikiLeaks spokesperson Kristinn Hrafnsson announced that the site had documents that could damage the Kremlin. "We want to tell people the truth about the actions of their governments," Hrafnsson said, announcing that the material would soon be published. An unnamed FSB official responded to Hrafnsson's purloined letter with a tacit threat, stating that "it's essential to remember that given the will and the relevant orders, [WikiLeaks] can be made inaccessible forever." The cybersecurity expert Gadi Evron has pointed out that this should be considered as an indirect threat to murder WikiLeaks staff, rather than take down its site. "Behind every Internet project, there are people," said Evron.²⁶ There never emerged a specific Russia-related WikiLeaks release other than the Cablegate documents in which American diplomats unsurprisingly called Russia a mafia state.²⁷

Three years later came Edward Snowden's Russian asylum bid, facilitated by WikiLeaks; Snowden's lawyer,

opacity is honest in that it does not hide its secrecy?

Anatoly Kucherena, is a prominent supporter of Putin and sits on a number of Russian government committees.²⁸ The radical transparency engendered by WikiLeaks and Snowden is now allied with a power that should be its target of exposure, rather than its host. Yet, black transparency has in recent years specialized in exposing the hypocrisy of nominally democratic governments that hide their fundamental reliance on secrecy. In Russia, by contrast, state power is ostensibly authoritarian and naturally opaque. This renders it immune to black transparency's most fundamental critique of the state.

The labyrinth of Russian media outlets involved in the permanent role-playing game of "postmodern dictatorship" seems somewhat aligned with the culture of black transparency as well. The conspiracy theories that are distributed by these media constantly use explanations like "cover up" and "inside job." Liberated from a marginal existence on the paranoid fringes of public discourse, conspiracy theories are—seemingly—compliant with the critical inclination to question everything. In them, the secret is acknowledged as a pervasive presence, even if the whole thing is a fantasy, and if its revelation was designed to lead us nowhere.

Fantasy and reality, fiction and fact, are made equivalent. They exist as one surface—a single, shareable veneer.

THE UN-WEST

The YouTube video tweeted by WikiLeaks as "proof" of the MH17 human-shield conspiracy theory was first posted on the so-called Anti-Maidan YouTube channel. It features a young, tall, black-haired female rebel from eastern Ukraine. Uniformed and holding a machine gun, Yelena from Slavyansk explains why she joined the resistance army:

Good day. My name is Yelena. I am in the city of Sloviansk. I am native to this town. I have joined the militia ranks. I cannot bear this anymore.

There is no water, electricity in Sloviansk. People get water from fountains. We are being bombed every day by Ukrainian Army on orders from Junta. Artillery, Airforce. And they drop bombs not on check-points. They drop bombs on people's houses. People don't have anywhere to live, anything to eat. People live in cellars with their children. More than half of civilian population is still here. How long are we to bear this. How is it that government sends Right Sector, mercenaries on their own people. They say that there are mercenaries here, Chechens and so on. The people fighting are from here—Sloviansk, that came out in defence of their own city. They want to just live, not merely exist.

Terrible things are happening. For example an incident that happened recently. Passenger plane was flying by. And Ukrainian attack aircraft hid behind it. Than he lowered his altitude a bit and droped bombs on residential sector of Semenovka town. Than he regained the altitude and hid behind the passanger plane again. Than he left. They wanted to provoke the militia to shoot at the passenger plane. There would be a global catastrophe. Civilians would have died. Than they would say that terrorists here did it. There are no terrorists here. There are regular people here, that came out in defence of their own city. They can't bear this anymore. How long is this going to go on. There are children here, elderly people, WW2 veterans that have to live through it again. Don't you have any humanity left in you?²⁹

Her statement includes no evidence.

In July 2014, the same Yelena is in Donetsk to marry a military commander going by the name of Motorola—a man almost half her height. The video of the ceremony is posted on a Russian YouTube channel, and now-

defunct news agency RIA Novosti has a photographer present at the wedding. The bride wears a white wedding dress, while the groom is in camouflage body armor.³⁰ Also present at the wedding is Igor “Strelkov” Girkin, Donetsk’s Russian-born defense minister who is a fervent participant in Czarist battle reenactments. While his haircut and moustache resemble the gentlemanly appearance of a nineteenth-century cavalry officer, Strelkov asserts the bizarre belief that the bodies on board the MH17 flight were already dead before the plane crashed.³¹ The elusive role-playing commander publishes messages on a Russian web platform for antiques, before other people “copy them on Facebook, VKontakte, and Livejournal. Some of these pages are maintained by Strelkov’s sincere fans. Others are run by Ukrainian activists; still others just by pranksters. As a result, it can sometimes be difficult to divine authentic quotes from fabrications.”³²

Putin’s pixelated Czarism thrives on undermining objectivity itself, and thus, the normative framework that judges his leadership and actions on the international scene. Dmitry Kiselev, the antigay ideologue who leads the state-run news agency Rossiya Segodnya, once made the following point: “Objectivity does not exist. [...] There’s not one publication in the world that’s objective. Is CNN objective? No. Is the BBC objective? No. Objectivity is a myth, which they propose to us and impose on us.”³³

Kiselev’s proposal should appeal to anyone who has ever tried bringing an unpopular story to the mainstream media and was being sidelined or ignored. Journalism and broadcasting are, and always were, deeply political in their capacity to amplify or suppress certain narratives and explanations, answering to different stakeholders and most of all, to different worldviews and imaginaries.

The underdog position of alternative media venues like WikiLeaks is now mimicked by state-sponsored Russian television outlets—up to a point where, under the guise of presenting an alternative explanation, the category of “fact” is obliterated altogether. For example, in

his 2014 interview with the BBC, Borodai mentioned that US President Barack Obama should not be blamed for his views on Ukraine as he is not in full possession of the facts. He added that the internet, from which Obama allegedly gets most of his information, is made of lies.

The possession by the Donetsk rebels of the missile launcher that brought down MH17 was documented by the citizen journalism collective Bellingcat. This group harvests material from social media and other publicly available sources to meticulously reconstruct events on the ground, using image metadata such as geolocation, the direction of shadows in pictures, and other forensic clues.³⁴ Bellingcat harvests, interprets, and rearranges data from the world’s digital overlay to understand how an event unfolds. In plotting such information back onto the map, it pierces through the surface of conspiratorial geofiction that Russia (and Ukraine) have wrapped around their war. To create a reality in which “nothing is true and everything is possible,”³⁵ Russia depends on the internet as much as everybody else does, and this is where the Russian position contradicts itself. Its soldiers—Donetsk rebels or not—constantly share on Facebook and Twitter, and send their videos to YouTube. Citizens do the same. All this produces millions of puzzle pieces waiting to become part of a bigger picture.

According to the researcher Jill Dougherty, “Russia is positioning itself as the ‘Un-West.’”³⁶ Black transparency is in alignment with this perspective. Russia is its current and possibly final stop in its forced search for a geopolitical outside; and in the case of Snowden, it is about the only place on Earth where he is free from persecution by the United States and its allies. However, there is a price to be paid for this alliance; black transparency has become part of an order where fantasy and reality coexist on the same plane—an anomaly that it finds impossible to critique. It is the hyperbole of corrupt government that paradoxically affirms the structural necessity of transparency.

Planetary computation helps the confusing political geography of the Un-West to find its image. In the case of Crimea, a seemingly “objective” standard like Google Maps already follows Kiselev’s ideas to the letter. Google Maps in Russia shows the territory as part of Russia. When opening Google Maps from Ukraine, it looks as if Crimea is still part of that country. On Google US, there is a dotted line between Russia and Crimea indicating a disputed border.³⁷ Google tells the various conflicting parties exactly what they want to hear.

