Data for Peace: The Future of the Internet of Things

Author : Michael Madison

Date : January 7, 2016

The Atomic Age of Data: Policies for the Internet of Things Report of the 29th Annual Aspen Institute Conference on Communications Policy, Ellen P. Goodman, Rapporteur, available at SSRN.

The phrase “Internet of Things,” like its cousin “Big Data,” only partially captures the phenomenon that it is meant to describe. *The Atomic Age of Data*, a lengthy report prepared by Ellen Goodman (Rutgers Law) following a recent Aspen Institute conference, bridges the gap at the outset: “The new IoT [Internet of Things] – small sensors + big data + actuators – looks like it’s the real thing. … The IoT is the emergence of a network connecting things, all with unique identifiers, all generating data, with many subject to remote control. It is a network with huge ambitions, to connect all things.” (P. 2) The Atomic Age of Data is not a scholarly piece in a traditional sense, but it is the work of a scholar, corralling and shaping a critical public discussion in an exceptionally clear and thoughtful way.

The IoT is in urgent need of being corralled, at least conceptually and preliminarily, so that a proper set of relevant public policy questions may be asked. What are the relevant opportunities and hazards? What are its costs and benefits, to the extent that those can be discerned at this point, and where should we be looking in the future? That set of questions is the gift of this report, which is the documented product of many expert and thoughtful minds collaborating in a single place (face to face, rather than via electronic networks).[1]

Simply defining the IoT is one continuing challenge. As *The Atomic Age of Data* affirms, the IoT isn’t the Internet, though it is enabled by the Internet and in many ways it extends the Internet. (P. 2) What it is, where it is, how it functions, what it might do in the future – or permit other to do – remains at least a little cloudy. The first contribution that *The Atomic Age of Data* makes is simply to map these contours, contrasting the Internet of Things with the network of networks that today we call the Internet, or the Internet of People. It identifies several distinguishing characteristics of the IoT: its sheer scale (the amount of data that can be gathered from ubiquitous sensor networks); the reduction or even elimination of user control over data collection; the widespread deployment of actuators, embedding a level of agency in the IoT; data analytics that rest atop communications and transactions; its demonstrably global character (in contrast to the initiated-in-the-US character of the Internet); and its framing of data as infrastructure, enabling the provision of a broad variety of services.

The bulk of *The Atomic Age of Data* consists of a comprehensive sorting of policy questions and recommendations. The foundational premise is the idea that data itself is (or are) infrastructure – “as a vital input to progress much like water and roads, and just as vulnerable to capture, malicious or discriminatory use, scarcity, monopoly and sub-optimal investment”. (P. 12) The analogy between data infrastructure and communications infrastructure is purposeful. Characterizing data as infrastructure, like characterizing communications as infrastructure, only frames policy and technical questions; it doesn’t resolve them. Data ownership and data access are related questions. They connect to questions of data formats, interoperability and interconnectivity, and common technical standards. Identifiability of data is a cross-cutting concern for privacy purposes. The respective domains of public and private investment in the IoT, and corresponding expectations of public access and use and private returns, remains open questions. The report clusters these topics together; one might label the cluster with a single theme: governance.[2]

How, or more precisely, by whom, will all of this data be produced? The report examines the adequacy of incentives for private (commercial) provision of data and the appropriate role for government as regulator and supplier of subsidies.

This “data as infrastructure” section of *The Atomic Age of Data* concludes with a series of policy recommendations,

focusing on two overarching principles (also reduced to several more specific recommendations): that there should be broad accessibility of data and data analytics, with open access to some (but not all); and that government should subsidize and facilitate data production, particularly in cases where data is an otherwise under-produced public good.

The Atomic Age of Data moves next to a review of privacy topics in the context of the IoT, beginning with when, whether, and how to design privacy protections into systems from the start, and the role and implementation of Fair Information Practice Principles (FIPPs). As the report notes, these are critical questions for the IoT because so much of the IoT is invisible to individuals and has no user interface to which data protection and FIPPs might be applied. To what extent should privacy protection be designed in to the IoT, and to what extent should privacy protection be a matter of strategies that focus on individual choice?[3]To what extent might choice undermine the production, collection, and processing (aggregation) of good data, or the right data? Privacy questions thus intersect with incentive questions. Cost, benefit, and values questions extend further. To what extent is choice even technologically feasible without compromising other societal values? Production, collection, identification, and processing/aggregating data lead next to related privacy questions about retention and curation of data.

This privacy section concludes with brief set of recommendations, focusing on three overarching principles (again with several more specific points): that IoT systems should design in privacy controls to minimize the collection of personally identifiable information; that IoT systems should effectuate FIPPs to the extent possible; and that individuals should have a way to control collection and transmission of their personal data.

