

Nathalie Maréchal, PhD

Networked Authoritarianism

How Data, Money, and
Repression Are Turning the
World Upside Down... And
How We Can Fight Back

Michael Cohen Secretly Taped Trump Discussing Payment to Playboy Model

By MATT APUZZO, MAGGIE HABERMAN and MICHAEL S. SCHMIDT LAST UPDATED: 12:58 PM ET

WASHINGTON — President Trump's longtime lawyer, Michael D. Cohen, secretly recorded a conversation with Mr. Trump two months before the presidential election in which they discussed payments to a former Playboy model who said she had an affair with Mr. Trump, according to lawyers and others familiar with the recording.

The F.B.I. seized the recording this year during a raid on Mr. Cohen's office. The Justice Department is investigating Mr. Cohen's involvement in paying women to tamp down embarrassing news stories about Mr. Trump ahead of the 2016 election. Prosecutors want to know whether that violated federal campaign finance laws, and any conversation with Mr. Trump about those



The Justice Department is investigating the involvement of President Trump's personal lawyer, Michael D. Cohen, in paying women to tamp down embarrassing news stories about Mr. Trump during the 2016 presidential campaign. JEENAH MOON/REUTERS

*When did you first realize we'd
slipped into an alternate timeline?*



NFL

MLB

NBA

NHL

NCAAF

NASCAR

ALL SPORTS

MORE

MLB HOME

VIDEO

PHOTOS

LISTS

SCORES

SCHEDULE

STANDINGS



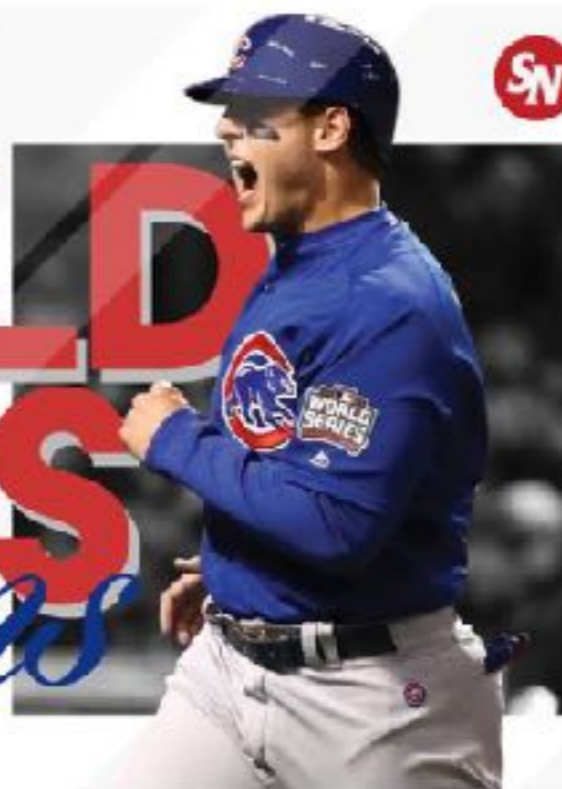
Cubs win World Series for first time in 108 years

MLB



CHICAGO CUBS

WORLD
SERIES
Champs



Getty Images

By **Justin McGuire**

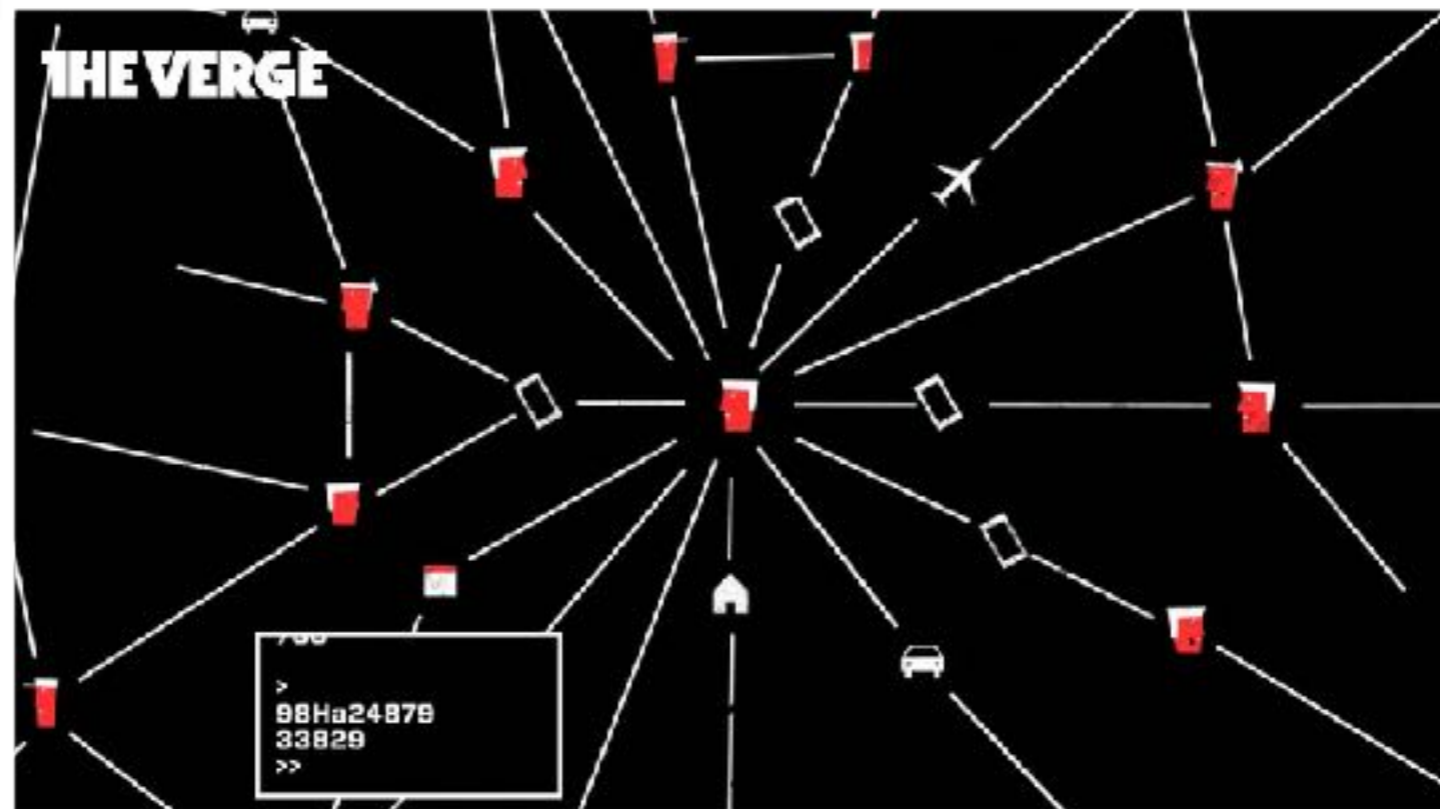


@JMcGuireSN

Published on Nov. 3, 2016

The curse is over. The Chicago Cubs are the World Series champs for the first time since 1908.

It gets worse...



PALANTIR HAS SECRETLY BEEN USING NEW ORLEANS TO TEST ITS PREDICTIVE POLICING TECHNOLOGY

Palantir deployed a predictive policing system in New Orleans that even city council members don't know about

By [Ali Winston](#) Feb 27, 2018, 3:25pm EST

Illustrations by [Garret Beard](#) and [Alex Castro](#)

[f](#) [t](#) [SHARE](#)

In May and June 2013, when New Orleans' murder rate was the sixth-highest in the United States, the Orleans Parish district attorney handed down two landmark racketeering indictments against dozens of men accused of membership in two violent Central City drug trafficking gangs, 3NG and the 110ers. Members of both gangs stood accused of committing 25 murders as well as several attempted killings and armed robberies.