FANTASY

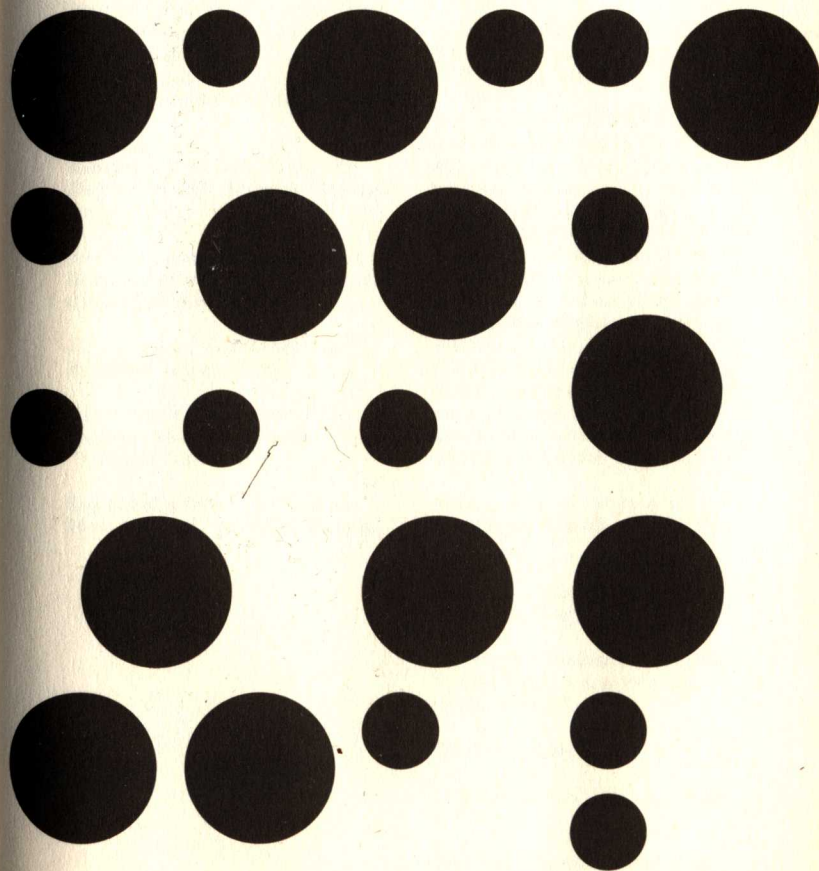
It is challenging to see this surface as a form of phantasmatic design, perhaps, as an “incessant indulgence in fiction and fantasy and other forms of escapism to cope with reality.”³⁸ Finally it is also possible to see it as a form of resistance. The Russian anticapitalist, feminist punk band Pussy Riot interrupts the country’s established socio-political order with short, audacious performances in public space, thus offering its militant punk rock as a form of political speech rather than private entertainment. Pussy Riot’s February 2012 anti-Putin “punk prayer” in Moscow’s Cathedral of Christ the Saviour lasted only one and a half minutes. The song was named “Mother of God, Drive Putin Away.” It provided the only effective answer to Putin’s Novorossiyan merger between church and state: their conflation on the same surface, wrapping an insult to both. The social capital acquired by the punk prayer was enormous relative to the scale and duration of the actual event. It landed three of its members in a Siberian labor camp. Pussy Riot’s actions are not about transparency; however they catalyze responses that make the government’s agenda transparent, its operations visceral and palpable. Putin understood this, and granted Pussy Riot amnesty in December 2013.

The subsequent embrace of Pussy Riot by Western liberals is based on a misreading of what the group stands for. It will gladly cash in on its popularity with the sup-

port of Madonna, but is fundamentally a prank on every kind of power, on every government. Pussy Riot is an intervention by fantasy against authority, a counter-fairy tale that thrives on our enduring need for always-new Black Knights. This time, they are wearing colorful balaclava masks.

This is transparency that thrives not on releasing information about the powerful, but on hijacking their deepest fantasies, triggering responses that are themselves disclosures. Current and future generations of activists, designers, artists, thinkers, musicians, programmers, and organizers will likely realize this. Nothing can stop them from seizing the night.

NOTES
ACKNOWLEDGMENTS
INDEX
CREDITS



COUP DE NET

- 1
Supposedly derived from coup d'état.
- 2
Nicolás Mendoza, "A Tale of Two Worlds: Apocalypse, 4Chan, WikiLeaks and the Silent Protocol Wars," *Radical Philosophy*, no. 166 (March/April 2011): 2.
- 3
WikiLeaks, Twitter post, November 25, 2011, 1:08 a.m.
- 4
Margarit Ralev, "Some Thoughts on the WikiLeaks Logo Design," *LogoBlink* (blog), May 10, 2011.
- 5
Heronimus, October 8, 2012, comment on *ibid*.
- 6
E-mail message to John Young, December 9, 2006, released on Cryptome Archive USB.
- 7
WikiLeaks, e-mail message to Daniel Ellsberg, September 9, 2006, released on Cryptome Archive USB.
- 8
Julian Assange, "Counterinsurgency," *WikiLeaks*, January 28, 2009.
- 9
"The Society of the Spectacle, Pt 1," YouTube video, 9:26, posted by "Azorek79," June 11, 2011.
- 10
Lapiz Solar, comment on WikiLeaks' Facebook post, March 6, 2013, 8:31 a.m.

THERE IS NO ORGANIZATION.
THERE'S ONLY YOU.

- 1
The words were used as a noir voice-over for Johan Grimontprez's seminal documentary art film *Dial H-L-S-T-O-R-Y* (1997), which portrays plane hijackings and looks at the media coverage they received.
- 2
Cited in Gabriella Coleman, "Is Anonymous Anarchy," *OMNI*, August 22, 2011.
- 3
Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (New York: W. W. Norton, 2003), 235.
- 4
For example, when in 2009 WikiLeaks published the loan book of Kaupthing, an Icelandic bank that collapsed under immeasurable debt in the financial crisis, Iceland's capital, Reykjavik, was already in revolt. The "Icelandic revolution" of 2009 had most if not all factors for a butterfly effect in place. In the small Nordic island nation, the international financial crisis resonated into an information cascade within its tightly knit population, leading to widespread outrage. Information given by WikiLeaks was essential for the cascade to happen. The sitting government was forced out and the constitution was rewritten, among other things.
- 5
Julian Assange, "Conspiracy as Governance," *Frontline Club* (blog), June 28, 2011.
- 6
Mark Fisher, "Reality Management," *k-punk* (blog), July 5, 2011.
- 7
Hito Steyerl, "Too Much World: Is the Internet Dead?," *e-flux journal*, no. 49 (November 2013).
- 8
"Media/Unsorted Articles," *WikiLeaks*.
- 9
"WikiLeaks Leak," *Cryptome*, January 9, 2007.
- 10
Clay Shirky, *Here Comes Everybody: The Power of Organizing without Organizations* (London: Penguin Press, 2008), 2.

11
Ibid., 3.

12
Ibid., 6.

13
Ibid., 7.

14
Nicholas Confessore, "Tale of a Lost Cellphone, and Untold Static," *New York Times*, June 21, 2006.

15
Clay Shirky, "'Stolen Sidekick': Moral Endeavor," *Chicana/o Studies 404: Chicana Feminisms, Spring 2012* (blog), January 31, 2012.

16
The atomization of the individual—and the crumbling of organized political alternatives—finds its imaginative apex in the child gladiators in the book and motion-picture series *The Hunger Games*. In this series, individuals are cherry-picked by the government to fight each other to the death in a broadcast spectacle set. This landscape, a walled arena, is a place where you are literally left only to care for yourself. Mark Fisher notes that "in an inversion of Hobbes, the war of all against all emerges as an artificial condition rather than a state of nature." Mark Fisher, "Dystopia Now," *Mark Fisher ReBlog* (blog), December 30, 2012.

17
Shirky, *Here Comes Everybody*, 163.

18
Steven R. Mann, "Chaos Theory and Strategic Thought," *Parameters* 12, no. 2 (Autumn 1992): 57.

19
John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica, CA: RAND Corporation, 2001), ix.

20
Originally attributed to *Whole Earth Catalog* founder Stewart Brand, the phrase "information wants to be free" has become a political catchphrase for techno-utopians the world over, a "rallying cry, typically invoked against any efforts to limit access to [...] information." See R. Polk Wagner, "Information Wants to Be Free: Intellectual Property and the Mythologies of Control," University of Pennsylvania Law School website, May 9, 2003.

21
Clay Shirky, "WikiLeaks and the Long Haul," *Clay Shirky* (blog), December 6, 2010.

22
Duncan J. Watts, "A Simple Model of Global Cascades on Random Networks," *Proceedings of the National Academy of Sciences of the United States of America* 99, no. 9 (April 30, 2002): 5766–71.

23
Kareem Fahim, "Slap to a Man's Pride Set Off Tumult in Tunisia," *New York Times*, January 21, 2011.

24
Peter Walker, "Amnesty International Hails WikiLeaks and Guardian as Arab Spring 'Catalysts,'" *Guardian*, May 13, 2011.

25
Julian Assange and Hans Ulrich Obrist, "In Conversation with Julian Assange, Part II," *e-flux journal*, no. 26 (June 2011).

26
Cited in Marie Colvin, "WikiLeaks Founder Baffled by Sex Assault Claims," *Australian Sunday Times*, December 27, 2010.

