22

Networked Reality Flow Hacks

PAOLO CIRIO

Media are hybridizing and multiplying quickly. There is awesome potential for jammers to intervene in the complex apparatus of networked media: Subtle messages and subversive memes flow through various media, reaching individuals and even power structures as never before. Images, videos, texts, maps, money: All forms of information flow as data in the networks, creating a massive informational environment in which we are all immersed.

The machines and software that process the flux of information flowing in the networks profoundly shape our existence. Global financial trading, just like our intimate relationships, is influenced by endless communications flowing through smart phones, e-mail inboxes, social media, instant news services, and mainstream media. Today, we use networked personal media for relating to each other, accessing knowledge, and organizing our personal lives and communities. By being constantly connected, people consume huge amounts of information while simultaneously feeding these networks with their personal data. People relate to their environments and each other mainly through networked media. Hence interventions in the flow of communications can influence power structures and shift perspectives in people's lives.

My project *Face to Facebook* (2011), developed in conjunction with Alessandro Ludovico, illustrates the potential of jamming the networked media by exploiting one of the most widely used social media platforms. Facebook documents the private lives of almost one billion persons all over the world, who share their intimate information and communicate in their most important social relationships using a social network owned by a private corporation. Consequently, Facebook has an incredible concentration of power over all these people, because Facebook holds and manages their data and their communications.

To subvert Facebook and disrupt its business and the trust that people put in it, we had to do a radical jamming action. I coded a little script that exploited a vulnerability of Facebook, enabling me to download one million public profiles of random Facebook users. It took months to harvest all the data; the script went automatically through thousands of profiles just by following friendship connections. The public data downloaded was just what is available on Google: name, surname, profile pictures, location, and likes. The second step of the project was to analyze the data gathered by processing all the pictures using custom-coded facial recognition software able to determine the gender of the person and his or her facial expression. At the end of this process the software found two hundred thousand faces and sorted them by six categories of temperaments for each gender. Our third step was to publish the sorted data on a custom-made fake dating website called Lovely-Faces.com. Thousands of random people from more than fifty countries were published on a cheesy dating website listed by presumed temperament, name, surname, location and personal likes, without knowing it.

As soon as we publicized the project through a press release to a few journalists, the news about the dating website Lovely-Faces.com went viral. After the first twenty-four hours the main German TV news channel and CNN covered the project, which caused the dating website to be flooded by people looking for their data.

The project was a culture jamming action against Facebook in that we subverted its primary resource: the data of the users and the relationships among them. However, it also became a social experiment, which was about looking at people's reactions when their data is provocatively used in another context without authorization. Through the website we received many messages from people—some angry insults (including five death threats), some enthusiastic support. (It's important to say that Lovely-Faces.com wasn't indexed by Google and we removed all the profiles of those who found themselves on the dating website. We didn't want to hurt anyone, and all the data was exposed only inside an artistic context.)

After two days, Facebook sent us a first cease-and-desist letter, asking us to shut down the dating website and delete all the "stolen" data; we were also banned from their services forever. We kept Lovely-Faces.com up for a week more before pulling it offline, because we couldn't afford a lawsuit. Facebook lawyers have continued to send us letters asking us to stop promoting the project.

Face to Facebook demonstrated the power of networked media flows and hacks today. On the one hand, it's possible to directly and intimately involve millions of people in a culture jamming project just though the network with which they are all connected. On the other hand, a subversive meme can spread globally in a very short span of time via mainstream and social media, influencing public opinion on issues regarding the whole society. Today memes flow by passing from node to node in networks; they are open to commentary and revision, and mutate as they circulate.

A few years later—in the wake of the global financial crisis of 2008–2009, Occupy Wall Street, and austerity debates—I launched another culture jamming project as a critical commentary on the increasing disparity in the distribution of wealth. *Loophole4All.com* (2013) promoted the sale of the real identities of over two hundred thousand anonymous Cayman Islands companies at low cost to democratize the privileges of offshore businesses in tax havens.

I hacked the governmental website of the Cayman Islands Company Register to compile a list of all companies registered in the major Caribbean offshore center. I made the data public for the first time, exposing it by digitally creating counterfeited certificates of incorporation documents for each company, all issued with my real name and signature. The counterfeit certificates were published on the website Loophole4All.com, where everyone was invited to hijack firms' identities by buying certificate of incorporations, starting at 99 cents, which would enable them to avoid taxes.

This massive corporate identity theft benefited from the legitimate Cayman companies' anonymous nature: The secrecy surrounding their real owners allows anyone to impersonate them. In short, this idea turned the main feature of offshore centers into a vulnerability, which was subsequently exploited by forging the legal paper documents of the certificate of incorporation.

This performance generated international media attention, engaged an active audience, and drew outrage from authorities on the Cayman Islands, global banks, the companies' real owners, international accounting firms, and law firms. I received ten international legal

threats and two cease-and-desist letters from Chinese firms for this artwork.

Using aggressive business strategies to compete against Cayman's incorporation services, the project set up a scheme to publish the stolen information through a company incorporated in City of London (Paolo Cirio Ltd.) and a data center in California, while the identities of the Cayman companies were sold through Luxembourg via PayPal.com to route the profit of the sale to Cirio's operational headquarters in Manhattan. The scheme took advantage of specific jurisdictions for legal liability, financial transactions, and publishing rights. I used physical mailboxes in the Caymans, London, and New York and set up most of this scheme through my passport, ultimately shielding my personal legal liability through my Italian citizenship.

