

STATEMENT OF NUALA O'CONNOR
SENIOR VICE PRESIDENT AND CHIEF COUNSEL FOR
DIGITAL CITIZENSHIP WALMART INC.
BEFORE THE UNITED STATES SENATE COMMITTEE ON
COMMERCE, SCIENCE, AND TRANSPORTATION
HEARING ON
EXAMINING LEGISLATIVE PROPOSALS
TO PROTECT CONSUMER DATA PRIVACY
DECEMBER 4, 2019

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to be here today. It is an honor to be part of such a distinguished panel. My name is Nuala O'Connor and I serve as the Senior Vice President and Chief Counsel for Digital Citizenship at Walmart. Walmart is a leading retailer serving customers in stores, online, and through their mobile devices. As our customers' shopping habits and expectations have changed, Walmart continues to evolve to meet their needs.

Our customers have integrated technology into almost every aspect of their daily lives -- including how they shop. Our customers expect a seamless experience, in store and online. Walmart is using technology and data to help our customers save both time and money. For example, connecting our app to our stores makes it easier to return items in a store after purchasing online. Data -- both about products and about customers - is helping us better source and manage our supply chain, more efficiently and quickly ship orders, and helps us anticipate customers' needs. Walmart is also using data and technology to improve food safety and respond to weather emergencies for our associates and customers. Indeed, it is very appropriate that we are talking about service and shipping and shopping today. Did you know there are only 21 shopping days until Christmas?

We at Walmart believe that data and technology can help our customers save money and live better. Walmart also recognizes that while personal data can enhance the customer experience, it creates responsibility on the part of the companies that hold it.

Walmart's goal is, quite simply, to be the country's most trusted retailer. Just as our customers trust Walmart to provide **every day low prices**, quality goods, and a **fast and friendly** store experience, so too our customers trust us to protect their data, and to use that data in a way that benefits them. While technology may have changed how we operate our business, it has not -- and it will not -- change our values.

In my brief time at Walmart, I've learned the importance the company places on its core values, including **Respect for the Individual**. It means meeting people where they are with dignity. In store, it means we greet our customers and help them find what they need. Online, it also means we greet our customers and help them find what they need. And in all cases, we safeguard their transactions and identity. Our business is selling products to the customer, **not** selling the customer's personally identifiable information.

Walmart is committed to working with policymakers to create public policy that will enhance consumer privacy, whether we meet those customers in the physical world, in the digital world, or, as is increasingly the case, both. We strongly support the *bipartisan* efforts of Members of this Committee as we work towards a national privacy law that protects the rights of all consumers in the United States.

Broadly, we support:

- **Customer Control** – Customers should have reasonable controls with regard to the collection, use and sharing of personal data. Customers should have an opportunity to reasonably access, correct or delete their data while limiting the sale of their data to third parties and its use in digital advertising.
- **Retail Sensibility** – Federal privacy policy should reflect a world blended with physical and digital experiences.
- **Consistency** – Policymakers should harmonize U.S. privacy legislation, preempting a patchwork of state laws.
- **Flexibility** – The rights and obligations of a national framework should be sufficiently flexible to preserve the ability for companies to innovate for their customers.

Towards that goal, we would like to offer a few reflections for the Committee’s consideration:

First, a comprehensive federal privacy law is urgently needed; a patchwork of inconsistent state law is insufficient to protect individual privacy and is inefficient for interstate commerce.

Because our roots are in the physical world, our perspective may differ from companies that operate primarily online. Walmart operates more than 4,700 stores in the United States. Each week, nearly 160 million people around the country shop with us – either at one of our stores or online. Our stores are present in local communities and are part of Americans’ daily lives in every state. Our customers often know our store associates by name and these personal relationships build trust. When customers buy something from our shelves, they trust us to have sourced it responsibly and to have priced it accordingly. They trust it to be a genuine product. They trust that they are being treated fairly.