Moviepass CEO Brags App Tracks Your Location Before and After Movies

Sidney Fussell • 3/05/18 4:52pm



Image: Darron Cummings (AP)

Under late capitalism, date night is now data night. Mitch Lowe, the CEO of Moviepass, [told an audience](#) last week that the app tracks user location, both before and after the movie. In his imaginatively titled keynote speech at the Entertainment Finance Forum, "Data is the New Oil: How will MoviePass Monetize It?" Lowe boasted about the "enormous" amount of data the "Netflix for movie theaters" app has on customers.

"We get an enormous amount of information," [Media Play News](#) first reported Lowe as saying. "We watch how you drive from home to the movies. We watch where you go afterwards."

Two question here: So does Moviepass actually track users' locations before and after they go see movies? If so, why?

Amazon Alexa recorded private conversation, sent it to random contact, woman says

By: Gary Horcher, KIRO7.com

Updated: May 24, 2018 - 7:32 AM

SEATTLE - A Portland, Oregon, family [contacted Amazon to investigate](#) after they say a private conversation in their home was recorded by Amazon's Alexa – the voice-controlled smart speaker – and the recorded audio was sent to the phone of a random person in Seattle, who was in the family's contact list.

"My husband and I would joke and say, 'I'd bet these devices are listening to what we're saying,'" said Danielle, who did not want [KIRO-TV](#) to use her last name.

Every room in her family home was wired with the Amazon devices to control her home's heat, lights and security system.

'Alexa, order me room service.' Amazon's voice assistant checks in to Marriott hotels

Jordan Valinsky

Next time you check in to a Marriott hotel, you might find an unexpected guest in your room: Alexa.

Amazon ([AMZN](#)) announced Tuesday a partnership with the hotel company to add Amazon Echo smart speakers into a select number of rooms.

Guests can use the Alexa-enabled device to order room service, turn on the lights, set alarms, notify housekeeping, ask for hotel information, call the front desk, play music and other typical Alexa functions.

In a promo video posted to [Amazon.com](#), a hotel guest is seen using various Echo models, such as the tall silo-shaped signature speaker and the hockey puck-sized Amazon Echo Dot.

Guests won't need an Amazon account to use the devices. But in the future, Amazon will allow them to sign in to their accounts to play their playlists and audiobooks.

[Related: Marriott cancels its 24-hour cancellation policy](#)

Having an Alexa device in a hotel room may make some guests feel uneasy -- but, in theory, they could unplug it. The gadget has sparked privacy concerns in recent years. In May, an Amazon Echo user based in Oregon [accused the device](#) of recording a conversation without their knowledge and sending it to a coworker.

In its [Alexa for Hospitality FAQs](#), Amazon briefly addresses privacy concerns, noting the microphone can be turned off and properties "can't listen to what you said to Alexa or what she said back."

[E-Commerce Guide by CNN Underscored: 10 super cool devices to use with](#)

Support The
Guardian

The
Guardian

News Opinion Sport Culture Lifestyle



Venmo: how the payment app exposes our private lives

A researcher has analysed millions of public transactions to prove just how much the app reveals about our life and habits

Olivia Solon in San Francisco

@oliviasolon Email

Tue 17 Jul 2018 03.01 EDT

Digital License Plates Roll Out In California

James Doubek • June 1, 2018 8:14 AM ET



A digital license plate made by Bay Area company Reviver Auto is displayed at the company's headquarters on May 30 in Foster City, Calif. The plates have the ability to track cars and play ads.

Justin Sullivan/Getty Images

California is testing new digital license plates on vehicles — opening up new possibilities and raising new privacy concerns.

The digital plates use the same technology behind Amazon's Kindle e-book reader to display large letters and numbers, as any other license plate would. But the devices are also able to show ads and personal messages and send data about their locations.

Sacramento is the first city to agree to test the technology. The city government received a shipment of 24 electric Chevrolet Bolts last week featuring the new plates, according to [The Sacramento Bee](#).

Facebook Gave Device Makers Deep Access to Data on Users and Friends

The company formed data-sharing partnerships with Apple, Samsung and dozens of other device makers, raising new concerns about its privacy protections.

By GABRIEL J.X. DANCE, NICHOLAS CONFESSORE and MICHAEL LaFORGIA JUNE 3, 2018



Facebook's chief executive, Mark Zuckerberg, at a Senate hearing in April. The company gave at least 60 phone and other device makers access to large amounts of user data. Leah Millis/Routers

As Facebook sought to become the world's dominant social media service, it struck agreements allowing phone and other device makers access to vast amounts of its users' personal information.

AT&T and Verizon both want to run massive ad-tracking networks to rival Facebook

Tracking everything that happens on your phone

By Nilay Patel | @reckless | May 30, 2016, 6:02pm EDT

f   SHARE



AT&T CEO Randall Stephenson spoke at the Code Conference today, where he took issue with the government's antitrust lawsuit blocking its purchase of Time Warner. Then he laid out exactly why he wants to buy it: to sell ads to the customers it already tracks.

[Time Warner's] Turner has an amazing inventory of advertising that they just kind of sell broadly. It's not a very targeted advertising approach. AT&T has an amazing amount of data — customer data for 40 million pay TV subscribers in North and South America, 130 million mobile subscribers, 16 million broadband subscribers. We have really great customer insight on what kind of shows and media content they're viewing, where they are, all kinds of information on the consumer. Can you pair a very formidable ad inventory with a very formidable amount of data and information on the customer — viewership data and all kinds of other information — and can you create something unique just from a straight advertising platform and change how you're monetizing content?



BY
ED JEFFERSON

SCIENCE & TECH 27 APRIL 2018

No, China isn't Black Mirror – social credit scores are more complex and sinister than that

In China and elsewhere, the implied threat isn't the tyranny of the crowd, but state and corporate power.

SIGN-UP

What a gift Charlie Brooker's dystopian series *Black Mirror* has been to journalists: any time a reporter covers a story about even vaguely dystopian technology, the main thing they have to do is determine which episode of *Black Mirror* it's like, saving everyone the bother of finding out what's really going on.

For instance: '*Black Mirror is coming true in China*', '*Black Mirror's chilling social credit score is a reality in China*', '*A 'Black Mirror' Episode Is Coming to Life in China*'. The story here, apparently, is that the

f Facebook

🐦 Twitter

Reddit

✉ Email

🖨 Print

Networked Authoritarianism

CHINA'S "NETWORKED AUTHORITARIANISM"

Rebecca MacKinnon

When an authoritarian regime embraces and adjusts to the inevitable changes brought by digital communications, the result is what I call “networked authoritarianism.” In the networked authoritarian state, the single ruling party remains in control while a wide range of conversations about the country’s problems nonetheless occurs on websites and social-networking services. The government follows this online chatter, and sometimes people are able to use the Internet to call attention to social problems or injustices and even manage to have an impact on government policies. As a result, the average person with Internet or mobile access has a much greater sense of freedom—and may feel that he has the ability to speak and be heard—in ways that were not possible under classic authoritarianism. At the same time, in the networked authoritarian state, there is no guarantee of individual rights and freedoms. Those whom the rulers see as threats are jailed; truly competitive, free, and fair elections are not held; and the courts and the legal system are tools of the ruling party.