27
Bill Keller, "The Boy Who Kicked the Hornet's Nest," in *Open Secrets: WikiLeaks, War, and American Diplomacy* (New York: Grove Press, 2011), 11.

28
Cited in Moritz Gathmann et al. "The Opinion-Makers: How Russia Is Winning the Propaganda War," trans. Daryl Lindsey, *Der Spiegel*, May 30, 2014.

29
Ed Payne and Catherine E. Shoichet, "Morales Challenges US after Snowden Rumor Holds Up Plane in Europe," *CNN*, July 5, 2013.

30
Associated Press, "European States Were Told Snowden Was on Morales Plane, Says Spain," *Guardian*, July 5, 2013.

31
The Charter of Fundamental Rights of the European Union enlists everyone's right to respect for his or her private communications, and to the protection of their personal data. Such principles, Snowden revealed, are routinely violated by the NSA and its partner agencies in

Europe. "Charter of Fundamental Rights in the European Union," *Official Journal of the European Communities*, December 18, 2000.

32
Joshua Yaffa, "Could VKontakte Be Edward Snowden's Next Employer?," *Bloomberg Businessweek*, August 2, 2013.

33
Becky Bratu, "The Spy Who Spurned Me: Anna Chapman Refuses to Discuss Snowden Proposal," *NBC News*, September 30, 2013.

34
Eli Lake, "Sorry, Snowden: Putin Lied to You about His Surveillance State—And Made You a Pawn of It," *Daily Beast*, April 18, 2014.

35
David Brooks, "Putin Can't Stop," *New York Times*, March 3, 2014.

36
The return of RT to Russian propaganda broadcasting during the 2014 Ukraine events is explored in this book's last chapter.

37
"Germany, Brazil Present UN Resolution on Cyberprivacy," *Al Jazeera America*, November 7, 2013.

38
Sarah Harrison, "Statement by Sarah Harrison," *WikiLeaks*, November 6, 2013.

39
Julian Assange to Metahaven about the aesthetic of the WikiLeaks website, conversation at Ellingham Hall, UK, February 2011.

40
"Julian Assange on M.I.A.: 'She's the World's Finest Megaphone for the Truth': WikiLeaks Founder Discusses 'Matangi' Rapper in New NME Interview," *NME*, November 12, 2013.

41
Cited in Nadeeka Alexis, "M.I.A. Spills on How She Got Julian Assange Live in Concert," *MTV News*, November 4, 2013.

42
Robert Booth, "Lady Gaga Takes Tea with Julian Assange," *Guardian*, October 9, 2012.

43
Huw Nesbitt, "Deterritorial Support Group: We Take a Closer Look at This Anonymous Group of Political Bloggers

and Masters of Internet Propaganda," *Dazed Digital*, 2011.

44
"Lady Gaga on Bradley Manning's Sentence: 'Devastating,'" *Huffington Post*, August 21, 2013.

45
"Analysing WikiLeaks: Bruce Sterling's Plot Holes," *Democracy in America* (*Economist* blog), December 24, 2010.

46
See Freedom of the Press website, www.securedrop.org.

47
Saroj Giri, "WikiLeaks beyond WikiLeaks?," *Mute*, December 16, 2010.

OPEN GOVERNMENT GLASS
CANDY

1
Evgeny Morozov, Twitter post, July 21, 2014, 2:52 p.m.

2
Saif Al-Islam Qaddafi, "The Role of Civil Society in the Democratization of Global Governance Institutions: From 'Soft Power' to Collective Decision Making?" (PhD diss., Department of Philosophy, London School of Economics and Political Science, 2007), 65.

3
Clare Birchall, "Data Goes Pop: Transparency as a Neoliberal Tool," YouTube video, 21:12, posted by "York Neoliberalism Conference," August 15, 2013.

4
This figurative quality also appears, somewhat differently, in the noble style *Seine Durchlaucht*, "His Serenity," or, "His Transparency." The style emerged in 1375 and applied to the prince-electors, or *Kurfürsten*, of the Holy Roman Empire. The prince-electors were members of a privileged boardroom that elected the Holy Roman King, and later, the emperor. The monarch of the ministate of Liechtenstein, a prominent tax haven, ironically, is the last remaining *Fürst* to be addressed as "His Transparency."

5
"A dispute then arose between Gallus and the emperor. Gallus proposed that the elections of magistrates should be held every five years, and that the commanders of the legions who before receiving a praetorship discharged this military service should at once become praetorselect, the emperor nominating twelve candidates every year. It was quite evident that this motion had a deeper meaning and was an attempt to explore the secrets of imperial policy." Tacitus, *Annals: Book II*, trans. Alfred John Church and William Jackson Brodribb, Internet Classics Archive (MIT).

6
Eva Horn, "Logics of Political Secrecy," *Theory, Culture & Society* 28, nos. 7-8 (December 2011): 103-22.

7
Henry Farrell and Martha Finnemore, "The End of Hypocrisy," *Foreign Affairs* 92, no. 6 (November/December 2013): 22-26.

8
Emphatically, this applies to the Obama administration's deployment of transparency advocacy, combined with accruing ever-increasing power in the executive branch, including the power to kill Americans anywhere on the planet without the interference of a judge.

9
Carl Schmitt, *Political Theology: Four Chapters on the Concept of Sovereignty*, trans. George Schwab (Chicago: University of Chicago Press, 2005), 6.

10
Paul Scheerbarth, "Glass Architecture" (excerpt), in *Programs and Manifestoes on 20th-Century Architecture*, ed. Ulrich Conrads (Cambridge, MA: MIT Press, 1971), 32.

11
Beatrice Warde, "The Crystal Goblet, or Printing Should Be Invisible" (lecture to the British Typographers' Guild, 1932). "You have two goblets before you. One is of solid gold, wrought in the most exquisite patterns. The other is of crystal-clear glass, thin as a bubble, and as transparent. Pour and drink; and according to your choice of goblet, I shall know whether or not you are a connoisseur of wine."

12
Detlef Mertins, "Utopia of Glass," in *Modernity Unbound* (London: Architectural Association, 2011), 102.

13
Ibid., 104.

14
Walter Benjamin, *The Arcades Project*, trans. Howard Eiland and Kevin McLaughlin (London: Harvard Belknap, 1999), 4.

15
Yevgeny Zamyatin, *We*, trans. Clarence Brown (London: Penguin, 1993), 71.

16
See Simon Sheikh, "Positively Representation of Banking Revisited," *e-flux journal*, no. 24 (April 2011).

17
Detlef Mertins, "Glass Architecture," in *Modernity Unbound*, 16.

18
Colin Rowe and Robert Slutzky, *Transparency* (1964; repr. Basel: Birkhäuser, 1997), 22-23.

19
Archon Fung, Mary Graham, and David Weil, *Full Disclosure: The Perils and Promise of Transparency* (New York: Cambridge University Press, 2007), 7.

20
Clare Birchall, introduction to "Secrecy and Transparency: The Politics of Opacity and Openness," *Theory, Culture & Society* 28, nos. 7-8 (December 2011): 10.

21
R. W. Apple Jr. "Archives," *New York Times*, June 23, 1996.

22
Ann Florini, "The Battle over Transparency," in *The Right to Know: Transparency for an Open World* (New York: Columbia University Press, 2007), 5.

23
New Statesman, "Assange: 'WikiLeaks Is the Intelligence Agency of the People,'" *New Statesman*, April 5, 2011.

24
WikiLeaks' Facebook page, August 17, 2013.

25
WikiLeaks, "Afghan War Diary 2004-2010," *WikiLeaks*, July 25, 2010.

26
Eric Limer, "What Could Be in Wikileaks' Giant 349GB 'Insurance' File?," *Gizmodo* (blog), August 17, 2013.

27
Bruce Schneier, "WikiLeaks Insurance File," *Bruce Schneier's Blog*, August 4, 2010.

28
Horn, "Logics of Political Secrecy," 103-22.

29
Edgar Allan Poe, "The Purloined Letter" (1845), in *Edgar Allan Poe: Annotated and Illustrated Entire Stories and Poems*, ed. Andrew Barger (Memphis, TN: Bottle Tree Books, 2008), 464.

