Kate Roger

9/17/17

In his book, *Data and Goliath*, Bruce Schneier dives into the world of data and its significance to notions of identity, privacy, and access. He explains that data is the byproduct of all computer activity, and that as our world becomes increasingly computerized, data becomes an increasingly pertinent and controversial part of our lives.

Both Schneier and the writers of *Blown to Bits* believe data is a neutral medium whose growing abundance is not categorically unfavorable. Schneier says the “smog of data we produce is not necessarily a result of deviousness on anyone’s part,” but rather an inevitability of computing processes (Schneier 2015, 20). It’s what we *do* with data that determines its character.

As Schneier makes clear in *Data and Goliath*, what we can do with data and how quickly we can do it are two important and rapidly-changing variables. Schneier argues that, because of the increasing ease of data transfer and storage, it has become more practical to save data and search for it later than to sort data and delete what’s unimportant (Schneier 2015, 22). What this means is that, more and more, we are saving *everything*. The writers of *Blown to Bits* use metaphor to explain that in the near future, we will have the capacity to store data pertaining to just about everything we do and say, and we’ll have the capacity to store it *forever* (Abelson, Ledeen, and Lewis 2008, 11). Schneier says that “it’s easy [for people] to dismiss concerns about [data] retention and use based on the assumption that there’s simply too much of it to save, and in any case it would be too hard to sift through for nuggets of meaningful information” (Schneier 2015, 21). It’s easy to assuage our fears by supposing nobody’s “really” taking stock of all of our data. And for the most part, both of these books claim, nobody is. However, somebody *could*, and that’s where the discussion of privacy comes in.

The writers of *Blown to Bits* say “computers contain a lot of stuff that isn’t useful today but somebody thinks might someday come in handy” (Abelson, Ledeen, and Lewis 2008, 2). They, and Schneier, consider this situation a site for possible danger. Schneier argues that his data, specifically his email archive, is “part of [his] brain” part of his “memories,” and that “access to that data trove is access to [him]” (Schneier 2015, 22).

So, the question arises: who has access to my data and therefore to me? And who should? *Blown to Bits* mentions that the PATRIOT act gives government agencies nearly unquestioned power to look through our data (Abelson, Ledeen, and Lewis 2008, 15). And a PBS article on “the end of privacy” following changing legislation says that not just the government, but “anyone from insurance companies, airlines, banks and retailers to political parties…could buy data profiles of consumers” (Smith 2017). A BBC article regarding the same legislation explains that these organizations have access to “precise geo-location, financial information, health information, children’s information, social security numbers, web browsing history, app usage history and the content of communications” (Lee 2017).

Taken together, these claims tell us a few things about the state of our privacy— or lack thereof. The writers of *Blown to Bits* argue that we live in a “post-privacy world,” that the data explosion has left our notion of privacy “in shambles” (Abelson, Ledeen, and Lewis 2008, 17). Schneier, I think, would agree.

The Oxford American Dictionary defines privacy as “the state or condition of being free from being observed or disturbed by other people”. I would argue, though, that in the context of data, privacy means a bit more than that— there is a question of proprietorship and identity tangled up in the conversation around data privacy.

Documentation of our identities in the form of data has multiplied as new sites of identification come to be— anything from Snapchat accounts to IP addresses, online memberships to savings accounts. Our identities now exist in shared space— they’re no longer localized: we don’t hide money under the bed, we hide it in the form of credit, online, accessible by password. We don’t have to follow someone home to learn their address; it just takes a few simple search mechanisms. People don’t have to want to find *you*, specifically, to access your personal data. Instead, your data becomes, in a sense, a form of capital to which various companies and organizations vie for access— or ownership.

The PBS article I mentioned earlier quotes GeekWire saying: “Historically, regulations have treated [personal] data as the property of the consumer,” but under pending regulatory changes, that data “will be viewed more like the property of internet providers” (Smith 2017). This shift points to an interesting development: there seems to be some level of dissociation between our “identities” and the data that represents those identities. And, at least legally, it’s unclear who exactly should be allowed access to that representative data.

In other words, do I *own* an Instagram account, or am *I* Instagram’s user? Is the information about myself that I vest in an Instagram account *my* data, or should Instagram have the right to do with that data whatever it would like? Or, more importantly, are the health records stored digitally about my medical history *mine*, or am *I* my health provider’s patient? Do my records belong to my health provider and even to potential researchers? There is an interesting disruption of the subject-object relationship in these examples, which makes sense given that the Web is intended to be a decentralized, collectively owned space.

As we are dissociated from our relevant data, then, it becomes easier and easier for public and private organizations to categorize us for their own means. And many (or most) of those organizations now have no obligation to inform us that parts of our identity are being subsumed into their work. “ISPs [can] sell [our] personal information without consent,” including but not limited to our “browsing history and geolocation” (Smith 2017). We’re being sold to the highest bidder.

But, as most sources agree, and to return to the thoughts of Abelson, Ledeen, Lewis, and Schneier, this so-called annihilation of privacy is mostly abstract and irrelevant to the average person. The danger arises when our data gets into the wrong hands, or is taken out of context, or put to nefarious purposes. It’s not hard to imagine a world (or a Black Mirror episode) where law courts use text messages, search histories, and geo-tracking maps from years past to build a case for someone’s conviction. And, as I stated earlier, the danger is not in the data itself, but in the way it’s used and construed. Data may be neutral to some degree, but the system it operates in is not by any measure. It’s sort of a double-edged sword: we’re being commodified as data points, dissociated from representations of our identities. But we’re also still attached to and held accountable to that data, and when the situation arises, our data is considered to be very much a part of our identities. So I worry that the increasing access to personal data will be used as a super tool for preexisting systems of bias and oppression. I also worry that because of the way we assume data to be objective and constant through time, we will foreclose opportunities for—and recognition of—metamorphosis. It is quite dangerous, I think, to use and judge people’s past selves without taking stock of their ability to evolve and grow, and without recognizing the significance of the changing contexts in which data exists.

I believe, then, that until the system our data lives in becomes safer, more clear-sighted, and more egalitarian, we need regulations in place to protect our data from manipulation by people that may not have our best interests at heart, or may not have our interests at heart at all. There is a reason, I think, why Singapore “protects all personal data ten years after a person’s death,” and why South Korea has laws “covering a person’s image or voice” (Gustke 2013). Like Schneier says, our identities are at stake here, and potentially our livelihoods. So until we can trust that the system we live in will access our data with compassion and thoughtfulness, privacy is vital to our safety, and, I think, to our freedom.

References:

Abelson, Hal, Ken Ledeen, and Harry Lewis. 2008. *Blown to Bits*. Boston: Addison-Wesley.

Gustke, Constance. 2013. “Which countries are better at protecting privacy?”. BBC. Last modified June 26. <http://www.bbc.com/capital/story/20130625-your-private-data-is-showing>.

Lee, Dave. 2017. “Anger as US internet privacy law scrapped”. BBC. Last modified March 29. <http://www.bbc.com/news/technology-39427026>.

Schneier, Bruce. 2016. *Data and Goliath*. New York: W. W. Norton & Company.

Smith, Iman. 2017. “Before you lament the end of your internet privacy, read this”. PBS. Last modified April 3. <http://www.pbs.org/newshour/rundown/lament-end-internet-privacy-read/>.