Journal of Democracy Volume 22, Number 2 April 2011

© 2011 National Endowment for Democracy and The Johns Hopkins University Press

Article

Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy

Nathalie Marechal

Annenberg School for Communication and Journalism, University of Southern California, Los Angeles, CA 90007, USA.
E-Mail: marechal@usc.edu

Submitted: 30 October 2015 | Accepted: 6 February 2017 | Published: 27 March 2017

Abstract

In the aftermath of the 2016 U.S. election, researchers, policymakers and the general public are grappling with the notion that the 45th president of the United States may very well owe his electoral victory to a sophisticated propaganda effort masterminded by the Kremlin. This article synthesizes existing research on Russia's domestic information controls, its internet policy at the global level (notably via internet governance processes), and the country's resurgence as a major geopolitical player to argue that policymakers as well as the general public should consider these themes holistically, particularly as they formulate responses to what many see as the Russian threat to Western liberal democracy. Russia may have lost the Cold War, but it is now waging information warfare against the liberal democracies of Europe and North America in a sophisticated bid to win the next round. Russia does not view internet governance, cybersecurity and media policy as separate domains. Rather, all the areas covered by these disciplines fall under "information security" for Russian foreign policy. The paper begins by tracing the history of information controls within what is now the Russian Federation before discussing the role of information and internet policy in Russian foreign policy, drawing connections between the Russian government's control and manipulation of information—including its internet policy—in the domestic and international arenas. Next, it discusses the spread of networked authoritarianism and suggests that a "geopolitics of information" will become increasingly necessary in the coming years. Just as networked authoritarianism establishes strategic infrastructures to control the message domestically and intervene in global media systems, liberal democracies need to rethink media and communication infrastructures to ensure they foster pluralistic, rights-respecting societies that are resilient to authoritarianism and extremism. In doing so, they should resist the temptation to respond to this threat in ways that will erode democracy even further, such as expanded surveillance and limits on free expression.

Keywords

2016 election; censorship; data localization; human rights; networked authoritarianism; propaganda; Russia; surveillance

Issue

This article is part of the issue "Post-Snowden Internet Policy" edited by Julia Poole (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

© 2017 by the author; licensee Cogitatio (Lisbon, Portugal). This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

1. Introduction

After a long and bitter electoral campaign, the results of the 2016 U.S. election have precipitated an ongoing constitutional crisis, and continued uncertainty about the role of Russia's government in Donald Trump's electoral victory has prompted renewed interest in Russia, a country that hadn't been at the forefront of the national agenda since the end of the Cold War. Several factors contribute to making the current situation a per-

fect storm of uncertainty and ambiguity, including: policymakers' and the public's comparative lack of knowledge about Russia; the difficulty of parsing out something resembling empirical truth from the jumble of official statements, leaks, speculations and claims made by the various actors involved; the tumultuous presidential transition; and the arcane nature of the empirical claims underlying the web of controversy surrounding the election and any role Russia might have had in influencing the result. It will take time and serious effort for the dust

Fake, misleading social media posts exploding globally, Oxford study finds

By Greg Gordon ggordon@mcclatchydc.com • WASHINGTON

By continuing to use this site, you give your consent to our use of cookies for analytics, personalization and ads. [LEARN MORE](#)



FILE - This Nov. 1, 2017, file photo shows some of the Facebook and Instagram ads linked to a Russian effort to disrupt the American political process and stir up tensions around divisive social issues, released by members of the U.S. House Intelligence committee, are photographed in Washington. Facebook says it will require political advertisers in the U.S. to label "issue ads" that disclose who paid for them, part of its ongoing efforts to prevent elections-related misuse of its platform. Such ads played prominently in Russia's efforts to interfere in the 2016 U.S. elections. Jon Elswick, File AP Photo

Russia's social media blitz to influence the 2016 U.S. election was part of a global "phenomenon" in which a broad spectrum of governments and political parties used Internet platforms to spread junk news and disinformation in at least 48 countries last year, an Oxford University study has found.

Including U.S. government programs aimed at countering extremists such as Islamic fundamentalists, about \$500 million has been spent worldwide on



Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation

Samantha Bradshaw, *University of Oxford*
Philip N. Howard, *University of Oxford*



EXECUTIVE SUMMARY

The manipulation of public opinion over social media platforms has emerged as a critical threat to public life. Around the world, a range of government agencies and political parties are exploiting social media platforms to spread junk news and disinformation, exercise censorship and control, and undermine trust in the media, public institutions, and science. At a time when news consumption is increasingly digital, artificial intelligence, big data analytics, and “black-box” algorithms are being leveraged to challenge truth and trust: the cornerstones of our democratic society.

In 2017, the first Global Cyber Troops inventory shed light on the global organization of social media manipulation by government and political party actors. This 2018 report analyses the new trends of organized media manipulation, and the growing capacities, strategies and resources that support this phenomenon. Our key findings are:

1. We have found evidence of formally organized social media manipulation campaigns in 48 countries, up from 28 countries last year. In each country there is at least one political party or government agency using social media to manipulate public opinion domestically.
2. Much of this growth comes from countries where political parties are spreading disinformation during elections, or countries where government agencies feel threatened by junk news and foreign interference and are responding by developing their own computational propaganda campaigns in response.
3. In a fifth of these 48 countries—mostly across the Global South—we found evidence of disinformation campaigns operating over chat applications such as WhatsApp, Telegram and WeChat.
4. Computational propaganda still involves social media account automation and online commentary teams, but is making increasing use of paid advertisements and search engine optimization on a widening array of Internet platforms.
5. Social media manipulation is big business. Since 2010, political parties and governments have spent more than half a billion dollars on the research, development, and implementation of psychological operations and public opinion manipulation over social media. In a few countries this includes efforts to counter extremism, but in most countries this involves the spread junk news and misinformation during elections, military crises, and complex humanitarian disasters.

How did we get here?



Through the looking glass

JOHN FEFFER and TOM ENGELHARDT 28 May 2015

The planet currently seems to be on the cusp of a decidedly unharmonic convergence. Did 'Market-Leninism' win the Cold War?



Francis Fukuyama. Demotix/Sergii Kharchenko. All rights reserved.



er of Foreign Policy In Focus, offers a
the Cold War era: a crowd of thinkers

Back in the 1960s and 1970s, however, this was a rather conventional view, at least among influential thinkers like economist John Kenneth Galbraith who predicted that the United States and the Soviet Union would converge at some point in the future with the market tempered by planning and planning invigorated by the market. Like many an academic notion, it didn't come to pass. The United States veered off in the direction of Reaganomics. And the Soviet Union eventually collapsed. So much for 'convergence theory', which like EST or cold fusion went the way of most crackpot ideas.

Or did it? Take another look at our world in 2015 and tell me if, somehow we haven't backed our way through the looking glass into that very alternative universe – with a twist. The planet currently seems to be on the cusp of a decidedly unharmonic convergence.

Consider what's happening in Russia, where an elected autocrat presides over a free market shaped by a powerful state apparatus. Similarly, China's mash-up of market Leninism offers a one-from-column-A-and-one-from-Column-B combination platter. Both countries are also rife with crime, corruption, growing inequality, and militarism. Think of them as the un-Swedens.

Nor do such hybrids live only in the east. Hungary, a member of the European Union and a key post-Communist adherent to liberalism, has been heading off in an altogether different direction since its ruling Fidesz party took over in 2010. Last July, its prime minister, Viktor Orbán, [declared](#) that he no longer looks to the west for guidance. To survive in an ever more competitive global economy, Orbán is seeking inspiration from various hybrid powers, the other un-Swedens of our planet: Turkey, Singapore, and both Russia and China. Touting the renationalization of former state assets and stricter controls on foreign investment, he has promised to remake Hungary into an 'illiberal state' that both challenges laissez-faire principles and concentrates power in the leader and his party.



