2017

Digitocracy

Joel R. Reidenberg
Fordham University School of Law, jreidenberg@law.fordham.edu

DOI:10.1145/3126489

Joel R. Reidenberg

Law and Technology
Digitocracy

Considering law and governance in the digital age.

Digital technologies have unleashed profound forces changing and reshaping rule making in the democracies of the information society. Today, we are witnessing a transformative period for law and governance in the digital age. Elected representative government and democratically chosen rules vie for authority with new players who have emerged from the network environment. At the same time, network technologies have unraveled basic foundational prerequisites for the rule of law in democracy like privacy, freedom of association, and government oversight. The digital age, thus, calls for the emergence of a *Digitocracy*—a new set of more complex governance mechanisms assuring public accountability for online power held by state and nonstate actors through the creation of new checks and balances among a more diverse group of players than democracy's traditional grouping of a representative legislature, executive branch, and judiciary.

Where Google and Facebook know more than most spy agencies about the lives of millions of citizens as well as the inner workings of companies and governments, information powerhouses and platforms can establish their own rules for citizens' interactions online. Where public-sector surveillance and private-sector tracking are so pervasive, citizens lose the ability to control the disclosure of their thoughts, friends, activities, and no longer have privacy. Where lone coders wreak massive havoc for private gain or for opposition to governmental policies, they can use their information resources to reject majority rule. Where technology can protect the anonymity of wrongdoers, rule-breakers can escape accountability. In short, the modern information society destroys one of the most fundamental truths of any democracy that "the power to make the laws rests with those chosen by the people."[a]

a *King v. Burwell*, 135 S. Ct. 2480, 2496 (2015).

We are witnessing a transformative period for law and governance in the digital age.

The Internet's Promise

Without a doubt, the Internet revolutionized the dissemination of information and the ability of individuals to engage with each other. The euphoria surrounding the early days of the Internet's expansion into the public sphere predicted that technology would expand democracy and empower citizens around the world. The conventional wisdom thought citizen participation would multiply online with e-government, and the public would have better oversight of the state thanks to new capabilities for monitoring administrative and executive actions. The power of the Internet to disseminate information from one to millions and the power of the Internet to foster conversations seemed an unstoppable force for democratic discourse. Popular movements like the Arab Spring, the Occupy Movement, and the Bernie Sanders U.S. presidential campaign illustrated that information technologies could indeed significantly enhance and enable political organizing on a new, unprecedented scale. Many expected that mechanisms like open electronic proceedings for rule making and open data for government transparency would herald better representative government and decision making.