30
Andy Greenberg, "An Interview with WikiLeaks' Julian Assange," *Forbes*, November 29, 2010.

31
Joe Rauch, "BoFA May Be the Next WikiLeaks Target," *Reuters*, November 30, 2010.

32
Nelson D. Schwartz, "Facing Threat from WikiLeaks, Bank Plays Defense," *New York Times*, January 2, 2011.

33
The Anonymous hack was a response to something unrelated: Aaron Barr, CEO of HBGary's federal division, announced in the *Financial Times* that he had unveiled Anonymous' leadership by sifting through Facebook and LinkedIn user profiles. See also Nate Anderson, "Spy Games: Inside the Convoluted Plot to Bring Down WikiLeaks," *Ars Technica*, February 14, 2011.

34
Mark Hosenball, "Exclusive: Assange Suggests Bank Documents Are a Snore," *Reuters*, February 9, 2011.

35
Cited in Ryan Gallagher, "WikiLeaks 'Blackmailed' over Bank of America Leaks," *Frontline Club*, July 4, 2011.

36
Cited in Mark Hosenball, "Some of WikiLeaks' Bank of America Data Destroyed," *Reuters*, August 22, 2011.

37
Birchall, "Data Goes Pop."

38
"#ogdcamp Opening Talk From Neelie Kroes," *Open Knowledge Foundation* (blog), October 20, 2011.

39
William D. Eggers, *Government 2.0: Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy* (Plymouth: Rowman & Littlefield, 2005), 129.

40
Ibid., 127.

41
Dan Wilchins, "Lehman Hires Jeb Bush as Private Equity Advisor," *Reuters*, August 30, 2007.

42
Eggers, *Government 2.0*, 125.

43
Beth Simone Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful* (Washington, DC: Brookings Institution Press, 2009), 29.

44

Novack mentions a few specific examples of those "civic groups": "The Cato Institute's Jim Harper launched the Washington Watch program to track bills in Congress and estimate their cost or savings, if implemented into law. The Center for Responsive Politics started OpenSecrets; and the New York gallery Eyebeam launched Fundrace (now part of the *Huffington Post* blog) to make the Federal Election Commission's databases easier to understand and search. PublicMarkup.org used collaborative editing software, known as a wiki, to mark up the Transparency in Government Act of 2008 and the various economic stabilization and bailout proposals floated during the economic crisis in the fall of that year. MapLight shines the light of transparency on money politics by illuminating who contributed to which politician and how he or she subsequently voted." *Ibid.*, 30-31.

45

Micah L. Sifry, *WikiLeaks and the Age of Transparency* (Berkeley, CA: Counterpoint, 2011), 142.

46

Ibid., 144.

47

Ibid., 186.

48

Shirky's original post on this topic has disappeared from his blog, but can be read on the *Goodreads* website: "Consulting with Libya in 2007," *Goodreads*, March 1, 2011.

49

Joseph S. Nye Jr., "Tripoli Diarist," *New Republic*, December 10, 2007.

50

Siddhartha Mahanta and David Corn, "Saif Qaddafi's Democracy-Loving Dissertation," *Mother Jones*, February 25, 2011.

51

Joseph S. Nye Jr., "Gaddafi and Change," *Huffington Post*, March 31, 2011.

52

Qaddafi, "Role of Civil Society," 385.

53

The Wine and Cheese Appreciation Society of Greater London / Kittens Editorial Collective, "On Wikileaks,

Bitcoin, Copyleft: Three Critiques of Hacktivism," *Kittens*, no. 1 (January 2013): 6.

CAPTIVES OF THE CLOUD

1

Cited in Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012), xx.

2

Brandon Tedder, "To the Cloud!," *Ezine Mark* (blog), February 20, 2012.

3

Sharon Gillett and Mitchell Kapor, "The Self-Governing Internet: Coordination by Design" (lecture, Coordination and Administration of the Internet Workshop, Kennedy School of Government, Harvard University, Cambridge, September 8-10, 1996).

4

John Markoff, "An Internet Critic Who Is Not Shy about Ruffling the Big Names in High Technology," *New York Times*, April 9, 2001.

5

Eric Schmidt, in "Conversation with Eric Schmidt Hosted by Danny Sullivan," Google Press Center website, August 9, 2006.

6

"Amazon: The Walmart of the Web," *Economist*, October 1, 2011.

7

Nathan Eddy, "Cloud Computing to Drive Storage Growth: IDC Report," *eWeek*, October 21, 2011.

8

Cited in Nick Bilton, "Disruptions: At Box, a Fast-Moving Chief Immersed in the Cloud," *Bits* (*New York Times* blog), August 26, 2012.

9

Barb Darrow, "Amazon Is No. 1. Who's Next in Cloud Computing?," *GigaOM*, March 14, 2012; Cade Metz, "Google: 'We're Like a Bank for Your Data,'" *Wired*, May 29, 2012.

10

Zack Whittaker, "Summary: ZDNet's USA Patriot Act Series," *ZDNet*, April 27, 2011.

11

Jeffrey Rosen, "The Patriot Act Gives Too Much Power to Law Enforcement," *New York Times*, September 8, 2011.

12

Matthew C. Waxman, interview by

Jonathan Masters, "Extending Patriot Act Powers," Council on Foreign Relations website, February 22, 2011.

13

Saskia Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages* (Princeton, NJ: Princeton University Press, 2008), 180.

14

Paul Taylor, "Privacy Concerns Slow Cloud Adoption," *Financial Times*, August 2, 2011.

15

Lucian Constantin, "Google Admits Handing Over European User Data to US Intelligence Agencies," *Softpedia*, August 8, 2011.

16

Winston Maxwell and Christopher Wolf, "A Global Reality: Governmental Access to Data in the Cloud," Hogan Lovells White Paper, May 23, 2012.

17

Mike Masnick, "Senators Reveal That Feds Have Secretly Reinterpreted the Patriot Act," *Techdirt*, May 26, 2011.

18

Kim Zetter, "Unknown Tech Company Defies FBI in Mystery Surveillance Case," *Wired*, March 14, 2012.

19

Babu Kurra, "Egypt Shut Down Its Net with a Series of Phone Calls," *Wired*, January 28, 2011.

20

Claire Connelly and Lee Taylor, "FBI Shuts Down Megaupload.com, Anonymous Shut Down FBI," *news.com.au*, January 20, 2012.

21

Ibid.

22

Jennifer Granick, "Megaupload: A Lot Less Guilty Than You Think," *Center for Internet and Society at Stanford Law School*, January 26, 2012.

23

David Kravats, "Uncle Sam: If It Ends in .Com, It's Seizable," *Wired*, March 6, 2012.

24

Michael Geist, "All Your Internets Belong to US, Continued: The Bodog.com Case," on Michael Geist's website, March 6, 2012.

25

Ronald Deibert et al., eds., *Access Controlled: The Shaping of Power,*

Rights, and Rule in Cyberspace (Cambridge, MA: MIT Press, 2010), 6.

26

Ibid., 11.

27

Ellen Nakashima, "A Story of Surveillance," *Washington Post*, November 7, 2007.

28

Ibid.

29

Dan Levine, "US Court Upholds Telecom Immunity for Surveillance," *Reuters*, December 29, 2011.

30

Deibert et al., *Access Controlled*, 381.

31

Declan McCullagh, "FBI: We Need Wiretap-Ready Web Sites—Now," *CNET*, May 4, 2012.

32

Geoff White, "'Black Boxes' to Monitor All Internet and Phone Data," *Channel 4*, June 29, 2012.

33

Alex Wawro, "What Is Deep Packet Inspection?," *PC World*, February 1, 2012.

34

Declan McCullagh, "Report: Feds to Push for Net Encryption Backdoors," *CNET*, September 27, 2010.

35

Communities against Terrorism, FBI flyers, on the Public Intelligence website, February 1, 2012.

36

"Facebook's Name Policy—Facebook Help Center," Facebook website; "Google+ Page and Profile Names—Google+ Help," Google+ website.

37

Alexis Madrigal, "Why Facebook and Google's Concept of 'Real Names' Is Revolutionary," *Atlantic*, August 5, 2011.

38

"Amazon.com Help: Pen Names and Real Names," Amazon website.

39

Mark T. Kieczorek, "Amazon Real Name Badge," *Marktaw* (blog), July 23, 2004; Amy Harmon, "Amazon Glitch Unmasks War of Reviewers," *New York Times*, February 14, 2004.

40

Cited in Declan McCullagh, "Obama to

Hand Commerce Dept. Authority over Cybersecurity ID," *CNET*, January 7, 2011.

41

Elizabeth Kolbert, "The Things People Say," *New Yorker*, November 2, 2009.

42

Cass R. Sunstein, *Republic.com 2.0* (Princeton, NJ: Princeton University Press, 2007), 44.