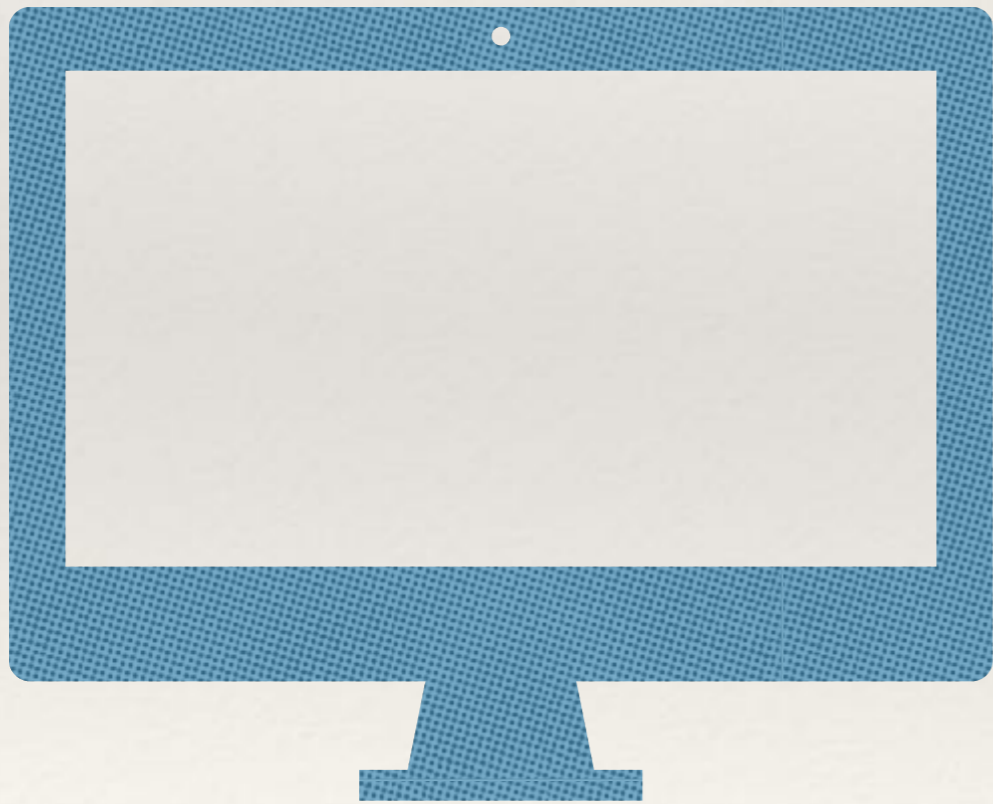
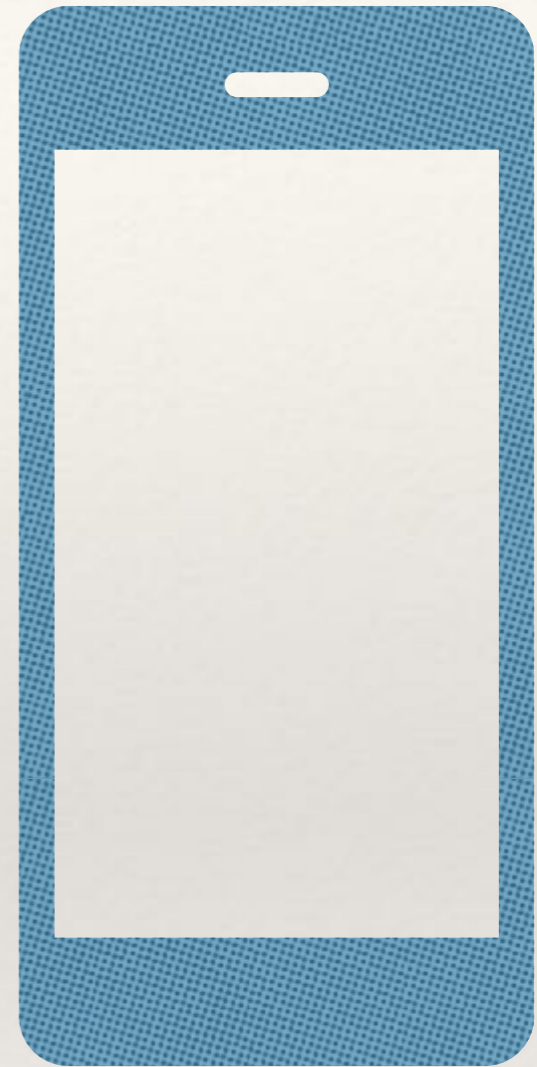
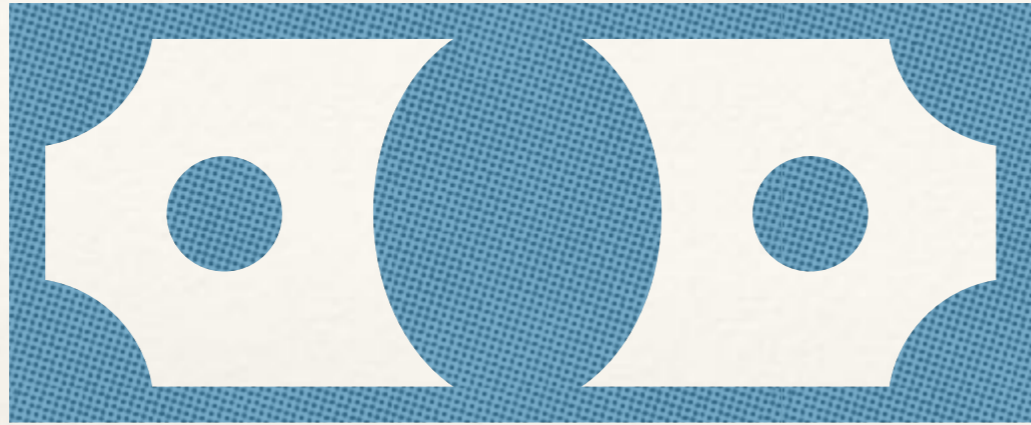
The United States is not exactly immune from such trends. The state has also become quite illiberal here as its reach and power have been expanded in striking ways. As it happens, however, America's *Gosplan*, our state planning committee, comes with a different name: the military-industrial-homeland-security complex. Washington presides over a planet-spanning surveillance system that would have been the envy of the Communist apparatchiks of the previous century, even as it has imposed a global economic template on other countries that enables enormous corporate entities to elbow aside local competition. If the American tradition of liberalism and democracy was once all about 'the little guy' – the rights of the individual, the success of small business – the United States has gone big in the worst possible way.

The convergence theorists imagined that the better aspects of capitalism and communism would emerge from the Darwinian competition of the Cold War and that the result would be a more adaptable and humane hybrid. It was a typically Panglossian error. Instead of the best of all possible worlds, the international community now faces an unholy trinity of authoritarian politics, cut-throat economics, and Big Brother surveillance. Even though we might all be eating off IKEA tableware, listening to Spotify, and reading the latest *Girl With the Dragon Tattoo* knock-off, we are not living in a giant Sweden. Our world is converging in a far more dystopian way. After two successive conservative governments and with a surging far-right party pounding [its anti-immigrant drumbeat](#), even Sweden seems to be heading in the same dismal direction.



Instead of converging toward Scandinavian socialism, the US has been slouching toward illiberalism for some time now. The Tea Party bemoans the “nanny” and “gun-control” state, but misses the deeply sinister ways in which that state has been captured by the forces of illiberality. The United States has expanded its archipelago of incarceration, our homegrown gulag, so dramatically that we have [more people](#) in prison – in total and by percentage of population – than any developed country on Earth. Our political system has been taken over by a [club of the rich](#) – our own *nomenklatura* – with corruption so embedded that no one dares call it by that name and critics instead speak of the “revolving door” and “voter suppression” and the “influence of money in politics”. The deterioration of public infrastructure has, as in the Soviet Union in the 1970s, turned the country into [an embarrassment](#) of falling bridges, exploding gas lines, bursting pipelines, backward railroads, unsecured power plants, and potential ecological catastrophes.

Add in spreading governmental surveillance and secrecy, unsustainable military spending, and a [disastrously interventionist](#), military-first foreign policy and the United States is looking a lot like either the old Soviet Union or the Russia of today. Neither is a flattering comparison. America has not yet descended into despotism, so the convergence is hardly complete. But it might be only one right-wing populist leader away from that worst-case scenario.