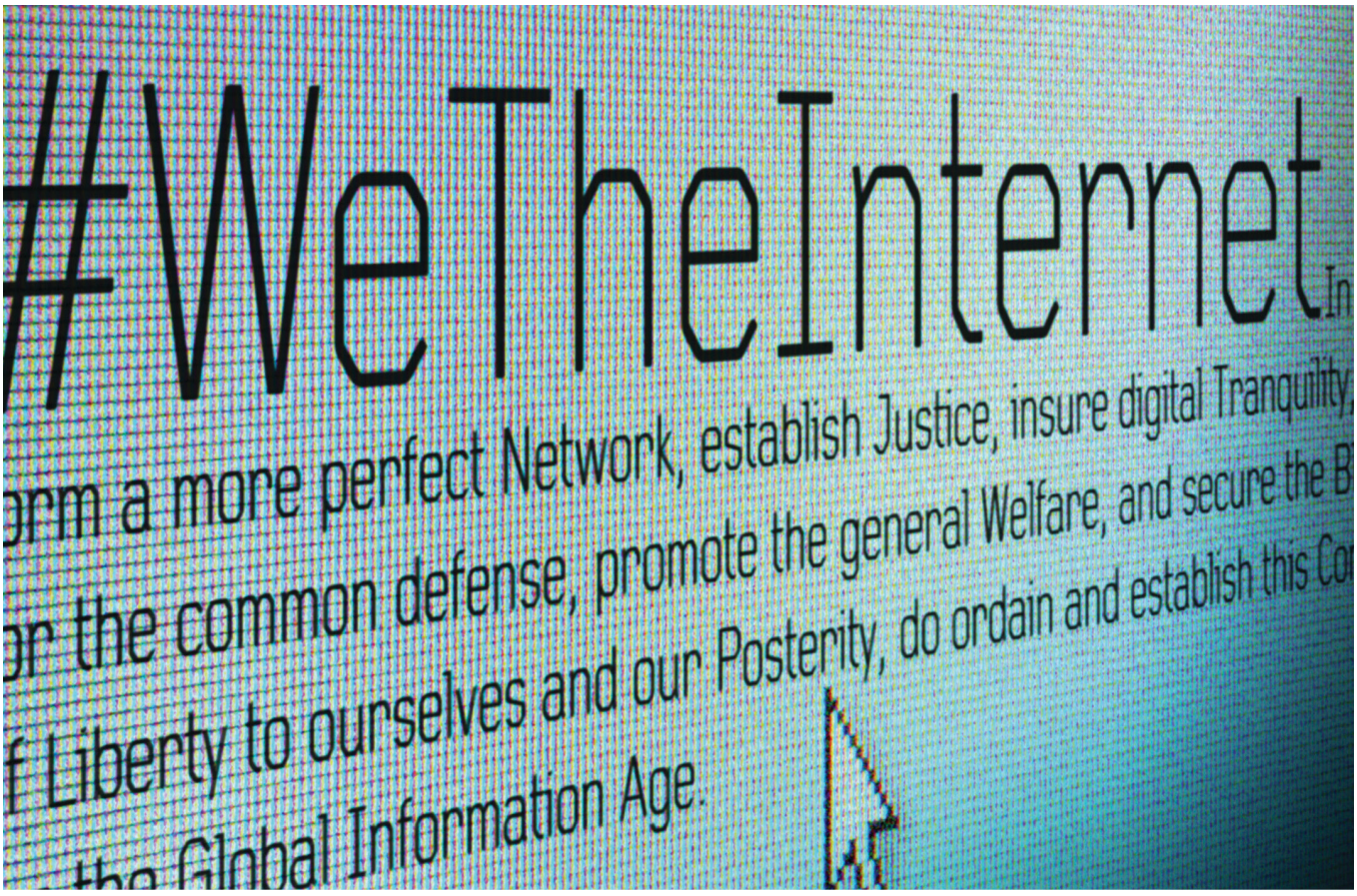

IMAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES

The Internet's technical infrastructure turns out to challenge the promise of the political empowerment of citizens. Just as network technologies offered organizational tools for political empowerment, the technologies themselves provided the means to reverse the hope that the Internet would be a one-way pro-democracy force. Network infrastructure proved that it could be used to frustrate empowerment dreams. Egypt, for example, pulled the plug on the Internet for several days during the Arab Spring uprisings to block political organizing; Brazil shut down WhatsApp for 48 hours; local police in the U.S. used stealth Stingray technology to engage in large-scale geo-surveillance of citizens. And, at the same time, Twitter bots flooded social media in order to shut down political dialog or to falsify support for candidates, while hate and bullying flourish online. In short, the Internet has embedded the means to block political empowerment and discourse.

Undermining Democracy

In the intervening years since the early euphoria over the Internet's political potential, the embedding of the Internet in our daily lives has effectively demonstrated new vulnerabilities. The Internet's infrastructure has already displaced three key areas essential to the rule of law in democracy: sovereignty, government accountability, and respect for law. Internet technologies restructure a state's ability to prescribe and assure the enforcement of law. Governments forfeit sovereignty to networks when services like cloud computing transcend borders and enable organizations to choose rules in the blink of an eye. Network architecture enables technology developers and service providers to embed rules for online activities through infrastructure choices. For example, cloud service providers like Dropbox make determinations every day on the security of users' data. These encryption decisions determine the very capability of states to examine user data in lawful investigations.

Network infrastructure undermines the oversight and accountability of government. While open government technologies enable greater transparency of public institutions, electronic tools also empower governments to circumvent traditional political checks and balances and the public's oversight of government suffers irreparably. For example, in Oakland, CA, the police engaged in a mass-scale surveillance program to geo-locate thousands of mobile phones using stingray devices without any judicial approval and, in New York City, the police program to record drivers through traffic cams and smart city sensors also escapes judicial oversight. At the same time, technologically enabled leaks and wide dissemination of non-public activities of government through sites like WikiLeaks may jeopardize legitimate functions of government such as international relations and active law enforcement investigations. Snowden's leaks, for example, are reported to have endangered the lives of British M16 agents in Russia and China.

