Inquiring Minds– 28 June 2019

Melissa Butler, Moderator

Is Privacy Passé?

Is "privacy" an outdated idea, like a flat earth or geo-centric universe? Should it go the way of 8-track tapes and typewriters and carbon paper? Should we mourn its passing?

The big questions: Is it desirable to maintain privacy today? Is it possible?
Do the advantages of living in a networked world outweigh the disadvantages?

We willingly sign on to websites, use social media or download apps for our phones, but should we think more about the trade-offs? What about tracking that happens without informed consent? Consider omnipresent cameras and facial recognition technology.

Does all this data need protection or control? Who should do it? Should big tech corporations do the policing? Or are they themselves out of control? Should we rely on the government? Or is government an even bigger threat?

Heidi Messer , "Why We Should Stop Fetishizing Privacy" *NY Times,* May 23, 2019

Big tech companies create jobs, encourage innovation and provide valuable services free. Why would we want to break them up?

Media coverage of the threat to personal privacy from technology tends to follow a narrative in which privacy is a virtue, Big Tech its evil predator and government the good knight capable of protecting it.

But this narrative ignores the realities of modern life and may lead to devastating trade-offs. It fetishizes privacy, demonizes technology and assumes that government is the right institution to protect us.

We live in a networked world. The internet is built for sharing things at little to no cost. We forward our emails, capture photos on cellphones and tweet opinions, all activities that leave a trail of data that can be collected without our knowledge. Privacy — the right to be free from unwanted intrusion — no longer exists in an absolute sense.

Regulating tech companies could create problems worse than the ones we seek to solve. The biggest companies — led by Facebook, Amazon, Netflix and Google in the United States, and Baidu, Alibaba and Tencent in China — are data networks, aggregating information to provide valuable services underwritten by advertising, e-commerce or user subscriptions.

They have all become both hugely profitable and vital to the global economy. The Department of Labor estimates that employment in the computer and information technology sectors in the United States will grow 12 percent from 2016 to 2026, much faster than the average for all occupations. The companies also provide income to millions of non-employees, including Airbnb hosts, Instagram influencers, eBay sellers, and Uber and Lyft drivers. If we constrict their fuel — data — we may hurt not only the quality, cost and speed of their services, but also the drivers of growth for the world's economy.

Innovation will also suffer. Our culture celebrates entrepreneurship and accepts failure as part of the process. As a result, the United States has been the architect of the new economy. But privacy evangelists have made villains of the very companies the world emulates. Rather than debate how to expand this economic opportunity, they call for fettering it.

The evangelists assert that regulating access to data or breaking up big companies will put that data back in our control. But this is naïve. We share our photos, emails and other personal data daily. Almost any individual or company, big or small, can collect and misuse it. Size doesn't make a difference.

If safety is the actual goal of protecting privacy, consider this: Large tech companies may be our best line of defense against hackers, state surveillance and terrorists. These companies have the talent and resources to match well-funded and sophisticated adversaries. As the threat of cyberwarfare grows, shouldn't we consider whether it would be prudent to break up companies that are our best allies against foreign and criminal intrusion?

Regulation also assumes that lawmakers understand how the internet operates. But many of the questions asked of the Facebook co-founder Mark Zuckerberg at his most recent congressional hearing reflected a staggering display of ignorance about the businesses that have fueled America's economic growth for over a decade.

Consumers, on the other hand, potentially can have more influence over these companies. When those companies violate the public's trust, the news travels fast — often on the platforms themselves — and people stop visiting the sites, causing them to lose revenue. After a scary internet meme known as Momo spread, millions of parents unplugged their children from YouTube. Consumer uproar over a bug in FaceTime that allowed eavesdropping led to an emergency ad campaign by Apple.

Privacy advocates often point to European privacy rules as a model for the United States. Under those rules, the General Data Protection Regulation, companies that operate in Europe or handle European data are required to obtain consent before collecting data. They also must provide users with the "right to be forgotten" — the ability to delete their information upon request.

In theory this might sound beneficial. But some services we highly value, such as spam filters, require analyzing emails quickly — and without consent. Allowing everyone "the right to be forgotten" will enable people to erase information about bad actions that society might benefit from seeing.

And do we really want to emulate European rules if they undermine competitiveness? With the uncertainty over how to comply with those rules, entrepreneurs have looked to markets on other continents, strengthening big companies that can afford to pay big penalties for their privacy violations. The rules make it more costly to build a data network, which could explain why there are no European rivals to America and China's big companies.