43

Cass R. Sunstein and Adrian Vermeule, "Conspiracy Theories: Causes and Cures," *Journal of Political Philosophy* 17, no. 2 (2009): 224-25.

44

Michael Kan, "Beijing to Require Users on Twitter-Like Services to Register with Real Names," *PC World*, December 16, 2011.

45

Michael Bristow, "China Arrests over Coup Rumours," *BBC News*, March 31, 2012; David Eimer, "China Arrests Six over Coup Rumours," *Telegraph*, March 31, 2012.

46

Shiv Malik, "Facebook Accused of Removing Activists' Pages," *Guardian*, April 29, 2012.

47

Tim Bradshaw, "Mark Zuckerberg Friends David Cameron," *Financial Times Tech Blog*, June 21, 2012.

48

MacKinnon, introduction to *Consent of the Networked*, xxi.

49

Cited in Elizabeth Dickinson, "Internet Freedom: The Prepared Text of US Secretary of State Hillary Rodham Clinton's Speech Delivered at the Newseum in Washington, D.C.," *Foreign Policy*, January 21, 2010.

50

Evgeny Morozov, "Is Hillary Clinton Launching a Cyber Cold War?," *Foreign Policy*, January 21, 2010.

51

Global Internet Freedom Consortium website.

52

"Save the Internet Campaign," FreePress website.

53

Tim Wu, "Network Neutrality, Broadband Discrimination," *Journal of Telecommunications and High Technology Law* 2 (2003): 141.

54

Joi Ito, "Weblogs and Emergent Democracy," ed. Jon Lebkowsky, *Joi Ito's Web*, July 10, 2002.

55

On a related note, cyberlaw professor Jonathan Zittrain in 2008 wrote *The Future of the Internet—And How to Stop It*, a book focusing on the rise of the web's "tethered appliances," which, like North Korean radio sets, can be tuned to exclude or disregard certain content, and are designed not to be tinkered with by their users. Zittrain argued that such closed service appliances—emphatically including design icons like iPods and iPhones, for example—would in fact contribute to stifle the generative and innovative capacity of the web.

56

Christina Bonnington and Spencer Ackerman, "Apple Rejects App That Tracks US Drone Strikes," *Wired*, August 30, 2012.

57

Nick Wingfield, "Apple Rejects App Tracking Drone Strikes," *Bits* (New York Times blog), August 30, 2012.

58

MacKinnon, *Consent of the Networked*, 119.

59

Cited in Gregg Keizer, "Apple Boots WikiLeaks App from iPhone Store," *Computerworld*, December 21, 2010.

60

"The Julian Assange Show: Cypherpunks Uncut (p. 1)," YouTube video, 1:21:06, posted by "RT," July 29, 2012.

61

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

62

Manuel Castells, *The Information Age: Economy, Society and Culture*, vol. 1: *The Rise of the Network Society* (Malden, MA: Blackwell, 2000), 442.

63

Ibid.

64

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

65

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

66

James Glanz, "The Cloud Factories: Power, Pollution and the Internet," *New York Times*, September 22, 2012.

67

Pier Vittorio Aureli, "Form," in *Uncorporate Identity*, ed. Metahaven and Marina Vishmidt (Baden: Lars Müller Publishers, 2010), 262.

68

Boris Groys, "Form," in *ibid.*, 263.

69

John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation website, February 8, 1996.

70

Sassen, *Territory, Authority, Rights*, 330.

71

Mueller, *Networks and States*, 268.

72

Microsoft Corporation, "About Microsoft"; Gillian Reagan, "The Evolution of Facebook's Mission Statement," *New York Observer*, July 13, 2009; Skype, "About Skype"; Instagram, "FAQ."

73

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).

74

"Data Haven by Bruce Sterling from Islands in the Net," *Technovelgy* (blog).

75

The Principality of Sealand is discussed at length in our book *Uncorporate Identity*. In our interview with the hacker, cryptographer, and internet entrepreneur Sean Hastings, a self-styled inventor of Sealand's data haven, he declared: "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, interview by Metahaven, "The Rise And Fall Of The Data Haven, Interview with Sean Hastings," in *Uncorporate Identity*, 65. Later examples include Seasteading, an enterprise founded by Patri Friedman, designed to be a set of sovereign floating sea vehicles under ultra-minimal 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. Cooper Smith, "Peter Thiel, PayPal Founder, Funds 'Seasteading,' Libertarian Sea Colony," *Huffington Post*, August 19, 2011.

76

Joi Ito, "Havenco Doing Well According BBC," *Joi Ito's Web* (blog), July 10, 2002.

77

James Grimmelmann, "Sealand, HavenCo, and the Rule of Law," *University of Illinois Law Review* 2012, no. 2 (2012): 460.

78

Ibid., 462-63.

79

Cory Doctorow, "Pirate Bay Trying to Buy Sealand, Offering Citizenship," *Boingboing* (blog), January 12, 2007.

80

Michael Froomkin, in "Internet Regulation at a Crossroads," YouTube video, 1:11:24, from a lecture at the Oxford Internet Institute, University of Oxford, posted by "OIIOxford," June 14, 2012.

81

Grimmelmann, "Sealand, HavenCo, and the Rule of Law," 479.

82

James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors," Duke Law website, 1997.

83

Ibid.

84

Grimmelmann, "Sealand, HavenCo, and the Rule of Law," 484.

85

WikiLeaks, "Icelandic Bank Kaupthing Threat to WikiLeaks over Confidential Large Exposure Report," *WikiLeaks*, July 31, 2009.

86

Xeni Jardin, "WSJ Obtains Wikileaks Financial Data: Spending Up, Donations Down," *Boingboing* (blog), December 24, 2010; Joshua Norman, "WikiLeaks' Julian Assange Now Making \$86k/year," *CBS News*, December 24, 2010.

87

WikiLeaks, "Banking Blockade," October 24, 2011.

88

Ryan Paul, "Wikileaks Kicked Out of Amazon's Cloud," *Ars Technica* (blog), December 1, 2010.

89

Alexia Tsotsis, "Sen. Joe Lieberman: Amazon Has Pulled Hosting Services for WikiLeaks," *Techcrunch* (blog), December 1, 2010.

90

Cited in Paul Owen, Richard Adams, and Ewen MacAskill, "WikiLeaks: US Senator Joe Lieberman Suggests New York Times Could Be Investigated," *Guardian*, December 7, 2010.

91

Yochai Benkler, "WikiLeaks and the Protect-IP Act: A New Public-Private Threat to the Internet Commons," *Dædalus* 140, no. 4 (Fall 2011): 154-55.

92

Boyle, "Foucault in Cyberspace."

93

James Grimmelmann, e-mail to the authors, July 17, 2012.

94

Charles Arthur, "WikiLeaks Claims Court Victory against VISA," *Guardian*, July 12, 2012.

95

Grimmelmann, e-mail to the authors, July 17, 2012.

96

Cited in Omar R. Valdimarsson, "Iceland Court Orders Valitor to Process WikiLeaks Donations," *Bloomberg*, July 12, 2012.

97

Arthur, "WikiLeaks Claims Court Victory against VISA."

98

William Neuman and Maggy Ayala, "Ecuador Grants Asylum to Assange, Defying Britain," *New York Times*, August 16, 2012.

99

Tiina Pajuste, "Assange v Swedish Prosecution Authority: The Misapplication of European and International Law by the UK Supreme Court—Part 2," *Cambridge Journal of International and Comparative Law*, June 20, 2012.

100

Mark Weisbrot, "Julian Assange Asylum: Ecuador Is Right to Stand Up to the US," *Guardian*, August 16, 2012. The British authorities sent a letter to Ecuador saying, "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."

101

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," *Daily Mail*, September 29, 2012.

102

Raffi Khatchadourian, "No Secrets: Julian Assange's Mission for Total Transparency," *New Yorker*, June 7, 2010.

103

Birgitta Jónsdóttir, Twitter post, November 13, 2011, 11:55 a.m.

104

Amazon, "AWS Security and Compliance Center," Amazon Web Services.

105

Amazon, "Amazon Web Services: Risk and Compliance White Paper," November 2013.

106

Malcolm Ross, "Appian World 2012—Developer Track," *Appian*, March 16, 2012.

107

Rebecca J. Rosen, "How Your Private Emails Can Be Used against You in Court," *Atlantic*, July 8, 2011.

108

Ibid.

109

Gleick, *The Information*, 395-96.

110

Glenn Greenwald, "DOJ Subpoenas Twitter Records of Several WikiLeaks Volunteers," *Salon*, January 8, 2011.

