Is the Internet of Things Your New Constitution?

Philip N. Howard
pnhoward@uw.edu
Professor, Oxford University and Univeristy of Washington
9/11/2015

Abstract

The internet of things, made up of billions of devices with small sensors, will contain our political lives, communicate our political values, and constitute our political identities. It will generate perfect behavioral data without allowing citizens to opt-out of data collection. Already visible in consumer technologies, the internet of things is unlikely to be stopped, and it is unlikely that national services, technology firms, and political lobbyists can be cut out of the rich data flows it will generate. However, there are several ways of preserving a role for citizens and civil society groups in a political system defined by its information infrastructure.

Constitutions are collections of codified and uncodified traditions and conventions that provide structure for political life. They explain a polity's system of governance and define the relationships between and among citizens and political actors. In the years ahead the internet of things, made up of billions of devices with small sensors, will encapsulate our political lives, communicate our political values, and constitute our political identities. It will generate perfect behavioral data without giving citizens the right to opt-out of data collection. The algorithms, terms of service and interoperability protocols are should not just be of interest to the engineers trying to build more consumer electronics. The scripts that make the Internet of Things operate will have immense implications for governments and governance.

Already emerging through an array of consumer electronics and industrial applications, the Internet of Things is at its core an information infrastructure from which public policy makers,

technology firms, and lobbyists will seek political information. Our toasters, SUVs, and flat-screen TVs already spy on us, something we chose to ignore or tacitly accept in exchange for better product and content. Freedom and privacy may not be the only political norm we sacrifice to have the Internet of Things. Constitutions are collections of rules that entrench governance systems and set the terms of political participation. In this essay I describe the political importance of the Internet of Things, evaluate its likely roles in governance and consequences for political participation. Finally, I identify some ways of preserving a role for citizens and civil society groups in a political system fully constituted by its information infrastructure.

The Internet of Things

The Internet of Things is the rapidly growing network of everyday "things"—eyeglasses, cars, thermostats—made smart with embedded power supplies, sensors and Internet addresses that relay information about user behavior and device status across information networksMost of these networked devices are everyday household items that are sending and receiving data about their conditions and our behavior. Unlike mobile phones and computers, devices on these networks are not designed for deliberate social interaction, content creation, or cultural consumption. The bulk of these networked devices simply communicate with other devices: coffee makers with coffee suppliers, car parts with service centres, clothes with designers, and on and on. This will not be an internet that can be experienced through a browser. Indeed, as technology develops, many of us will be barely aware that so many objects around us have

power, sensors, and the ability to send and receive data on its location, status, and how it is being used.

One industry analyst estimates that the Internet of Things will have an installed base of twenty-six billion devices by 2020, only a billion of which will be personal computers, tablets, and smartphones. An industry consulting firm estimates there will be thirty billion connected devices. A top manufacturer of networking equipment predicts there may be as many as fifty billion devices and objects. A report from the OECD on the internet of things estimates that a family of four will go from having an average of ten devices connected to the internet now to twenty-five in 2017 and fifty by 2022. In the next five years, more than a thousand networked 'nanosats'—small satellites that operate in formation and have low transition power—will be launched into space. Drone production, whether for the military or hobbyists, is difficult to track. But government security services have them, and activists and humanitarian organizations have them, too. Every one of those will have sensors and a radio that can broadcast information about the time, the device's location, its status, and how it has been used.

Industry estimates on the Internet of Things are often bullish. But it is safe to say that in five years time there will be around eight billion people on the planet, and up to four times as many connected devices. Engineers expect so many of these connected devices that they have reconfigured the addressing system to allow for 2 to the 128th power addresses–a system that would allow for each atom on the face of the earth to have 100 internet addresses. Not only

have we figured out how to give everything we produce an address. We also have enough bandwidth to allow device-to-device communications, and we have the capacity to store all the data those exchanges create. But how might the Internet of Things rival a Constitution as the primary structure of political life?

IoT as a Mechanism of Governance

In political science we treat governments and governance systems as representative systems. However, we must also evaluate them as sociotechnical systems. We look at the informal and formal ways that citizens express their preferences, or the means by which public policy is developed and enforced. The Internet of Things is a technology, or rather a technological system. It is not just a regulatory challenge. It is a massive information infrastructure that will fully formalize the ways that citizens express preferences. And it will be the means by which policy is developed and enforced. In all of history, there has never been anything like the constant and intimate feedback loop that the Internet of Things is creating between citizens and whoever is on the other end of their data.