Responsible data privacy is part of that trust. Building that trust requires clarity and consistency. While states have an important part to play, a patchwork of state laws would only serve to complicate, not clarify, the customer experience. For example, if I use my Walmart app, which you should all download if you haven’t already, on my 516-area code number, from my home in Maryland, to order the WoodWick Frasier Fir holiday candle to send to my sister in New Jersey (which in fact I did just last week – it’s amazing), from our website hosted in California, and the candle is shipped from Arkansas, which state privacy law would the company need to adhere to as it processes my data? My state? Or my sister’s? Alternatively, if a customer lives on the California border and shops at a Walmart in Nevada, does the Nevada store necessarily then give that customer, or all customers, California rights? Absent alignment on

state privacy laws, these implementation questions add complexity, uncertainty, and cost for the customer and company alike.

Second, legislation focused on a particular industry sector must be carefully crafted to avoid unintended effects on retail or other sectors.

For example, the concept of data portability was originally intended to provide greater control over an individual's social media communications or online accounts. However, data portability may have negative consequences in a blended business model or other industries. Should a national privacy law require us to directly port our customer data to another competitor, even in aggregated form, we are concerned that this data could be reverse engineered and allow competitors to discern proprietary business information and processes. Additionally, we have concerns about the security of customer data while in transit. We believe that the concept of data portability must simultaneously recognize values of individual privacy, technological innovation, and data security. We appreciate the work of Senators Warner, Hawley, and Blumenthal on data portability in their ACCESS Act (S. 2658) and we hope to see similarly nuanced treatment of data portability in the bipartisan bill.

Third, a comprehensive privacy law must consider the needs and operations of companies online, offline, and blended, or omnichannel. Legislation focused solely on the online space must not disadvantage or privilege similar activity in the physical world.

In my time at Walmart, I've learned a lot of acronyms, and so one I want to leave with you to day is: BOPI. What is a BOPI? It is a transaction where you buy something online and pick up instore. Walmart is doing great things with online grocery ordering and instore pickup and I encourage you to check it out. I did my first BOPI a few years ago, when I was buying a new bicycle for my daughter. As a busy working mother, I was scouring the internet late one night for deals on this particular yellow bike she wanted. Many excellent retailers could have sent it to us and dropped it, unassembled, on my front porch. But Walmart had it ready for pickup, already assembled. I walked in and showed them my phone with the purchase information, and I spent the weekend riding bikes with my children, instead of putting that bike together. That's the success of online ordering and instore pickup. It saved my family time and money, and allowed us to live better. That is our goal, and we hope legislation will provide a level playing field for companies, whether online, offline, or omnichannel – which is both.

Data portability is just one example of how policy to address digital actors can have unintended consequences for retail operations. We look forward to a continued dialogue with Members of this Committee to better understand things such as whether or not retailers are considered "edge providers" and how algorithm notification should apply to retail websites where sometimes hundreds of algorithms are used to create a seamless, consumer-requested personalization.

As a longtime privacy professional, I am delighted and grateful to see this momentum towards a comprehensive privacy law. Most recently, in the drafts released last week by Chairman Wicker and Ranking Member Cantwell, we greatly appreciate the transparency and consumer rights created by both proposals; the emphasis on data security – which is so essential

to maintaining personal privacy; the specific provisions that recognize commonly controlled and branded entities; and the recognition that data is used for broader consumer benefits, such as product recalls. We appreciate the balance struck by Chairman Wicker with structured rulemaking authority for the Federal Trade Commission. Conversely, we share broader industry concerns with Ranking Member Cantwell's draft related to provisions on private rights of action and preemption. We also believe some elements of both proposals could impede legitimate and beneficial uses of technology, such as using data to shorten wait times at our stores; communicating with customers about the timing of grocery pickups; and otherwise facilitating the customer experience and transaction efficiency.

Finally, regarding data practices at Walmart, please see the attached appendix. Thank you again, Chairman Wicker and Ranking Member Cantwell, for the opportunity to share how Walmart works to maintain and safeguard our customers' trust. We strongly support your efforts to update public policy to reflect the reality of our customers, whose retail habits include online transactions, store transactions, and some that are a combination of both. We look forward to supporting your efforts as you work towards a national privacy law. I stand ready to answer any questions you may have.

APPENDIX: Data usage at Walmart

We look forward to a continued dialogue during this process as we work to ensure customers' rights are protected not just in retail but across all industries.

Below please see data practices and usage as they apply to Walmart Inc. in the U.S., which includes Walmart Stores, Sam's Club and several recently acquired companies. Our customer-facing privacy policies describe our online and offline customer data practices. This information describes our practices related to individually identifiable customer data, not data that has been aggregated or anonymized. The data practices of Walmart's recently-acquired companies generally align with those of Walmart Inc. and Sam's Club. To the extent that there are substantive differences, they are noted in the discussion below.