The lack of data networks will make it much more difficult for Europe to compete in building artificial intelligence applications that could allow us to live longer, more fulfilling lives, precisely because they collect and store huge amounts of data, which in turn makes algorithms more accurate. Engineers today are focusing on using artificial intelligence not just to improve shopping and social networks, but also to cure diseases, provide clean energy and better manage food supply and transportation systems. My own company, Collective[i], is a data network that uses machine learning to help companies manage revenue with the goals increasing economic prosperity and reducing layoffs created by uncertainty.

Expecting government to sort this all out reflects a blind trust that defies historical experience. The Fourth Amendment was written to protect against arbitrary searches and seizures of property by the government. Regardless of how you feel about WikiLeaks or Edward Snowden, they revealed that governments are watching us. People forget that Apple has fought to protect the privacy of iPhone users from the F.B.I. And that the Chinese government uses access to data to stifle dissent and profile minority groups.

Finally, it is time to stop glorifying anonymity. In the internet underworld known as the dark web, where users go to be anonymous, there are no Facebooks or Googles to set standards for speech, no opt-out provisions for individual users, no trail of data the authorities can use to prevent or prosecute crimes.

Young people who have grown up on the internet — so-called digital natives — have a much more nuanced view of privacy. They start with an awareness that their data isn't private. They aren't shocked that companies collect it, perhaps because they know that this collection enables them to get valuable services free. They know their texts can be sent all over the internet, that any of their emails can be forwarded to anyone else, that their chat rooms can be infiltrated by strangers — with or without their consent. But if a platform violates their trust, they stop using it.

If we untether ourselves from the old paradigms, we can open our minds to real solutions to expand opportunity and innovation while ensuring our safety. Where privacy is actually the issue, our laws should focus on deterring companies, institutions and individuals from misusing data to cause actual harms, such as slander, harassment, human trafficking, discrimination, fraud and corruption.

The big tech companies are neither heroes nor villains in this narrative. They create jobs and render certain jobs obsolete. They amplify the best and worst things about us. Simply saying that privacy infringements seem "creepy" or "scary" does not justify regulating all of these corporations.

Progress is a messy business. Instead of trying to preserve what was, let's realistically debate the world we want. Privacy is a relatively modern idea, born of human progress. It should continue to evolve as we continue to progress.

Jonathan Salem Baskin, "Let's Stop Fetishizing Tech," May 24, 2019

An op-ed in today's *New York Times* entitled "Let's Stop Fetishizing Privacy" was a lovingly blind paean to the glories of unrestricted and unrepentant technology. The last paragraph read like a challenge to those who might disagree with the author:

> "Progress is a messy business. Instead of trying to preserve what was, let's realistically debate the world we want. Privacy is a relatively modern idea, born of human progress. It should continue to evolve as we continue to progress."

OK, game on.

First off, let's skip the sweeping generalizations and invented strawmen:
Privacy advocates aren't Luddites who don't believe in progress, or hope to undermine competition.
Consumers don't have much control over the business practices of tech firms; in fact, we've reached a point at which we can't function without them, irrespective of our opinions.

Government involvement isn't inherently evil or wrong (after all, it gave us ARPANET), and the opacity of digital business practices has kept them in the dark, along with most of the rest of us.

Now to the author's specific arguments:

Regulating tech companies could create problems worse then the hoped-for solutions. Unintended consequences are an issue, for sure, and we only have to look at what no regulation of digital businesses has made possible or worse: social discord, bullying and personality disorders, an even greater fetishizing of children as consumers, and all of the crime that is exclusively online. Do we really have to endure these awful problems, not to mention all of the long-term effects we can't yet imagine, because trying to ameliorate them could be worse?

Regulating tech companies could damage the world's economy. The author cites employment in the tech sector, but really bases this argument on all those gig economy workers who depend on the free flow of data as the drivers of economic growth. Only that growth comes with immense side-effects (see point above), not to mention the fact that the vast majority of the revenue stemming from that free flow of data goes to the owners of capital, not to workers (most Uber and Lyft drivers make under $4/hour, for instance). So the author is right on this point, however unintentionally: Since tech companies are certainly remaking the world's economy, we should debate if it's the world we want.