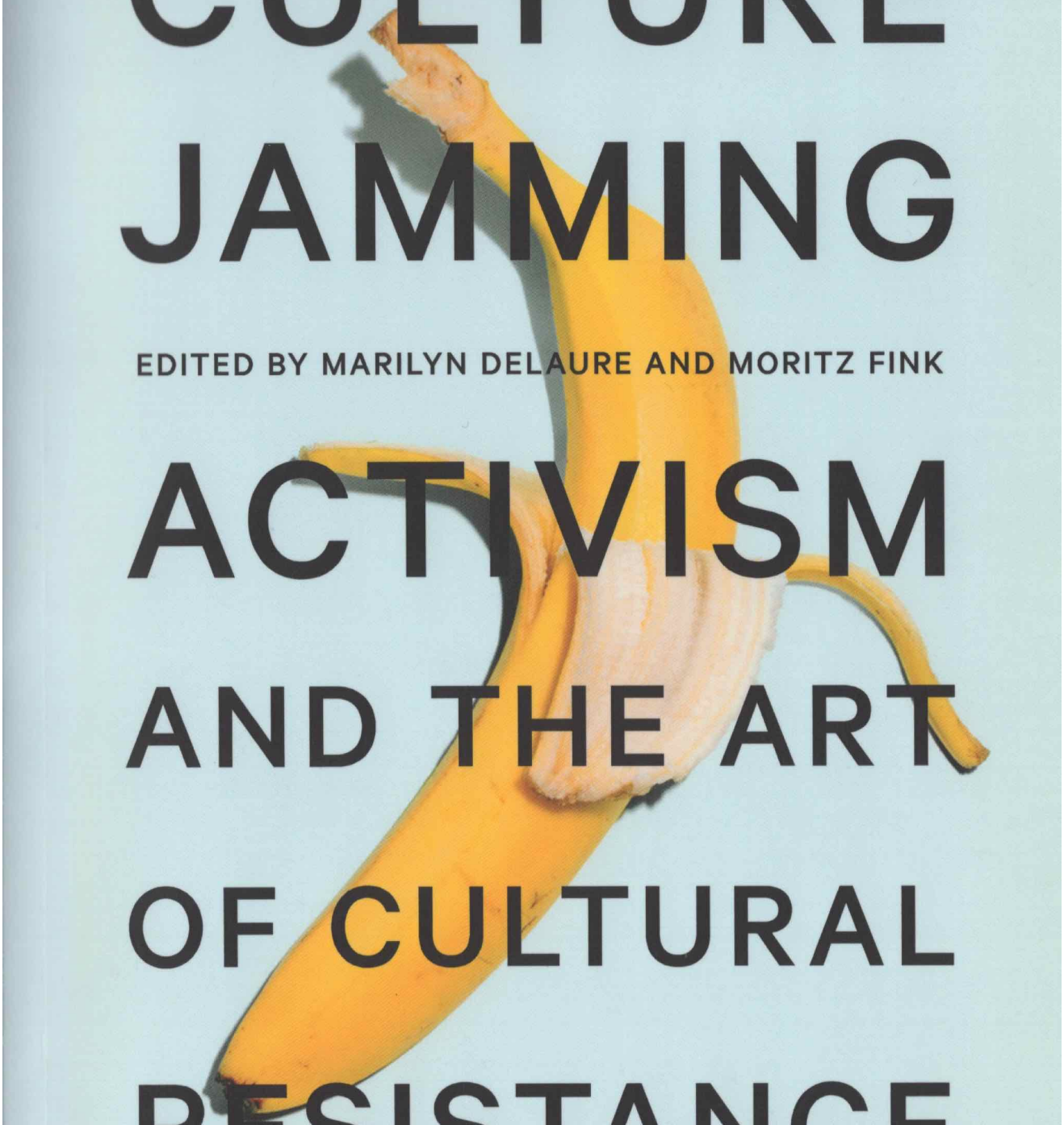
Loophole4All provocatively questions the transparency, secrecy, and anonymity of the global financial industry, exposing the mechanics of institutionalized illegality and the inequality of globalization, as well as some of the origins of austerity measures like budget cuts on public services and jobs in Western countries.

The website received significant amounts of traffic from India, Hong Kong, Singapore, and China. Not coincidentally, these countries are frequently involved in offshore centers like the Cayman Islands. Such offshore centers facilitate political corruption, misreport manufacturing costs and retail prices, and obfuscate foreign investments as tricks to maximize profit for the development of these new economic powers.

The infrastructure provided by new media and networked culture offers great possibilities for tech-savvy culture jammers. Hacking and phishing data can help create memes that reveal flawed policies and dishonest business practices inherent in the corporate world. As these memes spread, they awaken people to the injustices of existing power structures.

CULTURE JAMMING

EDITED BY MARILYN DELAURE AND MORITZ FINK



ACTIVISM AND THE ART OF CULTURAL RESISTANCE

WITH A FOREWORD BY MARK DERY