DISRUPTIVE TECHNOLOGIES BRIEFING
February 28, 2019

Intrusive Disruptive Technology: Big Brothers Are Watching Us

The *Wall Street Journal* had an excellent series revealing how apps share users' data with Facebook without users' knowledge. So if you logged your weight, pregnancy status, or blood pressure into certain apps, Facebook got that information too, according to a 2/22 *WSJ* article. In response, a number of the apps announced that they would stop sharing the data. It's the latest black eye for Facebook, but the company is far from the only organization collecting reams of data on our every move.

As the Internet of Things takes off, the data collected on our "private" behavior is exploding. Any "smart" device—cars, door locks, fitness and health wearables, security systems, speakers, and appliances—may be collecting data about us. And as cameras have gotten less expensive and identification software has improved, cameras have begun popping up in unexpected places, including advertisements and even airplane seats. Perhaps most disconcerting: DNA databases can now identify everyone, regardless of whether or not a person has provided a DNA sample.

So far, there's barely a hue and cry over privacy encroachment. The usefulness of connected items seems to outweigh privacy concerns. In fact, people in China barely blink at all the personal information the government collects. But things have a way of unexpectedly reaching a tipping point. Below, Jackie lays out numerous ways Big Brothers are watching:

(1) *Smile, you're on Candid Camera*. Cameras have gotten small and cheap, and now they're everywhere. There are dozens of hidden cameras built into Westfield shopping centers' digital advertising billboards in Australia and New Zealand. "The semi-camouflaged cameras can determine not only your age and gender but your mood, cueing up tailored advertisements within seconds, thanks to facial detection technology," according to a 2/23 article in *The Guardian*.

There are more than 1,600 billboards installed in 41 Westfield centers across Australia and New Zealand. The data collected are anonymous and collected using facial detection, not facial recognition, software. In other words, the cameras only want to know how old and cheery you are, not exactly who you are. But that seems like a distinction that could quickly be programmed away without notification.

China has more than 176 million cameras used for street surveillance, policing, and business. In cashless stores, customers pay simply by having their faces scanned. At hotels, customers can check in or pay with a facial scan, *The Guardian* article noted.

Singapore Airlines' planes have a camera in the back of seats. The airline said the cameras were put there by the plane's manufacturer and were disabled and not being used, according to this 2/19 article on CNET.

And if you think your mug is safe in the USA, think again. New York City has more than 1,600

LinkNYC kiosks, which provide free Wi-Fi to all. Almost 10 feet tall, they have screens filled with advertisements and fun facts. Each kiosk also has three cameras, 30 sensors, and heightened sight lines for viewing above crowds, according to a 9/8 article in *The Intercept*.

The kiosks are owned by CityBridge, a group of private companies including Intersection. One of Intersection's largest investors is Sidewalk Labs, which is owned by Alphabet. Sidewalk Labs CEO Daniel Doctoroff, who was also NYC's former deputy mayor of economic development, has said: "By having access to the browsing activity of people using the Wi-Fi—all anonymized and aggregated—we can actually then target ads to people in proximity and then obviously over time, track them through lots of different things, like beacons and location services, as well as their browsing activity. So, in effect, what we're doing is replicating the digital experience in physical space."

City officials say they will protect citizens' privacy. "[T]he City does not, and will never, allow the network operator—CityBridge—to exploit individual identifiers or precise location of LinkNYC users," said Samir Saini, Commissioner of the NYC Department of Information Technology and Telecommunications. However, the company doesn't undergo regular audits.

(2) *The spy at home*. Internet-connected devices in our home are increasingly common. And while that may mean added convenience, these devices and their apps may be producing—and collecting—data about you and your home. *Which?*, a UK publication akin to *Consumer Reports*, studied a number of home devices to determine what information was being collected and published results in a 6/1 article.