LIBERATION TECHNOLOGY

Larry Diamond

Optimists discern in these events a striking ability of the Internet—and other forms of “liberation technology”—to empower individuals, facilitate independent communication and mobilization, and strengthen an emergent civil society. Pessimists argue that nothing in China has fundamentally changed. The Chinese Communist Party (CCP) remains firmly in control and beyond accountability. The *weiquan* movement has been crushed. And the Chinese state has developed an unparalleled system of digital censorship.

Both perspectives have merit. Liberation technology enables citizens to report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom. But authoritarian states such as China, Belarus, and Iran have acquired (and shared) impressive technical capabilities to filter and control the Internet, and to identify and punish dissenters. Democrats and autocrats now compete to master these technologies. Ultimately, however, not just technology but political organization and strategy and deep-rooted normative, social, and economic forces will determine who “wins” the race.

Liberation technology is any form of information and communication technology (ICT) that can expand political, social, and economic freedom.

Journal of Democracy Volume 21, Number 3 July 2010

© 2010 National Endowment for Democracy and The Johns Hopkins University Press

LIBERATION TECHNOLOGY

Larry Diamond

It is tempting to think of the Internet as unprecedented in its potential for political progress. History, however, cautions against such hubris. In the fifteenth century, the printing press revolutionized the accumulation and dissemination of information, enabling the Renaissance, the Protestant Reformation, and the scientific revolution. On these foundations, modern democracy emerged. But the printing press also facilitated the rise of the centralized state and prompted the movement toward censorship.³ A century and a half ago, the telegraph was hailed as a tool to promote peace and understanding. Suddenly, the world shrank; news that once took weeks to travel across the world could be conveyed instantly. What followed was not peace and freedom but the bloodiest century in human history. Today's enthusiasts of liberation technology could be accused of committing the analytic sins of their Victorian forebears, "technological utopianism" and "chronocentricity"—that is, "the egotism that one's own generation is poised on the very cusp of history."⁴

Journal of Democracy Volume 21, Number 3 July 2010

© 2010 National Endowment for Democracy and The Johns Hopkins University Press

LIBERATION TECHNOLOGY

Larry Diamond

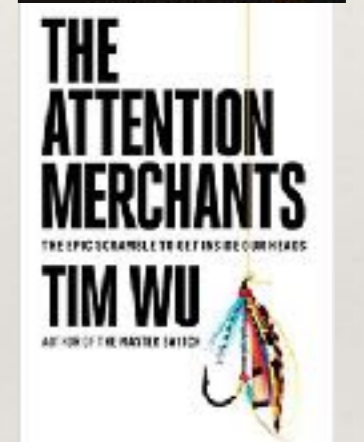
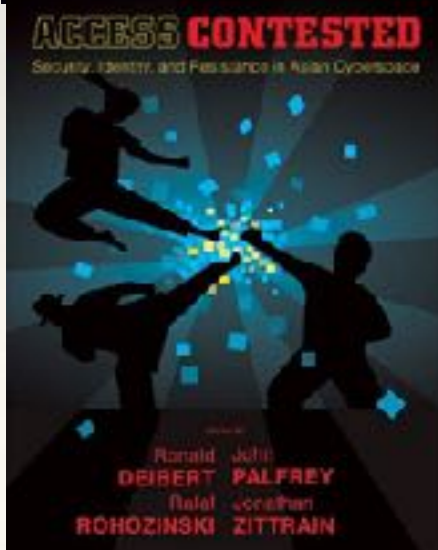
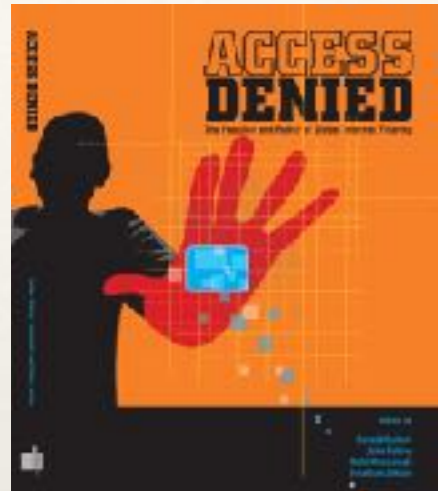
Mobilizing against authoritarian rule represents only one possible “liberating” use of digital ICT. Well before mobilization for democracy peaks, these tools may help to widen the public sphere, creating a more pluralistic and autonomous arena of news, commentary, and information. The new ICTs are also powerful instruments for transparency and accountability, documenting and deterring abuses of human rights and democratic procedures. And though I cannot elaborate here, digital ICT is also liberating people from poverty and ill health: conveying timely information about crop prices, facilitating microfinance for small entrepreneurs, mapping the outbreaks of epidemics, and putting primary healthcare providers in more efficient contact with rural areas.⁵

Journal of Democracy Volume 21, Number 3 July 2010

© 2010 National Endowment for Democracy and The Johns Hopkins University Press

5 generations of information controls

- ❖ 1st gen: access restrictions & DNS blocking (Deibert et al., 2008, 2010, 2011)
- ❖ 2nd gen: “Just-in-time” blocking, internet shutdowns (Deibert et al., 2008, 2010, 2011)
- ❖ 3rd gen: disinformation & propaganda (Deibert et al., 2008, 2010, 2011)
- ❖ 4th gen: (re) territorialization of internet governance (Deibert, 2016)
- ❖ 5th gen: attention hacking (Tufekci, 2017; Wu, 2016)



Surveillance Capitalism

- ❖ The business model for the internet
- ❖ How we get “free” content and services
- ❖ ... but also an infrastructure for total social control

Research article

Big other: surveillance capitalism and the prospects of an information civilization

Shoshana Zuboff^{1,2}

¹Harvard Business School Emerita, Boston, MA, USA;

²Berkman Center for Internet and Society, Cambridge, MA, USA

Correspondence:

S Zuboff, Berkman Center for Internet and Society, Cambridge, MA, USA.

E-mail: Szuboff@hbs.edu

Abstract

This article describes an emergent logic of accumulation in the networked sphere, ‘*surveillance capitalism*,’ and considers its implications for ‘information civilization.’ The institutionalizing practices and operational assumptions of Google Inc. are the primary lens for this analysis as they are rendered in two recent articles authored by Google Chief Economist Hal Varian. Varian asserts four uses that follow from computer-mediated transactions: ‘data extraction and analysis,’ ‘new contractual forms due to better monitoring,’ ‘personalization and customization,’ and ‘continuous experiments.’ An examination of the nature and consequences of these uses sheds light on the implicit logic of surveillance capitalism and the global architecture of computer mediation upon which it depends. This architecture produces a distributed and largely uncontested new expression of power that I christen: ‘Big Other.’ It is constituted by unexpected and often illegible mechanisms of extraction, commodification, and control that effectively exile persons from their own behavior while producing new markets of behavioral prediction and modification. Surveillance capitalism challenges democratic norms and departs in key ways from the centuries-long evolution of market capitalism.