We are accustomed to defining politics as a process by which a few people represent the interests of many, either through some democratic process or by fiat. But the Internet of Things is increasingly reporting on our actual behavior, generating politically valuable data, and reflecting our habits, tastes, and beliefs. Hence, political communication be less and less about a dialogue between and among citizens and politicians. Increasingly, political communication systems are coordinated by network devices that citizens and politicians are exploiting with

varying degrees of sophistication. We are launching such a system now, in the Internet of Things, and when it is fully embedded in our polities the unambiguous categories of democracy and dictatorship may no longer apply. Instead, it may be more revealing to characterize a government on the basis of its policies and practices regarding network devices and information infrastructure.

"Big Data" is often defined as large amounts of information, collected about many people, from over many kinds of devices. Political campaign managers have already adapted their political analysis and communication tools to be able to interpit and manipulate the public sphere through device networks. Polls, registration rolls and credit-card data help campaign managers efficiently target the citizens most likely to give donations and show up on voting day. And having Big Data has allowed party strategists to focus on the coveted mid-spectrum of politics: undecided or ideologically "soft" voters in a bid to see the personalities, policies, and content that will attract and appeal to them.

While lobbyists and campaign managers are playing with these rich and voluminous records of our lives, government agencies are tapping them, too. Tax agencies use complex fraud detection programs that look for suspicious Internet addresses and metadata. Ten years ago, New York state identified and stopped 50,000 fraudulent tax returns; last year its new analysis techniques caught 250,000. In Los Angeles, the city government's data-sharing program with a Google-owned navigation service is expected to turn smartphones into traffic sensors that will route participating drivers, and help reduce congestion and make the city more navigable. Such

programs have their critics, but many government offices in the U.S. are now openly seeking help in analysing the plethora of data at their disposal.

Clearly, this next Internet is going to make Big Data truly gargantuan, with real consequences for our political lives. Research and polls will no longer be small survey samples with noticeable error margins and carefully worded questions. Device networks will generate precise details — all of the time. The end result will not be a stream of data, it will be a tsunami of information about our real-world behavior, movements, and habits, not just our attitudes and aspirations.

Just how much does our smartphones, watches, and wearable technologies betray us to the wider world? Cell phones have the ability to take one location point per second. If you give an application on your phone permission to use location information, it will send information to a server at the rate the developer chooses and battery life allows. If you use a crowd-sourcing application for traffic data, your phone is sending data about your commute. If you use an application to keep track of your jogging, your phone is generating geotagged data about your movements relative to other people. Every time you take a picture, check in with your favorite social networking application, or track your health, data is sent from your phone to a cell phone tower or router and over a vast network of digital switches. More important for political life, the data flows through many different kinds of organizations: the companies that maintain your digital networks, the startups that build the apps, and the third-party advertising agencies that have licensed access to this information. Platform developers and social media, such as Google, Facebook and Microsoft, can also retrieve this data at several points in the information flow. Of

course, the U.S. National Security Agency and perhaps other governments or other uninvited organizations can tap in.

The current objective for geolocation engineers is to design chips that require so little power that they can be left on all day. This would mean being able to generate one location point per second, all day long. As the price of making chips declines, more can be put into devices other than your cell phone. The Internet of Things will be an immense layer of networked devices, and it will be defined by communication between devices more than between people. In short, it will be a different kind of internet: infinitely large, pervasive, and ubiquitous. And what will be the political impact of such connectivity?

The Internet of Things could be the most effective mass surveillance infrastructure we've ever concived and built, and the most detailed constitutional structure for our political interaction. Before us is a final chance to integrate new devices into institutional arrangements we might all like. Indeed, such active civic engagement with the rollout of the Internet of Things is the last best chance for an open society.

The Internet of Things as a Mechanism of Political Participation

The politics of the future will be guided by a new power paradigm. Whoever controls the largest device networks will get the most sensor data, and hence will manage the largest number of connections between and among people and devices. As more of the things we manufacture are powered and networked, "inanimate" objects will be replaced by devices that

talk with our other devices. They will communicate with their original manufacturer, the information services we subscribe to, national security agencies, contractors, cloud computing services, and anyone else in the data stream. They will work the behavioral data they have assembled and with algorithms—the script of our new constitution—mete out capacities and constraints on our political lives. Subsequently, civic engagement will increasingly become involuntary. None of us will have the opportunity to opt-out of the behavioral data collection that generates public policy.

The basis of a democracy is voluntary civic engagement. A person's participation in setting government policy is intentional and a matter of choice. In democracies, citizens express their preference through activism and voting. Historically, governments and politicians eager to interpret (and manipulate) citizen intent also relied on opinion polls, conversations with civic groups, social science research, and huge record-keeping projects like the census. Politicians have long tried to interpret citizen intent and manipulate it through rhetoric and campaign tricks.

But pervasive device networks will change the rules, making voluntary conversations among elected officials, political parties, lobbyists and civic groups *less* important than the plethora of near-perfect data generated by the objects around us. Activism and petition-signing will be overshadowed by volumes of behavioral information cleverly extracted from the Internet of Things.