111

Cited in Kevin Poulsen, "Feds: WikiLeaks Associates Have 'No Right' to Know about Demands for Their Records," *Wired*, June 2, 2011.

112

Birgitta Jónsdóttir, "Evidence of a US Judicial Vendetta against WikiLeaks Activists Mounts," *Guardian*, July 3, 2012.

113

Bernard Keane, "The Boston Fishing Party and Australians' Rights Online," *Crikey* (blog), January 17, 2012.

114

Wikileaks, Twitter post, January 17, 2012, 1:14 p.m.

115

Keane, "Boston Fishing Party."

116

Gabriella Coleman, discussion with Bob Garfield, "The Many Moods Of Anonymous," NYU Steinhardt, March 4, 2011.

117

Steve Fishman, "Hello, I am Sabu" *New York Magazine*, June 3, 2012.

118

Nate Anderson, "LulzSec Leader 'Sabu' Worked with FBI since Last Summer," *Ars Technica* (blog), March 6, 2012.

119

Charles Arthur, Dan Sabbagh, and Sandra Laville, "LulzSec Leader Sabu Was Working for Us, Says FBI," *Guardian*, March 7, 2012.

120

Sassen, *Territory, Authority, Rights*, 382-83.

ALL TOMORROW'S CLOUDS

- 1
pouremecoffee, Twitter post, August 16, 2013, 4:11 a.m.
- 2
Carl von Clausewitz, *On War*, trans. J. J. Graham (London: N. Trübner, 1873).
- 3
"Iceland: A Radical Periphery in Action; Smári McCarthy Interviewed by Metahaven," *Volume #32: Centers Adrift* (July 2012): 98–101.
- 4
"30C3—Bullshit Made in Germany by Linus Neumann," YouTube video, 1:00:37, posted by "Marco Hininger," December 28, 2013.
- 5
Rosie Gray, "Ecuador Rebrands Itself as the Home of Internet Freedom," *BuzzFeed News*, December 6, 2013.
- 6
"The Cloud, the State, and the Stack: Metahaven in Conversation with Benjamin Bratton," *Metahaven* (blog), December 16, 2012.
- 7
Shane Harris, "The Cowboy of the NSA: Inside Gen. Keith Alexander's All-Out, Barely-Legal Drive to Build the Ultimate Spy Machine," *Foreign Policy*, September 9, 2013.
- 8
Kim Zetter, "NSA Chief Tells Hackers His Agency Doesn't Create Dossiers on All Americans," *Wired*, August 27, 2012.
- 9
Philip Bump, "The NSA Admits It Analyzes More People's Data Than Previously Revealed," *Wire*, July 17, 2013. "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."
- 10
Guardian US Interactive Team, "Three Degrees of Separation: Breaking Down the NSA's 'Hops' Surveillance Method," *Guardian*, October 28, 2013.
- 11
Eben Moglen, "Snowden and the Future, Part 1: Westward the Course of Empire" (lecture, Columbia Law School, October 9, 2013).
- 12
Justin Elliott and Theodor Meyer, "Claim on 'Attacks Thwarted' by NSA Spreads Despite Lack of Evidence," *ProPublica*, October 23, 2013.
- 13
Glenn Greenwald, Ryan Gallagher, and Ryan Grim, "Top-Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit 'Radicalizers,'" *Huffington Post*, November 26, 2013. A document that reveals the NSA plot was published by the *Huffington Post*. The director of the NSA, who is described as "DIRNSA," is listed as the "originator" of the document.
- 14
Cited in Ruth Marcus, "James Clapper's 'Least Untruthful' Answer," *Washington Post*, June 13, 2013.
- 15
Jason Howerton, "James Clapper Apologizes for Lying to Congress about NSA Surveillance: 'Clearly Erroneous,'" *Blaze*, July 2, 2013.
- 16
Yochai Benkler, "Time to Tame the NSA Behemoth Trampling Our Rights," *Guardian*, September 13, 2013.
- 17
Jennifer Granick, "NSA SEXINT Is the Abuse You've All Been Waiting For," *Just Security*, November 29, 2013.
- 18
Luke Johnson, "James Clapper, Director of National Security Intelligence Who Mised Congress, to Establish Surveillance Review Group," *Huffington Post*, August 13, 2013.
- 19
David Weigel, "New NSA Reform Bill Authorizes All the NSA Activity That Was Making You Angry," *Slate* (blog), November 1, 2013.
- 20
Mark Hosenball, "Obama Halted NSA Spying on IMF and World Bank Headquarters," *Reuters*, October 31, 2013.
- 21
Elizabeth Dickinson, "Internet Freedom: The Prepared Text of U.S. Secretary of State Hillary Rodham Clinton's Speech, Delivered at the Newseum in Washington, D.C.," *Foreign Policy*, January 21, 2010.

- 22
Clinton's 2011 statement on internet freedom met with considerable skepticism from the press, in particular because of the US government's crackdown on WikiLeaks. See for example Dan Sabbagh, "Hillary Clinton's Speech: Shades of Hypocrisy on Internet Freedom," *Guardian*, February 15, 2011.
- 23
Philip N. Howard, "The Arab Spring's Cascading Effects," *Pacific Standard*, February 23, 2011.
- 24
Mustafa Nayem, "Uprising in Ukraine: How It All Began," *Open Society Foundations Voices*, April 4, 2014.
- 25
Metahaven, "From Public Relations to Social Standards: A Conversation with David Grewal," in *Uncorporate Identity*, ed. Metahaven and Marina Vishmidt (Baden: Lars Müller Publishers, 2010), 540.
- 26
Cited in Alan Rusbridger, "The Snowden Leaks and the Public," *New York Review of Books*, November 21, 2013.
- 27
Cited in David Cole, "We Kill People Based on Metadata," *New York Review of Books* (blog), May 10, 2014.
- 28
Lorraine Twohill, cited in Claire Cain Miller, "Google Bases a Campaign on Emotions, Not Terms," *New York Times*, January 1, 2012.
- 29
Evgeny Morozov, "Future Shock: Meet the Two-World Hypothesis and Its Havoc," *New Republic*, May 27, 2013.
- 30
Julian Assange, "The Banality of 'Don't Be Evil,'" *New York Times*, June 1, 2013.
- 31
Clinton, "Internet Freedom."
- 32
"Between Two Ends of the WikiLeaks Investigation: Parallel Constructing the FBI's Secret Authorities," *Emptywheel*, February 19, 2014.
- 33
Evgeny Morozov, "The World Is Not Enough—How to Reinvent the Internet," *Der Feuilletonist*, January 20, 2014.
- 34
Slavoj Žižek, "Corporate Rule of Cyberspace," *Inside Higher Education*, May 2, 2011.
- 35
Kate Crawford, lecture at Data Drama, Princeton University, April 6, 2014.
- 36
Cited in Fiona Duncan, "Normcore: Fashion for Those Who Realize They're One in 7 Billion," *New York Magazine*, February 26, 2014.
- 37
Stanford/NYU Report, *Living Under Drones*, September 2012.
- 38
Hannah Arendt, "The Conquest of Space and the Stature of Man," in *Between Past and Future* (London: Penguin, 2006), 273–74.
- 39
Diana Saco, *Cybering Democracy: Public Space and the Internet* (Minneapolis: University of Minnesota Press, 2002), 51.
- 40
See Brian Kuan Wood, "Is It Love?," *e-flux journal*, no. 53 (March 2014).
- 41
See "Evgeny Morozov," "The Folly of Solutionism," *Economist*, May 2, 2013.
- 42
Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010), 268.
- 43
Bruce Schneier, "The US Government Has Betrayed the Internet: We Need to Take It Back," *Guardian*, September 5, 2013.
- 44
Benjamin Bratton, "Some Trace Effects of the Post-Anthropocene: On Accelerationist Geopolitical Aesthetics," *e-flux journal*, no. 46 (June 2013).
- 45
"Newsnight: Paxman vs Brand—Full Interview," YouTube video, 10:46, posted by "BBC Newsnight," October 23, 2013.
- 46
Jesse Darling, "On the Ghostmodern Performative Poetics of Snapchat," *Brave New What?* (blog), January 20, 2013.