Journal of Information Technology (2015) **30**, 75–89. doi:10.1057/jit.2015.5

Keywords: surveillance capitalism; big data; Google; information society; privacy; internet of everything

Introduction

A recent White House report on ‘big data’ concludes, ‘The technological trajectory, however, is clear: more and more data will be generated about individuals and will persist under the control of others’ (White House, 2014: 9). Reading this statement brought to mind a 2009 interview with Google Chairperson Eric Schmidt when the public first discovered that Google retained individual search histories that were also made available to state security and law enforcement agencies, ‘If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time ... It is possible that that information could be made available to the authorities’ (Newman, 2009). What these two statements share is the attribution of agency to ‘technology.’ ‘Big data’ is cast as the inevitable consequence of a technological juggernaut with a life of its

Most articles on the subject of ‘big data’ commence with an effort to define ‘it.’ This suggests to me that a reasonable definition has not yet been achieved. My argument here is that we have not yet successfully defined ‘big data’ because we continue to view it as a technological object, effect or capability. The inadequacy of this view forces us to return over and over to the same ground. In this article I take a different approach. ‘Big data,’ I argue, is not a technology or an inevitable technology effect. It is not an autonomous process, as Schmidt and others would have us think. It originates in the social, and it is there that we must find it and know it. In this article I explore the proposition that ‘big data’ is above all the foundational component in a deeply intentional and highly consequential new logic of accumulation that I call *surveillance capitalism*. This new form of information capitalism aims to predict and modify human behavior as a means to produce revenue and market control. Surveillance capitalism

How the NSA collects your data

Content

Metadata

Info Sharing

Upstream

SOURCES

Telecommunications Cables

AT&T

VERIZON

SPRINT

FACEBOOK

APPLE

GOOGLE

MICROSOFT

YAHOO

AOL

PATRIOT ACT
Section 215

FISA AMENDMENTS ACT
Section 702

NSA



FAIRVIEW, STORMBREW,
BLARNEY, AND OAKSTAR
("Upstream" Data)

PRISM
(Internet Content)

MARINA
(Internet Metadata)

MOONLIGHTPATH
(Internet Metadata,
planned Sept. 2013)

MAINWAY
(Phone Metadata)

NUCLEON
(iPhone Content)

SHELLTRUMPET &
EVILOLIVE
(Internet Metadata)

SPINNARET
(Internet Metadata,
planned Sept. 2013)



why are black women so



why are black women so angry
why are black women so loud
why are black women so mean
why are black women so attractive
why are black women so lazy
why are black women so annoying
why are black women so confident
why are black women so sassy
why are black women so insecure

ALGORITHMS OF OPPRESSION

HOW SEARCH ENGINES
REINFORCE RACISM

SAFIYA UMOJA NOBLE

"This book is downright scary—but...you will emerge smarter and more empowered to demand justice." —NAOMI KLEIN



AUTOMATING INEQUALITY

HOW HIGH-TECH TOOLS PROFILE,
POLICE, AND PUNISH THE POOR



VIRGINIA EUBANKS



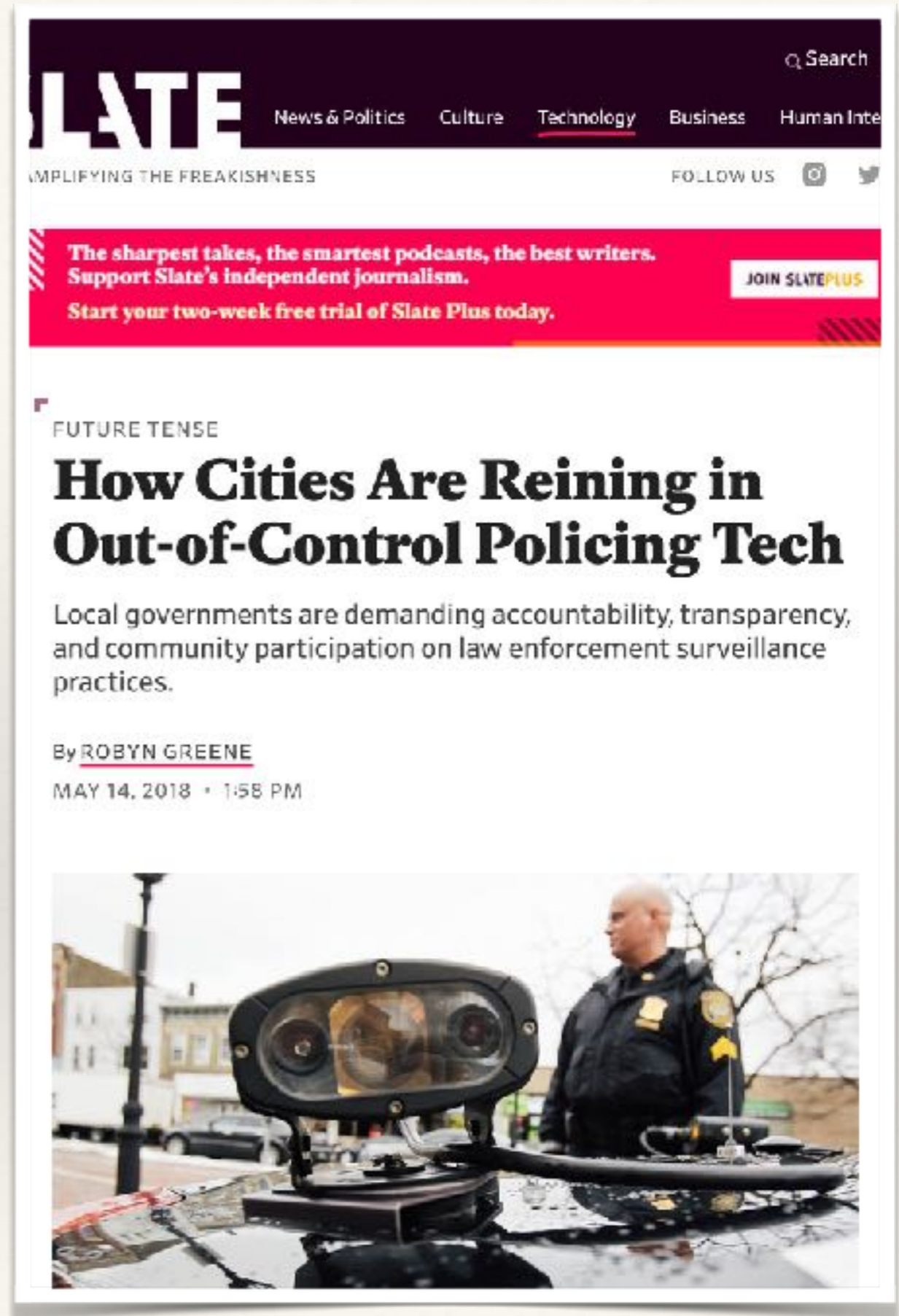
Cambridge
Analytica

So what do we do about it ?

Think Global, Act Local

Legislation Regulation

- ❖ City level
- ❖ State / provincial level
- ❖ National level
- ❖ Supra-national



The image shows a screenshot of a Slate website article. At the top, the Slate logo is visible in white on a dark background, with navigation links for 'News & Politics', 'Culture', 'Technology', 'Business', and 'Human Inte'. A search bar is in the top right. Below the navigation, a red banner promotes 'Slate Plus' with the text: 'The sharpest takes, the smartest podcasts, the best writers. Support Slate's independent journalism. Start your two-week free trial of Slate Plus today.' and a 'JOIN SLATEPLUS' button. The article title is 'How Cities Are Reining in Out-of-Control Policing Tech' under the 'FUTURE TENSE' category. The author is 'ROBYN GREENE' and the date is 'MAY 14, 2018 • 1:58 PM'. The article text begins with 'Local governments are demanding accountability, transparency, and community participation on law enforcement surveillance practices.' Below the text is a photograph of a police officer in a dark uniform standing next to a police car. The car's dashboard is visible in the foreground, featuring a large, circular, dual-lens camera or sensor unit mounted on it.

Think Global, Act Local

Legislation Regulation

- ❖ City level
- ❖ State/provincial level
- ❖ National level
- ❖ Supra-national



California's privacy law a commendable step toward national standard

BY DANIEL SEPULVEDA AND DIPATAN GHOSH, OPINION CONTRIBUTORS — 07/18/18 12:40 PM EDT
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

4 COMMENTS

Just In...