A HP Envy 5020 printer sends to HP servers the file name, size, and number of pages being printed along with the ink being used. A Philips Sonicare Bluetooth electric toothbrush sends Philips data on users' brushing frequency and technique if the app is being used.

The ieGeek 1080p wireless security camera's app gave testers access to more than 200,000 passwords and device IDs for other ieGeek cameras. "We could then see live video feeds of other users, and talk to those users via the camera's microphone (which we didn't do). ieGeek/Sricam fixed this flaw in late March 2018, but we've subsequently found and disclosed other critical vulnerabilities with the camera and app," the article stated. The iRobot Roomba vac uses a camera to create a map of the rooms in your house that it can store in the company's cloud.

Household devices continue to get smarter. Amazon filed a patent for a new version of Alexa that can analyze speech and emotion, according to a 10/9 article in *The Telegraph*. A user who is coughing while speaking to Alexa will be offered the opportunity to buy chicken soup or cough drops at Amazon. More creepily, the device can track emotions, detect by your voice if you are bored, tired, or crying, and suggest things to do for those moods.

The Telegraph notes that a patent filing is not proof that the company is working on the features described or will be successful creating such products. But it certainly doesn't seem like a stretch.

(3) *Given away by DNA*. Here's an amazing statistic: Only 2% of people with European heritage have to share their DNA in order to identify DNA samples from the 98% of people who have not shared their DNA. So if your cousin gets her DNA tested, law enforcement officials may be able to tap into that DNA sample to identify you as the killer.

GEDmatch and FamilyTreeDNA allow law enforcement to acess their data bases, according to a 2/26 Bloomberg article. Police compared crime-scene DNA to DNA collected by GEDmatch. They found family bloodlines that matched the crime-scene DNA and used other social media sources to build a family tree that led to the arrest of the Golden State Killer.

(4) *The dark side.* While data from a toothbrush or pictures taken by a Wi-Fi booth may seem innocuous, it's easy to see how nefarious situations could arise. "Imagine drug companies using [DNA] to target ads, life insurers using vast networks of relatedness to determine risk, or a scorned ex-lover employing the technique in some very 21st century stalking," the Bloomberg article warned.

Trouble is already brewing in China, which ran a program dubbed "Physicals for All" in Xinjian, home to Muslim Uighurs. The government has detained up to a million Uighurs in camps to "re-educate" them and encourage them to be more subservient to the Communist Party, explains a 2/21 *NYT* article.

Government officials collected DNA samples, iris scans, and other personal data from 36 million people in Xinjian over two years, presumably without consent. "Collecting genetic material is a key part of China's campaign, according to human rights groups and Uighur activists. They say a comprehensive DNA database could be used to chase down any Uighurs who resist conforming to the campaign," the article explained. A slippery slope indeed.

Consider the tech industry officially on notice. Federal Trade Commission's (FTC) Bureau of Competition has announced the creation of a task force that will monitor competition in US technology markets, watching for anticompetitive conduct. The task force will include experts in online advertising, social networking, mobile operating systems and apps, and platform businesses, and it will coordinate with its counterparts in the FTC's Bureau of Consumer Protection.

Mike O'Rourke, chief market strategist at Jones Trading, highlighted the task force and its formation "under an Administration that touts itself as the most de-regulatory Administration in the history of the United States."

We'll be watching to see if the feds are watching how Big Brother is watching us.

Contact us by email or call 480-664-1333.

Ed Yardeni, President & Chief Investment Strategist, 516-972-7683
Debbie Johnson, Chief Economist, 480-664-1333
Joe Abbott, Chief Quantitative Strategist, 732-497-5306
Melissa Tagg, Director of Research Projects & Operations, 516-782-9967
Mali Quintana, Senior Economist, 480-664-1333
Jackie Doherty, Contributing Editor, 917-328-6848
Valerie de la Rue, Director of Institutional Sales, 516-277-2432
Mary Fanslau, Manager of Client Services, 480-664-1333
Sandy Cohan, Senior Editor, 570-775-6823