- 47
Carne Ross, "Citizens of the World, Unite! You Have Nothing to Lose but Your Data," *Guardian*, October 31, 2013.
- 48
The US Congress withdrew two proposed bills—SOPA and PIPA—after coordinated widespread protests on January 18, 2012. Around the same time, the Anti-Counterfeiting Trade Agreement (ACTA) was successfully defeated by citizens in the European Union. Internet users (also known as citizens) were previously successful in preventing SOPA and PIPA from being signed into law. Online giants like Google and Wikipedia played a role in endorsing the protests. US Congress recalled SOPA and PIPA in February 2012.
- 49
All subsequent Michael Boldin/Nullify NSA quotes are from an e-mail correspondence with the authors, December 4, 2013.
- 50
"The Surveillance State Has an Achilles Heel," Nullify NSA's website.
- 51
Elizabeth Dvoskin and Frances Robinson, "NSA Internet Spying Sparks Race to Create Offshore Havens for Data Privacy," *Wall Street Journal*, September 27, 2013.
- 52
Caroline Copley, "Swisscom Builds 'Swiss Cloud' as Spying Storm Rages," *Reuters*, November 3, 2013.
- 53
"Freeports: Über-Warehouses for the Ultra-Rich," *Economist*, November 23, 2013.
- 54
Jonathan A. Obar, "Phantom Data Sovereigns: Walter Lippmann, Big Data and the Fallacy of Personal Data Sovereignty," Social Science Research Network website, March 25, 2013.
- 55
Zachary N. J. Peterson, Mark Gondree, and Robert Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data on the Cloud," *Usenix* (2013): 4.
- 56
See the extensive study: Anselm Franke, Eyal Weizman, and Ines Geisler, "Islands: The Geography of Extraterritoriality," *Archiv* 6 (December 2003): 19-21.

- 57
"John Perry Barlow on the Right to Know," YouTube video, 1:02:57, posted by "Forbes," February 1, 2012.
- 58
"Iceland: Cracks in the Crust," *Economist*, December 11, 2008.
- 59
"The Constitutional Council Hands Over the Bill for a New Constitution," *Stjornlagarad*, August 4, 2011.
- 60
"Iceland's Media Law: 'The Switzerland of Bits,'" *Economist*, June 17, 2010.
- 61
"Birgitta Jónsdóttir—Samara/Massey Journalism Lecture," YouTube video, 53:31, from a lecture at the Samara/Massey Journalism Seminar Series in Toronto on January 11, 2011, posted by "Samara Canada," July 21, 2011.
- 62
"Iceland: A Radical Periphery in Action."
- 63
Grimmelmann, e-mail to the authors, July 17, 2012.
- 64
Eleanor Saitta, e-mail to the authors, November 4, 2012.
- 65
Ryan Paul, "Pirate Bay Plans to Build Aerial Server Drones with \$35 Linux Computer," *Ars Technica* (blog), March 22, 2012.
- 66
Ernesto Van der Sar, "World's First Flying File-Sharing Drones in Action," *TorrentFreak* (blog), March 20, 2012.
- 67
"Electronic Countermeasures @ GLOW Festival NL 2011," Vimeo video, 3:49, posted by "liam young," 2011.
- 68
Ernesto Van der Sar, "The Pirate Bay Ships New Servers to Mountain Complex," *TorrentFreak* (blog), May 16, 2011.
- 69
"An Open Source Sky: Metahaven in Conversation with Liam Young," *Metahaven* (blog), January 30, 2013.
- 70
Franke et al., "Islands," 19-21.
- 71
Pierre Englebert and Denis M. Tull,

WHEN PIXELS BECOME TERRITORIES

- 1
"Anguished Dad's Open Letter to Putin: 'Thank You for Murdering My Child,'" *CBS News*, July 21, 2014.
- 2
Cited in Shaun Walker, "Moscow Braces for Economic Winter as Rouble Becomes a Standing Joke," *Guardian*, December 6, 2014.
- 3
Benedict Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (London: Verso, 2006), 85.
- 4
Benjamin Bratton's concept of "the Stack" is a comprehensive set of layers in which planetary computation has added to the existing configuration of territory and its inhabitants. The thesis is also a contemporary reiteration of Carl Schmitt's treatise, *The Nomos of the Earth* (1950)—itself an ambitious attempt to describe the world's political geography resulting from global spatial divisions beginning with the division of land. The correct translation of the Greek word *nomos*, explains Schmitt, is not so much "law," but the larger concept of "order." Schmitt's book is curious, Latin-ridden, impenetrable, and suspect as Schmitt omits the Second World War from the discussion. The Third Reich, a major twentieth-century attempt at achieving geopolitical totality, is not mentioned even once. Schmitt's academic reputation was tarnished for his alliance with the Nazis—while perhaps Leo Strauss and others at the University of Chicago just kept on reading him, as their own dirty little secret, until Schmitt was rediscovered by the Left through the work of the political theorist Chantal Mouffe. All the same, *The Nomos of the Earth* is heavily detailed. "For centuries," writes Schmitt, "humanity had a mythical image of the earth, but no scientific understanding of it as a whole." The concept of order, as opposed to law, is well explained by his account of European powers that, while perhaps still lacking a clear view of the entirety of the globe, had already constituted that every non-state territory they'd encounter outside

of Europe would be legitimately theirs. Europe founded a global order, or *nomos*, the *Jus Publicum Europaeum*. One could say that European powers could preemptively project super-jurisdiction on parts of the world over which they had no effective authority yet. Schmitt argues that the bracketing of European interstate war arose from “the emergence of a new spatial order—a balance of territorial states on the European continent in relation to the maritime British Empire and against the background of vast free spaces.” In other words, internal peace was guaranteed by an outside that was pretty much up for grabs. The recognition of the sea, as an order of its own as opposed to land, is equally prevalent in Schmitt’s account: “In the perspective of the *jus publicum europaeum*, all land on the earth belonged either to European states or to those of equal standing, or it was land free to be occupied, i.e., potential state territory or potential colonies. [...] The sea remained outside any specific state spatial order: it was neither state or colonial territory nor occupiable space. It was free of any type of state spatial sovereignty. [...] The sea had no borders other than coasts. It was the only territorial surface free of all states and open for trading, fishing, and the free pursuit of maritime wars and prize law, without regard to proximity or geographical borders.” Post-Schmitt, there is a valid comparison to be made of the sea’s *nomos* with the internet—more precisely, its cyber-utopian variation. The title of pirate, currently carried by Pirate Party members across Europe, still bears tribute to the analogy between the internet and the sea. The *nomos* of the latter was, writes Schmitt, “universal in its own right,” with its own concepts of “enemy, war, booty, and freedom.” The Pirate Bay, from which Pirate parties ultimately derived their title, represents (in regard to copyright and intellectual property) a liberation from previously existing moral and legal ties, just as sixteenth- and seventeenth-century pirates “reinterpreted” the principle that the oceans belong to all, from the Berlin Wall to the paywall. Pirate parties, the parliamentary political entities that

emerged out of the Pirate Bay then, so to speak, translated Pirate Bay beliefs into the coding language of liberal democracy, mostly as individual civil rights to privacy and information.

The stack’s *nomos* consists of layer upon layer of sprawling digital infrastructure: the earth is like a cake with layers of (digital and physical) icing. To begin with, the internet’s base structure of IP blocks and addresses assigned to territories on the globe creates a total map, an all-encompassing inside space to which no outside exists; there are no undiscovered IP addresses to match with undiscovered territories, so the space of conquest lies solely within newly assigned IP addresses to new entities on the network within existing territories. See Benjamin Bratton, *The Stack: On Software and Sovereignty* (MIT Press, forthcoming); and Carl Schmitt, *The Nomos of the Earth in the International Law of the Jus Publicum Europaeum*, trans. G. L. Ulmen (New York: Telos Press Publishing, 2003), 50, 141, 172, 175.

5

“Design and Geopolitics: The Alterglobal, Soft Power, and Disaster Capitalism: An Interview with Benjamin Bratton,” *Print* 65, no. 5 (October 2011): 62.

6

“‘She Annexes Your Heart’: Reasons Why Crimea Prosecutor Poklonskaya Not to Be Messed With,” *RT*, March 30, 2014.

7

“Super-Cute Crimean Prosecutor Becomes Japanese Meme,” YouTube video, 2:25, posted by “primetimeru,” March 20, 2014.

8

“Natalia Poklonskaya,” *knowyourmeme.com*, last updated in June 2014, by “Anotubus.”

9

“Itachi Kanade,” *Tokyo Otaku Mode*.

10

“Quick Draw Natalia Poklonskaya (Нармаля Поклоноская),” drawing by “Itachj,” *Itachi Kanade* (blog), March 17, 2014.

11

Itachj, March 19, 2014, comment on *ibid*.

12

“Re-Open Commission,” post by “Itachj,” August 18, 2013, 8:48 a.m., Itachi Kanade’s profile page on *deviantART*.