House Dems want answers on cuts to ObamaCare outreach groups

HEALTHCARE — 2655 AGO

Dem lawmaker's office rehired aide after dismissing him over sexual harassment allegations; report

HOUSE — 6H 473 AGO

Intel chief unaware Trump was planning to meet with Russians in Oval Office

NATIONAL SECURITY — 16M 705 AGO

Andrea Mitchell breaks news to US intel chief that Putin is coming to DC

NATIONAL SECURITY — 16M 123 AGO

Intel head: There's a 'risk' that Putin recorded meeting with Trump

NATIONAL SECURITY — 11M 35 AGO

Top intel chief: I don't know what Trump, Putin discussed in meeting

NATIONAL SECURITY — 24M 505 AGO

Pollster: Images of migrant families at the border made the issue non-partisan

WHAT AMERICANS THINKING — 26M 175 AGO

2 DISARDS

f SHARE

TWEET

PLUG ONE



© Getty Images

California has passed a baseline consumer privacy law called the California Consumer Privacy Act — the first ever to make it into statute in any American state. The politics triggering this development were intriguing: a real estate developer seized on the public sentiments induced by the Cambridge Analytica incident and took on Silicon Valley's titans, funding a \$3 million campaign for a ballot initiative to legislate sweeping new privacy reforms.

Boxed in by the popularity of the initiative, internet-based and internet-dependent companies — which are most affected by privacy legislation because their business models are premised on access to personal data — were forced to accept the reality that some form of privacy legislation would pass. Hereafter, California lawmakers worked feverishly to construct a bill that could be more workable for businesses than the ballot initiative but which would still protect individual privacy. The law was negotiated, written, and passed in a previously unimaginable period of just seven days.



It is frustrating that such an important law was developed in such a short period of time; situations like these can result in unintended consequences, loopholes, or lax protections for consumers. It will have implications for all Americans;



Most Popular

1 Whoopi Goldberg, Jeanine Pirro get...

3,750 SHARES

2 Mueller releases list of more than...

2,518 SHARES



3 George Will charges that Trump...

1,600 SHARES

4 Opinion: One FBI text message in...


702 SHARES

LOAD MORE

Think Global, Act Local

Legislation Regulation

- ❖ City level
- ❖ State / provincial level
- ❖ National level
- ❖ Supra-national

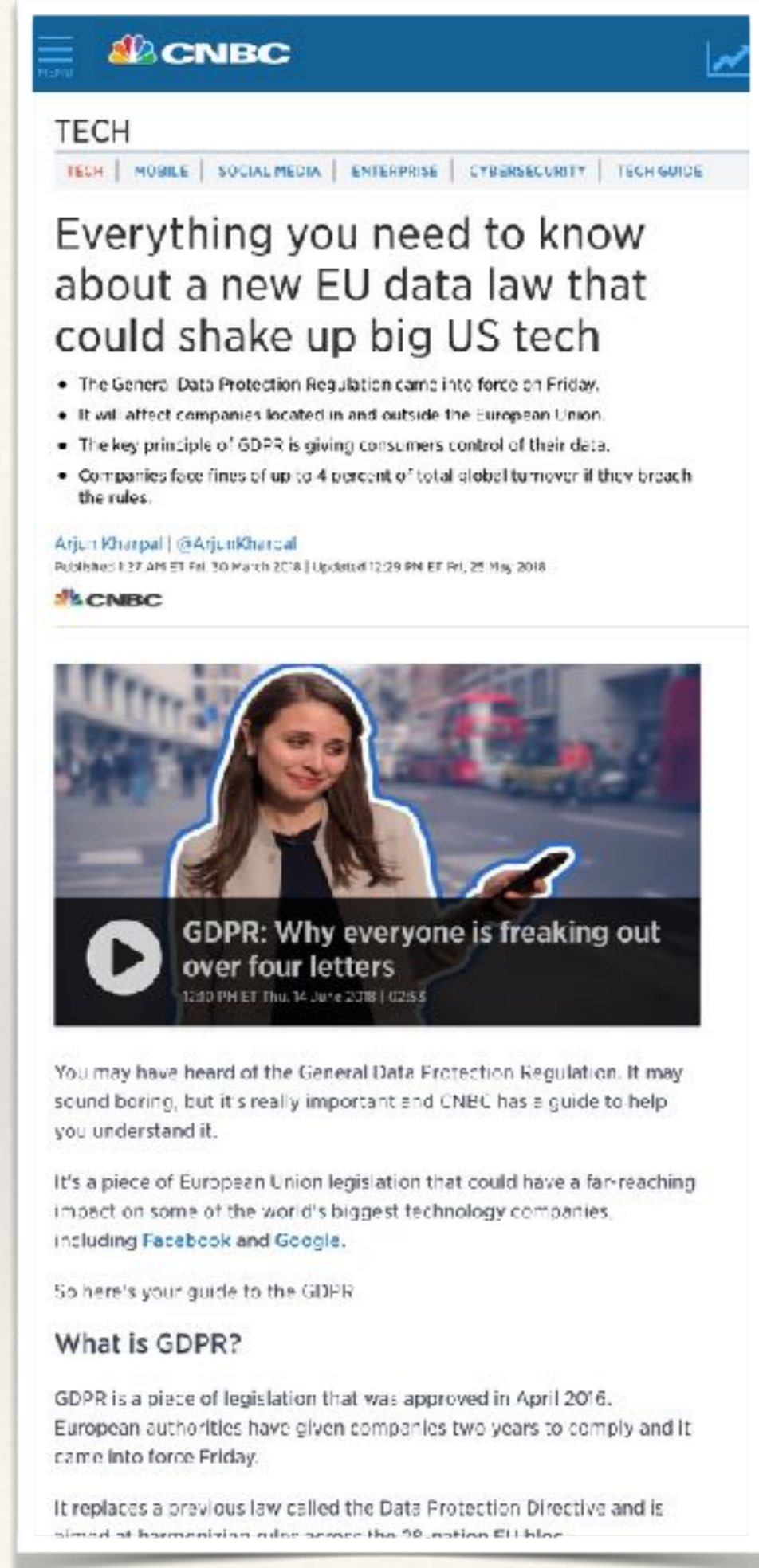


The image is a screenshot of a Quartz news article. At the top, there are social media icons for Facebook and Twitter, the Quartz logo, and an email icon. The article title is "Facebook's quiet battle to kill the first transparency law for online political ads" in a large, bold, black font. Above the title is the sub-header "ACTIONS SPEAK LOUDER" in blue. Below the title, the authors "By Heather Timmons & Hanna Kozłowska" and the date "March 22, 2018" are listed. The main image shows Mark Zuckerberg speaking at a podium, wearing a grey t-shirt, against a blue background with a diamond pattern. Below the image is a caption: "Zuckerberg said he'd 'love to see' regulation on ad transparency. But that's not the company's message to lawmakers. (Reuters/Stephen Lam)"

Think Global, Act Local

Legislation Regulation

- ❖ City level
- ❖ State / provincial level
- ❖ National level
- ❖ **Supra-national**



The image is a screenshot of a CNBC article titled "Everything you need to know about a new EU data law that could shake up big US tech". The article is written by Arjun Kharpal and was published on March 30, 2018. It discusses the General Data Protection Regulation (GDPR) which came into force on Friday, May 25, 2018. The article highlights that the law will affect companies both inside and outside the European Union, and that its key principle is giving consumers control over their data. Companies that breach the rules face fines of up to 4 percent of their total global turnover. Below the article is a video player with the title "GDPR: Why everyone is freaking out over four letters" and a play button icon. The video was published on June 14, 2018.

TECH

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Everything you need to know about a new EU data law that could shake up big US tech

- The General Data Protection Regulation came into force on Friday.
- It will affect companies located in and outside the European Union.
- The key principle of GDPR is giving consumers control of their data.
- Companies face fines of up to 4 percent of total global turnover if they breach the rules.

Arjun Kharpal | @ArjunKharpal
Published: 1:27 AM ET Fri, 30 March 2018 | Updated: 12:29 PM ET Fri, 25 May 2018

GDPR: Why everyone is freaking out over four letters
12:50 PM ET Thu, 14 June 2018 | 02:55

You may have heard of the General Data Protection Regulation. It may sound boring, but it's really important and CNBC has a guide to help you understand it.

