Beyond Big Brother

Dallas' new Sam's Club Now location foreshadows greater corporate privacy challenges.

by **STEVE THOMAS**

SHUTTERSTOCK

DALLAS IS GROUND ZERO for an innovative experiment that heralds a future where consumers enjoy personalized, interactive, brick-and-mortar shopping, but that also portends crushing privacy obligations for every industry that operates in the retail space. In November, Walmart opened its first Dallas Sam's Club Now on Greenville Avenue. No cashiers. Shoppers must download and use the Sam's Club Now app and use their phones to scan every purchase. To pay, they simply scan a code with an exit host as they leave.

That app incorporates Walmart's proprietary "Scan & Go" technology, which was tested in Texas, Arkansas, Florida, and Tennessee, but abandoned in May because, according to third-party reports, the basket size of a typical Walmart shopping trip made the process difficult for many customers. A Walmart spokesperson admitted that "there was low participation."

Yet just six months later, Sam's Club Now opened in Dallas. It's totally reliant on that same technology, but also backed by a new tech office in downtown Dallas, separate from other Sam's Club and Walmart technology operations in California and Arkansas, and the only Sam's Club office dedicated solely to tech work. The company chose Dallas for SCN and its new technology office because of local tech talent and recruiting potential, and because it's just a five-hour drive from Walmart headquarters in Bentonville, Arkansas.

At the end of October, CEO Jamie Iannone said SCN "will be the epicenter of innovation for Sam's Club." He characterized the new store as "a technology lab that doubles as a live, retail club" where the company will "incubate, test, and refine technologies to help define the future of retail." Along with scanning purchases and handling payment, the SCN app helps shoppers navigate aisles and locate items. It keeps track of prior purchases and can make suggestions for additional items to buy. "We'll use all available technologies," said Iannone, "including computer vision, augmented reality, machine learning, artificial intelligence, robotics, just to name a few—to redefine the retail experience."

Eventually, the Dallas store will be equipped with more than 700 cameras to help "manage inventory in new ways and optimize the layout," said Iannone, which implies keeping a close eye on consumer behavior.

The Walmart organization is not doing this for grins. Despite being the world's third-largest supermarket chain by number of locations, and the world's third-largest employer after the U.S. Department of Defense and China's People's Liberation Army, Walmart faces stiff competition for dominance in the swift evolution of interactive physical retail.

"Unattended retail" has been around a long time, growing from the humble vending machine to the self-checkout kiosks deployed in many grocery stores over the last decade. But e-commerce is making continuous gains, and now Amazon (which owns Whole Foods Market) has the industry on edge with plans to open as many as 3,000 cashierless Amazon Go stores by 2021. Retailers are rushing to catch up, including Kroger and Albertson's in North Texas, each of which is charting its own path toward a cashierless future.

DETAILED CONSUMER DOSSIERS

Critical to these cashierless projects is the systematic monitoring and capture of consumer shopping decisions and preferences, which are then often coupled with other "big data" information available to provide those shoppers with a more personalized experience. Information captured by retailers, both online and ►

continued from page 63

in stores, often finds its way into the treasure troves of data brokers, allowing them to develop and sell incredibly detailed consumer dossiers that go far beyond demographics to include behavioral quirks, biases, religious beliefs, purchasing patterns, and a host of other personal details.

Four years ago, 91 percent of respondents to a Pew Research survey said they "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used. Legislators and regulators recognize the problem, and have been scrambling to catch up, hurriedly knitting a patchwork of sector-specific laws with little coordination among jurisdictions. The Federal Trade Commission, for example, is watching big data, brokers of data, and how companies obtain, use, and protect consumer information. The U.S. lacks a comprehensive data security law, so as an interim method of addressing privacy concerns, the FTC has used its general authority under Section 5 of the FTC Act, which authorizes it to investigate "unfair or deceptive acts and practices in or affecting commerce."

INCREASED SCRUTINY

In 2014, the FTC used Section 5 to bring claims against data brokers and others for selling payday loan application information to third parties that used the data to unlawfully debit consumer bank accounts. After settling the matter in 2016, the FTC noted that regulators "are examining companies that trade in consumer information with increased scrutiny." Relying on Section 5 gives the FTC broad authority to address such clearly criminal conduct and to demand that companies live up to promises made in their privacy policies, but offers little guidance to industries and wholly fails to address a variety of activities involving consumer information that privacy policies don't clearly reveal. Telling consumers that their information will be used "for marketing purposes" could mean adding their name to an email list or selling their buying habits to the highest bidder.

Over the past decade, the Texas legislature has passed several privacy laws, one example being the addition to the Business & Commerce Code of Title 11, addressing "Personal Identity Information," which includes an entire chapter prohibiting a person (such as a data broker) from "reidentifying" information that has been "deidentified" and released by a state agency. And many states, including Texas, now have data breach notification laws running parallel to federal laws.

More ominous, however, is the European Union's General Data Protection Regulation (GDPR), effective May 25, 2018,

which imposes a host of responsibilities on those who collect information on individuals (even their own employees), including various required notices to the individuals, records of any uses of the information, restrictions on transferring the information out of the EU, and an obligation to modify information systems to give those individuals access and editing capabilities.

Because the GDPR applies to virtually any enterprise that has activities in the EU, companies in the United States are by no means immune.

NO AVOIDING BIG DATA

The regulations discussed above are just the beginning. Every data breach puts more pressure on legislators to impose greater legal protections for personal information. And the breaches keep happening. On Nov. 30, 2018, Marriott announced a massive data breach dating back four years and exposing the personal information of about 500 million customers.

That breach was limited to factual details such as passport numbers, dates of birth, and credit card information. Stores like Sam's Club Now and Amazon Go will be collecting behavioral information—the kind of details data brokers and marketers salivate over. In a report issued four years ago, the FTC found that data brokers "operate with a fundamental lack of transparency," and recommended that "Congress consider enacting legislation to make data broker practices more visible to consumers and to give consumers greater control over the immense amounts of personal information about them collected and shared by data brokers." Such protections necessarily would extend to retail stores collecting the information.

Giving individuals greater control over the use of their personal information was a primary goal of the GDPR, and future legislation in the U.S. will almost certainly impose similar requirements. The more information companies collect, and the greater the sensitivity of that information, the more likely they are to be subject to significant compliance obligations.

There's no avoiding big data. As with the historical appearances of electricity and the internet, its development is forcing companies to assess its impact and innovate accordingly or risk being left behind. Part of that impact will be substantial burdens for compliance with privacy laws, including disclosure of information uses, mechanisms for consumer access and editing, even deletion rights, and likely much more as the regulatory landscape develops. D

STEVE THOMAS IS A BUSINESS AND TECHNOLOGY LITIGATOR IN DALLAS.