The balance of the report is divided among four additional topics that are treated more briefly, though in each case the topic concludes with a short set of basic recommendations. The first is “Equity, Inclusion, and Opportunity,” which collects questions about prospects of citizen empowerment and disempowerment via the IoT. Data collection in some respects signifies “who counts” in modern society – whose voice and presence “matters,” both individually and collectively, but also, in some respects, whose voice and presence is worth watching. The report points out the relevance of comparable concerns with respect to the deployment of broadband communications infrastructure and its impacts on things like access to education and health resources. The second is “Civic Engagement,” which touches on how IoT technologies might be used both by governments and by the private sector to increase democratic accountability. The third is “Telecommunications Network Architecture,” which concerns the intersection of the IoT and competition, service innovation, and interoperability among IoT systems and related communications networks. The key topic here is the heterogeneity of the data generated by IoT applications, recalling the question of whether the Internet of Things is, or should be, truly a single “Internet” at all, with interconnected networks, connections across verticals (home, health, transport, for example), and common platforms. (P. 39) The fourth is security, which raises the relatively simple question of security vulnerabilities introduced at both the level of individual devices and at systemic levels. The question may be simple but the answer assuredly is not; this section of the report is comparatively brief, perhaps because the salience of the interest is so obvious.

The Atomic Age of Data finishes with a case study, on The Smart City, which refers to the idea of networks of ubiquitous sensors deployed within urban infrastructure to generate data about usage patterns and service needs. (P. 45) The discussion of this use case is decidedly and appropriately pragmatic, putting utopian hopes for the Smart City in context and noting privacy and surveillance concerns and related but independent equity concerns.

To conclude this review:

This is an enormously clear, useful, and timely product. One cannot critique a report of a conference on the ground that it did not address a critical topic, if the conference itself did not address that topic. Yet as helpful as *The Atomic Age of Data* is in canvassing the policy territory of the IoT, I couldn’t help but notice how the boundaries of that territory are implicitly defined. *The Atomic Age of Data* contains a lot of discussion of “Internet” topics and less discussion of “things.” In this day and age, one should never take things or thing-ness for granted. What is a thing? 3D printing, the current label for additive manufacturing, promises to revolutionize the meaning of “thingness” – because objects may be dynamic and emergent, as well as static and fixed[4] – just as the “Internet of Things” promises to revolutionize the

meanings of identity and presence.

“Data for Peace,” the title of this review, builds a bit on the naïve sense of modernity and progress expressed (purposefully, no doubt) by the report’s *Atomic Age* title. During the 1950s and 1960s, “atomic” things were full of optimism. Later, we learned that splitting the atom changed the meanings of matter in unexpected ways. “Atomic” gave way to a variety of more complex political, cultural, and technological expressions and concerns, few of which were foreseen at the dawn of the Atomic Age. Similarly, 3D printing may turn out to change the meanings of matter in unexpected – but other – ways. As the IoT and Big Data mature — along with 3D printing – I expect that future reports on its implications will be similarly but unexpectedly complex.

1. Recent and related but less comprehensive reviews of IoT policy questions include *Internet of Things: Privacy & Security in a Connected World*, Federal Trade Commission Staff Report (January 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; and Rolf H. Weber, *Internet of Things—Governance Quo Vadis?*, 29 Computer Law & Security Report 341 , (2013), doi:10.1016/j.clsr.2013.05.010. [?]
2. For an expansive treatment of infrastructure and governance issues, *see* Brett M. Frischmann, *Infrastructure: The Social Value of Shared Resources* (2013). [?]
3. The significance of these questions is highlighted in the Mauritius Declaration, cited in Ellen P. Goodman, *The Atomic Age of Data: Policies for the Internet of Things*, 25 (2015); *see also Mauritius Declaration on Internet of Things*, 36th Annual Conference of Data Protection and Privacy Commissioners (October 14, 2014), http://www.caa.go.jp/planning/kojin/pdf/1E_Mauritius_Declaration.pdf. [?]
4. *See* Deven R. Desai & Gerard N. Magliocca, *Patents, Meet Napster: The Disruptive Power of 3D Printing*, 102 Georgetown L.J. 1691 (2014). [?]

Cite as: Michael Madison, *Data for Peace: The Future of the Internet of Things*, JOTWELL (January 7, 2016) (reviewing *The Atomic Age of Data: Policies for the Internet of Things* Report of the 29th Annual Aspen Institute Conference on Communications Policy, Ellen P. Goodman, Rapporteur, available at SSRN), http://cyber.jotwell.com/data-for-peace-the-future-of-the-internet-of-things/.