This information will be of incalculable value. It will inform firms of consumer habits, enlighten governments as to the needs of citizens, and reveal the whims of voters to politicians. Political lobbying isn't a new sport, but the Internet of Things is going to be a game-changing resource for lobbyists. The more a lobbyist knows about the behavior of voters and donors, the easier it is to activate and organize those people on clients' behalf. Furthermore, smart data mining will cost good money, which will place it out of the reach of many civic groups, scientists and journalists. Hence, society's watchdogs will not be able to use this data to check on what big political players are doing with this megadata.

It is also important to realize that governance systems don't just involve states: they appear whenever a powerful actor can set some rules and restrictions on people's behavior. For example, Uber has ordered its drivers to stay away from protests in China, and it has a way to enforce the rule: they will use drivers' cellphones to track car location and cancel the contracts of violators. Though Uber's policy is a business decision, this rule has the political implication of cutting off a transportation option for Chinese citizens who want to help reform their government.

Conclusion

But the Internet of Things need not be a threat to personal privacy and political freedom. This second Internet can be regulated. The next internet is still far enough away that citizens can have a voice in how it is constructed and operated: to create systems, rules, and regulations that ensure that the Internet of Things will serve people, and not betray them. But such a

Constitution has to created from the ground up. To shape the next Internet responsibly and wisely, citizens will have to understand what the Internet of Things truly will be — an information infrastructure for public life. And there are things we can do now to build political participation.

As individuals, we need to keep track of where our data ends up. This, of course, is easier said than done. Even at this early stage, it would be difficult to list of all the third-party vendors, market analysts and government agencies that have access to the data we generate. Down the road, we may have little choice on where our data ends up. Standards to determine access to data are now being set behind closed doors, defined by industry engineers arguing for secrecy and proprietary systems. If these arguments succeed, the next Internet will be even more personally intrusive, publicly unaccountable and susceptible to surveillance than the current one.

To prevent that, a basic step would be to require that any connected device be able to divulge a list of the 'ultimate beneficiaries' who will benefit from its sensor data. Critics may argue this will be impossible. They will say that terms of service always get modified, ownership structures change over time, and the number of third parties paying for access to our data will lengthen over time. But the mere complexity of the Internet of Things proves that there are no limits in data sharing. If the smart lightbulb you buy is able to relay some data up the network to other organizations, it should also be able to pull down a list of the corporate, government and civic entities using your data.

After that, we need to make sure the Internet of Things has some branches designed for civic engagement, not simply government policymaking and industry marketing. These days, it is normal for civil-society groups to have an Internet strategy or a social-media strategy. Soon they will need to consider their IoT strategy.

With billions of sensors to learn from, there's no reason governments shouldn't try to learn about public preferences, or for firms to do in-depth market research on the behavior of their customers. And it is very likely that citizens and consumers will benefit from this data mining through better products and services. But people can insist that governments provide ways to ensure that citizens are allowed to choose how their individual data is being used.

Traditionally, politics was what happened when one person or organization tried to represent another person or organization. In the years ahead, much of that representative work will be done by devices—the everyday objects that render behavioral data when built with sensors and linked to a networ. you purchase a smart lightbulb and your home is suitable networked, remember that in an important way, your device will have yield information about your consumption of goods, services and energy that may inform wise public policy. This influence how retailers and governments serve our communities, long after you've bought the lightbulb, and regardless of whether we cast a vote.

The inescapable conclusion: the protocols and algorithms that make the Internet of Things will also be a Constitutional script for our political lives. For democracies, the Internet of Things will transform how we as voters affect and interact with government — and how government touches and monitors our lives. Authoritarian governments will have their own uses for this Internet, and have already found ways to use this information to bolster their regimes. Many of the the worst-case scenarious presented in this essay are unavoidable. But we have to act now, and everyone, both citizens and leaders, must realize what is at stake and at risk if action is delayed.

ACKNOWLEDGEMENTS AND FUNDING DISCLOSURE

For discussion at the University of Pennsylvania on September 17th 2015 at the Penn Program on Democracy, Citizenship and Constitutionalism. I am grateful to workshop participants for their feedback. I gratefully acknowledge the support of the National Science Foundation, "EAGER CNS: Computational Propaganda and the Production/Detection of Bots," BIGDATA-1450193, 2014-16, Philip N. Howard, Principal Investigator. Project activities were approved by the University of Washington Human Subjects Committee, approval #48103-EG. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

ABOUT THE AUTHOR

Philip N. Howard is a professor of communication, information and international affairs at the University of Washington and Oxford University. Howard is the author of *The Managed Citizen* (Cambridge, 2006),

the *Digital Origins of Dictatorship and Democracy* (Oxford, 2010), and most recently of *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (Yale, 2015). He is a frequent commentator on technology and politics for the national and international media. He blogs at www.philhoward.org and tweets from @pnhoward.