Innovation will suffer. Yeah, right. Pretty much anything that gets done digitally was invented in the analog world, and in every instance those innovations were regulated. Roads and buildings get built even though there are regulations to keep them safe. Disclosure regulations doesn't stop companies from raising money or going public, and accounting rules don't stop people from inventing or operating successful businesses. Transparency on ingredients don't keep food makers from inventing products. makes publishing more credible, not less. The idea that regulations impede innovation is a canard.

Large tech companies may be our best line of defense against bad actors. This is actually a valid point, insomuch that they created the opportunities for those bad actors in the first place. I agree that digital business should shoulder a far greater amount of the burden and cost of keeping people safe, not just protecting their own interests in the data they've acquired. But I don't think that's what the author meant…

Lack of data networks will make it harder for Europe to compete on AI, et al. This is a hard argument to follow, but I think the author believes that requirements for user consent unduly hamper companies from getting the data they need, and then using it to operate in real-time. The US and Chinese dominance in AI and all things Internet-related is offered as proof, but maybe Europeans don't want to live in a surveillance state? Sounds like another good opportunity for that realistic debate the author proposes.

It is time to stop glorifying anonymity, because the dark web is anonymous and therefore more threatening that the web on which we chat and buy shoes, and young people kinda don't care about privacy anyway. This is typical tech propaganda on so many levels: the state of things is inevitable so why try to change it, we should take at face value the opinions of people who've been misinformed or lied to, and the big tech firms are simply agnostic to any issues of good or bad, or right or wrong (tech doesn't cause problems, people do).

Humanity's journey through history can be seen as an evolution toward more anonymity, not less, as people have fled the chance identifiers of ethnicity, class, and social roles to try to live as individuals according to their own agency. The same goes for being able to rise above mistakes, or even simple definitions declared by those personal choices, which the author argues society has a vested interest in knowing (therefore deriding the idea of "the right to be forgotten").

Forget mistakes: How about the right to rise above, or apart from the collective record of every purchase, decision, or physical movement? Are we really better off chained to an endless series of data points, both positive and negative, that yield both wondrous insights about our health while enabling businesses and governments to manipulate us?

Now that's a debate we should have, but it won't start until people like the author stop fetishizing tech.

Michael Kwet, "In Stores, Secret Surveillance Tracks Your Every Move*" NY Times*, June 16, 2019.

Imagine you are shopping in your favorite grocery store. As you approach the dairy aisle, you are sent a push notification in your phone: "10 percent off your favorite yogurt! Click here to redeem your coupon." You considered buying yogurt on your last trip to the store, but you decided against it. How did your phone know?

Your smartphone was tracking you. The grocery store got your location data and paid a shadowy group of marketers to use that information to target you with ads.

Recent reports have noted how companies use data gathered from cell towers, ambient Wi-Fi, and GPS. But the location data industry has a much more precise, and unobtrusive, tool: Bluetooth beacons.

These beacons are small, inobtrusive electronic devices that are hidden throughout the grocery store; an app on your phone that communicates with them informed the company not only that you had entered the building, but that you had lingered for two minutes in front of the low-fat Chobanis.

How Accurate Are Bluetooth Beacons?

Most location services use cell towers and GPS, but these technologies have limitations. Cell towers have wide coverage, but low location accuracy: An advertiser can think you are in Walgreens, but you're actually in McDonald's next door. GPS, by contrast, can be accurate to a radius of around five meters (16 feet), but it does not work well indoors.

Bluetooth beacons, however, can track your location accurately from a range of inches to about 50 meters. They use little energy, and they work well indoors. That has made them popular among companies that want precise tracking inside a store.

Most people aren't aware they are being watched with beacons, but the "beacosystem" tracks millions of people every day. Beacons are placed at airports, malls, subways, buses, taxis, sporting arenas, gyms, hotels, hospitals, music festivals, cinemas and museums, and even on billboards.

In order to track you or trigger an action like a coupon or message to your phone, companies need you to install an app on your phone that will recognize the beacon in the store. Retailers (like Target and Walmart) that use Bluetooth beacons typically build tracking into their own apps. But retailers want to make sure most of their customers can be tracked — not just the ones that download their own particular app. So a hidden industry of third-party location-marketing firms has proliferated in response. These companies take their beacon tracking code and bundle it into a toolkit developers can use.

The makers of many popular apps, such as those for news or weather updates, insert these toolkits into their apps. They might be paid by the beacon companies or receive other benefits, like detailed reports on their users.

Location data companies often collect additional data provided by apps. A location company called Pulsate, for example, encourages app developers to pass them customer email addresses and names.