13

“I Get Recruited!,” post by “Itachj,” Itachi Kanade’s profile page on *deviantART*.

14

“Enjoykin—Nyash Myah,” YouTube video, 2:22, posted by “Enjoykin,” April 15, 2014.

15

“Crimean Prosecutor Music Clip Hits 3.7 Mn Views in Three Days,” *RT*, April 18, 2014.

16

Alexandra Garmazhapova, “(Pa)trolling the RuNet,” *openDemocracy*, May 22, 2014.

17

Jay Carney, cited in Jeff Mason and Arshad Mohammed, “Obama Blasts Russia in Tense Call with Ukraine,” *Reuters*, April 14, 2014.

18

Chris Elliot, “The Readers’ Editor on ... Pro-Russia Trolling below the Line on Ukraine Stories,” *Guardian*, May 4, 2014.

19

“Титлер 21 века: предсказание Ванги,” YouTube video, 0:59, posted by “Russian Topic News,” January 14, 2012.

20

Robert Mackey and Glenn Kates, “Russian Ad Compares Putin Foe to Hitler,” *The Lede* (New York Times blog), January 13, 2012.

21

“Transcript: Borodai Defends Ukraine Rebels over MH17,” *BBC*, July 24, 2014.

22

Harriet Salem, “The Other Side of the Same Coin: Mpet Moscow’s Parachute Politicians in Eastern Ukraine,” *Vice*, August 2, 2014.

23

Anderson, *Imagined Communities*, 86.

24

Sara Firth, interview by Nathalie Olah, “Sara Firth: ‘Why I Quit Russia Today Over Flight MH17,’” *Vice*, July 21, 2014.

25

WikiLeaks, “Rebels Complained Back in June that #Ukraine Was Using Passenger

Jets As Human Shields,” Twitter post, July 24, 2014, 6:42 a.m.

26

Cited in Simon Shuster, “WikiLeaks: Is Russia the Next Target?,” *Time*, November 1, 2010.

27

“Wikileaks: Russia Branded ‘Mafia State’ in Cables,” *BBC News*, December 2, 2010.

28

Roman Goncharenko, “Snowden’s Lawyer Is Putin Fan,” *Deutsche Welle*, November 6, 2013.

29

“Militia Soldier Elena, from Sloviansk English Subtitles,” YouTube video, 2:15, posted by “DES KIS,” December 11, 2014.

30

“Ukraine Crisis Wedding of Legendary Militia Soldier Motorola English Subtitles,” YouTube video, 3:12, posted by “DES KIS,” December 11, 2014.

31

Wills Robinson, “Now Rebel Commander Blamed for Downing MH17 Says ‘Bodies Aren’t Fresh’ Claiming Corpses at Crash Site Have Been ‘Dead for Days,’” *Daily Mail*, July 18, 2014.

32

Oleg Kashin, “The Most Dangerous Man in Ukraine Is an Obsessive War Reenactor Playing Now with Real Weapons,” trans. Ilya Lozovsky, *New Republic*, July 22, 2014.

33

Cited in Jill Dougherty, *Everyone Lies: The Ukraine Conflict and Russia’s Media Transformation*, Harvard University Shorenstein Center on Media, Politics and Public Policy Discussion Paper Series #D-88 (July 2014).

34

“Origin of the Separatists’ Buk: A Bellingcat Investigation,” *bellingcat*, November 8, 2014.

35

See Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia* (New York: Public Affairs, 2014).

36

Dougherty, *Everyone Lies*.

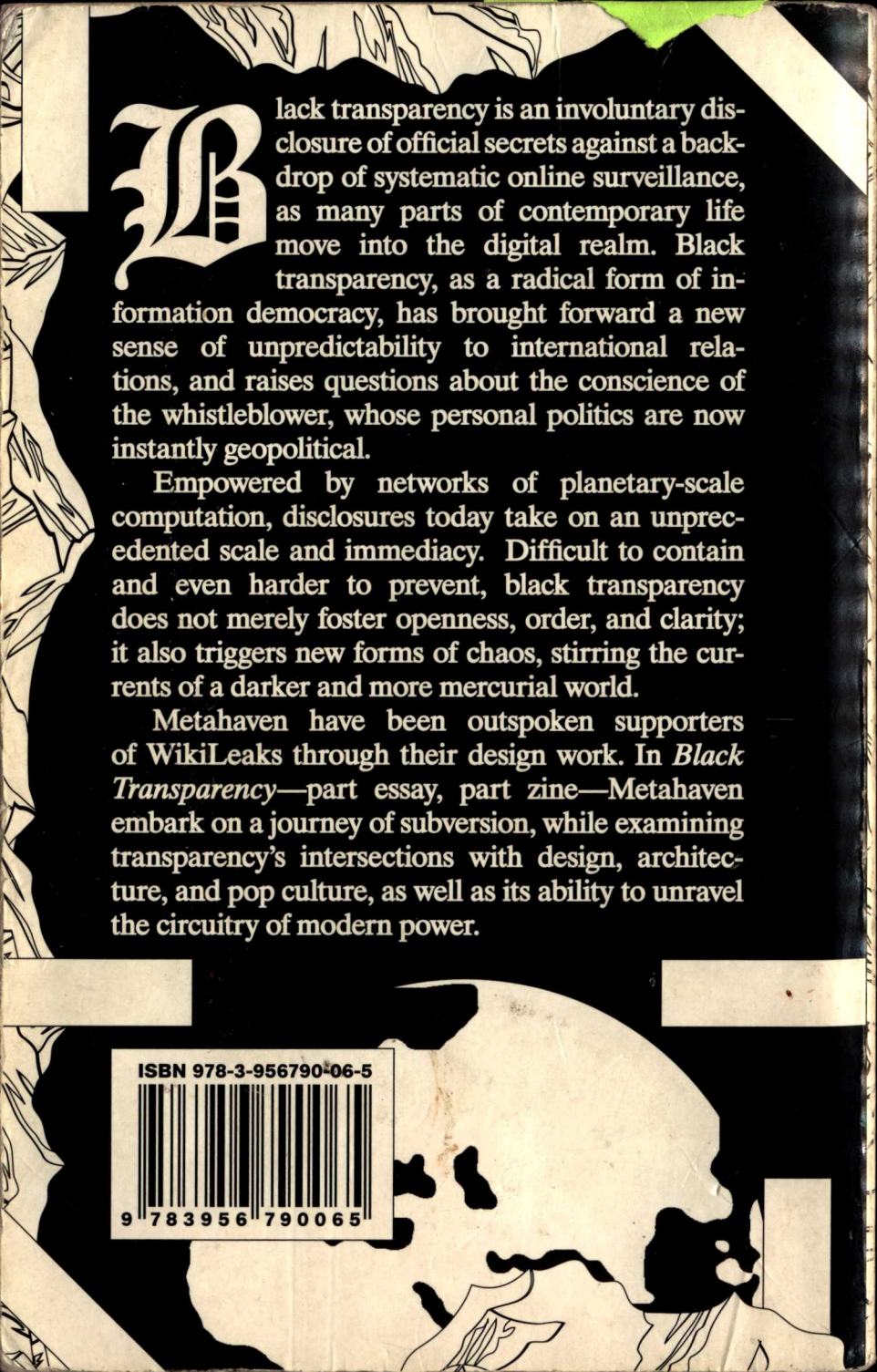
37

John Gravois, interview with Tess Vigeland, “With Crimean Borders in

Dispute, Google Maps Has It Both Ways,"
NPR Newscast, April 12, 2014.

38

Daniel van der Velden, "Basic
Necessities," in *Here There Everywhere*,
ed. Renny Ramakers and Agata Jaworska
(Amsterdam: Droog, 2014), 136.



Black transparency is an involuntary disclosure of official secrets against a backdrop of systematic online surveillance, as many parts of contemporary life move into the digital realm. Black transparency, as a radical form of information democracy, has brought forward a new sense of unpredictability to international relations, and raises questions about the conscience of the whistleblower, whose personal politics are now instantly geopolitical.

Empowered by networks of planetary-scale computation, disclosures today take on an unprecedented scale and immediacy. Difficult to contain and even harder to prevent, black transparency does not merely foster openness, order, and clarity; it also triggers new forms of chaos, stirring the currents of a darker and more mercurial world.

Metahaven have been outspoken supporters of WikiLeaks through their design work. In *Black Transparency*—part essay, part zine—Metahaven embark on a journey of subversion, while examining transparency's intersections with design, architecture, and pop culture, as well as its ability to unravel the circuitry of modern power.

ISBN 978-3-956790-06-5



9 783956 790065