It's a piece of European Union legislation that could have a far-reaching impact on some of the world's biggest technology companies, including [Facebook](#) and [Google](#).

So here's your guide to the GDPR

What is GDPR?

GDPR is a piece of legislation that was approved in April 2016. European authorities have given companies two years to comply and it came into force Friday.

It replaces a previous law called the Data Protection Directive and is aimed at harmonizing rules across the 28-nation EU bloc.

Corporate Social Responsibility

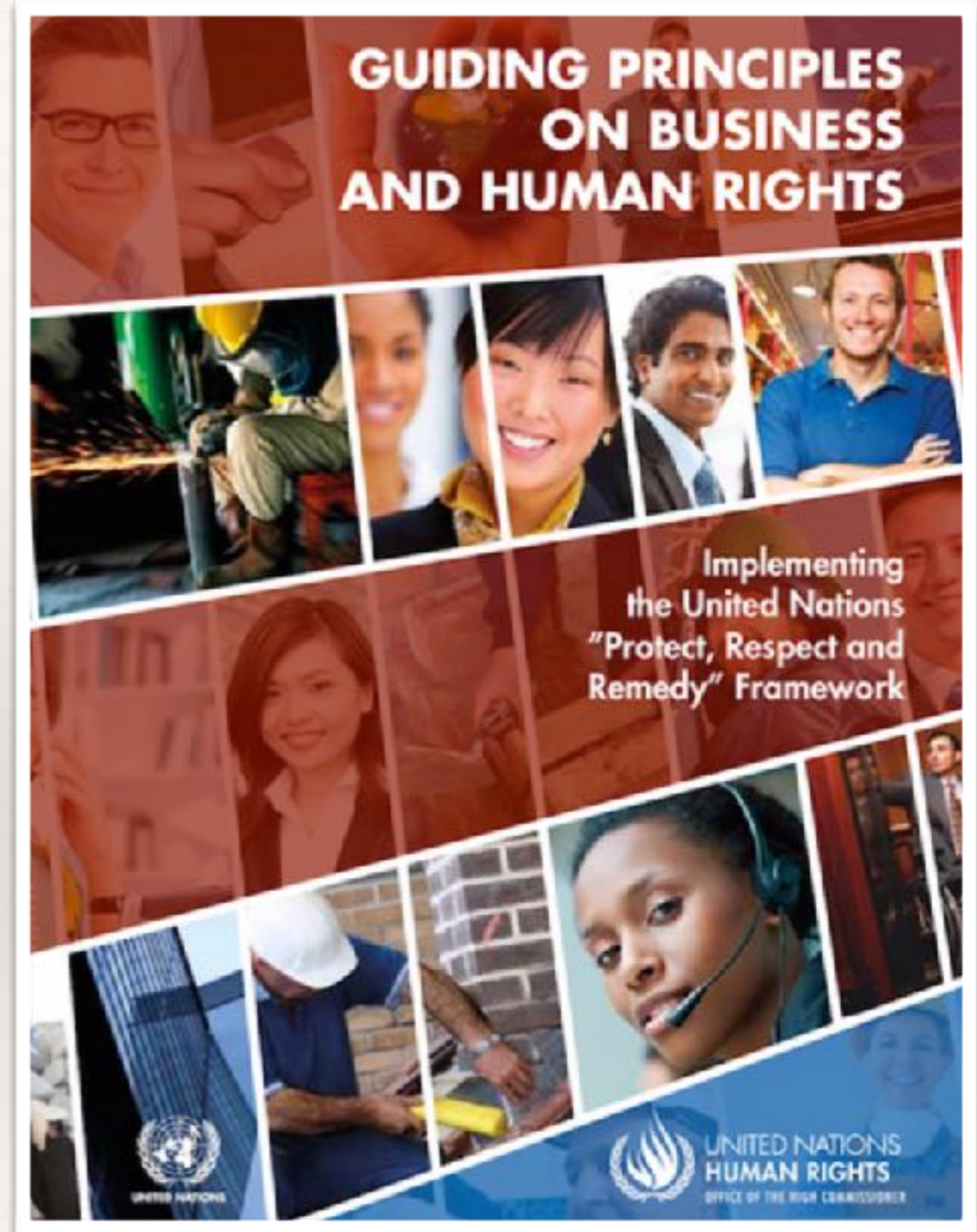
- ❖ Pressure companies to voluntarily improve practices related to privacy, free expression, and other human rights
- ❖ UN Guiding Principles on Business and Human Rights: companies have a duty to respect human rights
- ❖ Example: Ranking Digital Rights Corporate Accountability Index



Sovereigns of Cyberspace

Corporate Social Responsibility

- ❖ Pressure companies to voluntarily improve respect for privacy, free expression, and other human rights
- ❖ **UN Guiding Principles on Business and Human Rights: companies have a duty to respect human rights**
- ❖ Example: Ranking Digital Rights Corporate Accountability Index



Corporate Social Responsibility

- ❖ Pressure companies to voluntarily improve respect for privacy, free expression, and other human rights
- ❖ UN Guiding Principles on Business and Human Rights: companies have a duty to respect human rights
- ❖ **Example: Ranking Digital Rights Corporate Accountability Index**



It's more than just the internet!

Media Reform

- ❖ Net neutrality
- ❖ Fairness Doctrine
- ❖ Breakup monopolies
- ❖ Diversify ownership
- ❖ Fund public service media
- ❖ Support independent journalism

Break Facebook's Power and Renew Journalism

We must take the Internet back from monopolies.

By Victor Pickard April 18, 2018



Facebook CEO Mark Zuckerberg testifies before a House Energy and Commerce hearing in Washington on April 11, 2018. (AP Photo / Andrew Harnik)

Facebook's sudden fall from grace has toppled long-held assumptions that it couldn't be regulated. Now a rare bipartisan consensus has emerged that Facebook's unaccountable power may require government intervention.

Live Your Values

Everyday Resistance

- ❖ **Don't participate in surveillance capitalism if you don't have to**
- ❖ Harm reduction — purity is impossible
- ❖ Some of my least favorite consumer products and services



Live Your Values

Everyday Resistance

- ❖ Don't participate in surveillance capitalism if you don't have to
- ❖ **Harm reduction — purity is impossible**
- ❖ Some of my least favorite consumer products and services



Live Your Values

Everyday Resistance

- ❖ Don't participate in surveillance capitalism if you don't have to
- ❖ Harm reduction — purity is impossible
- ❖ **Some of my least favorite consumer products and services**





WE LIVE IN **CAPITALISM**.
ITS POWER SEEMS
INESCAPABLE.

SO DID
THE DIVINE RIGHT
OF ***KINGS***.

-ANY
HUMAN POWER
CAN BE RESISTED
AND CHANGED BY
HUMAN BEINGS.



ELEMENTS

TECHNO-FUNDAMENTALISM CAN'T SAVE YOU, MARK ZUCKERBERG

By Siva Vaidhyanathan April 27, 2018



For years, the Facebook C.E.O. has clung to the belief that new technology can solve the problems caused by old technology. But that philosophy is what got us into our current mess.

Illustration by Erik Carter

It was like a verbal tic. Last week, in two days of testimony before Congress, Mark Zuckerberg, the C.E.O. of Facebook, invoked a magical-sounding phrase whenever he was cornered about a difficult issue. The issue was content moderation, and the phrase was “artificial intelligence.” In 2004, Zuckerberg explained, when Facebook got its start, it was just him and a friend in his dorm room at Harvard. “We

Copyrighted Material

anti-
social
media

How Facebook
Disconnects Us and
Undermines Democracy

siva vaidhyanathan

Copyrighted Material

Questions ?

nathaliemarechal.net ~ @MarechalPhD