Laws lose their authority when governments can no longer control the use of power to enforce rules and hackers have control over weapons of mass disruption. Network infrastructure removes the state's monopoly on the use of coercive, police power to enforce rules and protect its citizens. Technol-

ogy allows lone-wolf actors unchecked by states to create and deploy weapons of mass disruption whether through malware, ransomware, or botnets. For example, hospitals across the U.S. in the spring of 2016 faced a wave of ransomware attacks that left some in a "state of emergency." ISIS uses crowd sourcing to sow terror in the U.S. and Europe. Simultaneously, the infrastructure empowers private actors to engage in vigilante actions. The underground group, Anonymous, recently illustrated such actions when they threatened an electronic attack against ISIS following the Paris massacres in November 2016. In essence, individuals and associations now have tools—outside the ability of state control—to enforce their choices and rules online in ways that are independent of the state. To be sure when a Texas college discovered in 2015 that Facebook provided better real-time information for an on-campus police emergency than 911, it becomes clear the state has even lost control over basic information it needs to protect its citizens.

Beyond undermining key aspects of the rule of law, the Internet's infrastructure has toppled critical, substantive legal pillars of democracy. Freedom of thought and association as well as public safety are essential elements of democracy and privacy is a prerequisite. Yet, the network infrastructure contradicts the basic tenents of freedom of association and privacy. Network functionality works thanks to ubiquitous data surveillance. The resulting transparency of citizens to those in the network undermine both state and citizen's respect for the rule of law. States lose important checks and balances against omnipotent acquisition of information and citizen's freedom of thought and association are undercut. Counterintuitively, public safety and security are also destabilized by the transparency when stalkers, social engineering hackers, and cyberwarriors find the informational keys to success readily accessible online.

Freedom of expression is another cornerstone of democracy. Yet, democracies have a capability problem dealing with socially destructive content like hate, threats, and cyberbullying that jeopardize public order and individual safety. Technology allows rapid and widespread dissemination of harmful content, while wrongdoers can shield their activities from accountability through encryption and anonymity tools. At the same time, freedom of expression limits the authority of states to ban nefarious online content. In the U.S., for example, there is no public recourse for the rapid growth of anti-Semitic Twitter accounts. Users must appeal to the social media firms who, in turn, then decide what to suppress or censor. By contrast, in Europe, platforms bear more legal responsibility for content, but firms are often left in the same position as an all-powerful censor. In effect, government is unable to suppress the vile and corrosive online material that threatens citizens without resorting to oppressive, anti-democratic controls.

Beyond undermining key aspects of the rule of law, the Internet infrastructure has toppled critical substantive legal pillars of democracy.

The Opportunity of Digitocracy

The information society lacks a model of governance suited to the digital age. Going forward, the digital age will need a new system of checks and balances for its political decision making—a "*Digitocracy*"—offering the opportunity to develop new governing principles that articulate *who* regulates *what* to preserve public accountability online.

Our challenge is how to construct the appropriate checks and balances. Digitocracy's dynamic will be much more complex than the analog world. Online private rule making like Twitter's decisions regarding censorship, Adobe's technical protections on digital content, and Facebook's settings for privacy have become more powerful in people's lives than rules from the democratic constitutional framework. Business organizations are likely to serve as counterweights to government power. Google's Transparency Report, Apple's defiance of an FBI request for encryption keys, and Microsoft's challenge to U.S. government access to foreign-based servers each reflect a check on the state's intrusiveness. And, individuals like Snowden may serve as counterweights to states and businesses. Individuals and associations of individuals have direct authority when they coalesce with online tools ranging from social media to hacktivism as they perceive the need to interject and amplify their end goals online. All while national government provides checks on overreaching private actors. Where each actor from a state to an individual can assure mass disruption online, fair governance will require co-existence among the rule-making actors.

At the core, the assurance of public accountability online is the key objective of Digitocracy. The mechanisms for states, private actors and citizens to co-exist as rule-makers in the networked society are likely to be defined in unexpected ways incorporating notions of federalism, multistakeholder governance, and subsidiarity. These tools will draw the boundaries of rule-making authority among the state actors, platform operators, corporate organizations, and empowered users. Each actor, whether state or non-state, has an important role to prevent overreaching by the other actors. In essence, Digitocracy constructs a more multifaceted set of interwoven checks and balances to establish limits on the powers of both state and non-state actors and a reliance on both to protect the public good. For our future, now is the time to begin the robust public discussion on our means of governance in the digital age. C

Joel R. Reidenberg (jreidenberg@law.fordham.edu) is the Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University, Director, Fordham Center on Law and Information Policy, and Visiting Research Affiliate, Center for Information Technology Policy, Princeton University.

The author is preparing a book on this topic to be published by Yale University Press.