Direct/indirect data collection (including from third parties): Walmart collects data to complete transactions and to provide services for our customers. The customer data we collect is also used to enhance the design of our customers' experiences in our stores, on our mobile apps, and online. For us, the purpose of data collection is to provide the best products and shopping experience to our customers, not to turn our customers into products.

The specific categories of customer information we collect, directly or indirectly, to better serve our customers include information we receive from our customers and information we receive from others:

- **Personal Information Provided Directly by Our Customers** – Our customers provide personal information directly to us, whether by creating accounts on our digital properties (e.g., Walmart.com, Walmart Mobile App/Walmart Pay, Sam's Club Membership), through transactions online, by shopping in one of our physical locations, or through other services we offer (e.g., Auto Centers, Vision Centers, and Pharmacies).
- **Personal Information Provided by 3rd parties** – We also receive personal information about our customers from other sources to help correct or supplement our records, improve the quality and personalization of our services, and to detect, prevent and, investigate fraud.
- **Purchase/Transaction History** – When customers shop with us, whether online or in our stores, we collect data about their purchases and transactions not only to facilitate common retail functions like payment processing, product returns, and product recalls, but also to develop insights that will inform our efforts to make our customers' interactions with us easier and more enjoyable, and to let our customers know about other products and services they may want.
- **Health Care Data** – We also seek to help patients live healthier lives by using the data they provide to our pharmacies, vision centers, and care clinics. We use patient data to deliver treatment, payment, and health care services as well as to perform health care operations. The data is collected either directly from the patients or may be collected from their physicians, health insurance company, or others involved directly in their health care. Treatment and health care services include programs such as medication therapy management or prescription refill reminders. Health care operations include internal analytics and quality review activities. We collect,

protect, and use this data in compliance with state and federal health care privacy and security laws.

- **Browsing Information** – In order to provide a continuous and more personalized shopping experience, we use tools to collect browsing information, such as first-party cookies and web beacons to collect information about the use of our websites and mobile apps. From this, we can measure the effectiveness of our online customer interactions to help improve the customer shopping experience for future visits while also ensuring a seamless and pleasant experience during the current session. For example, this would allow our customers to shop on our website, leave to check another site, and then return to our site where they left off and continue their shopping experience. As a participant in ad networks, we allow third-party cookies on our website in order to provide our customers with a more personalized experience, where products are presented through more relevant advertising, and for website analytics.
- **Device Information** – When customers use our online sites, mobile apps, or other services, we may collect technical device information in order to provide our services. Examples of device information we collect include Internet Protocol (IP) address, the type of mobile device or browser used, a unique device identifier, and other information about a customer’s session on our websites.
- **Location Information** – We are continually improving the in-store shopping experience to make it easier for our customers to locate products within the store. For example, when accessing Walmart.com from a desktop browser, we are able to use our customers’ IP address to help them locate the nearest store. When customers enable location sharing through one of our mobile apps on their devices, we can provide information about the nearest Walmart or Sam’s Club. Also, enabling location sharing allows customers to search a store’s unique product inventory, locate departments and products within the store, and facilitate online grocery pick-up. Finally, we may be able to recognize the location of a mobile device in stores where we provide customers free WiFi access.

We do not sell or rent individually identifiable customer data to third parties. Under some circumstances, we may share individually identifiable customer data with third parties: (i) to help with our business activities, including fulfilling customer orders and processing payments through service providers like shipping or billing vendors, payment card processors, third-party delivery services, and our marketplace vendors; (ii) to offer optional third-party service or installation plans on the products we sell, and to offer co-branded products or services, such as a co-branded Walmart credit card; (iii) in response to a valid legal or law enforcement inquiry, subpoena or search warrant or for the protection and safety of customers; (iv) to help customers choose from a range of financial services products for which Walmart is an agent; or (v) with a customer’s consent.

Some of Walmart’s recent acquisitions share customer information, such as customer names, addresses, and email addresses, with other companies for their own marketing and business purposes. These sharing practices are disclosed in the privacy policies of the Walmart acquisitions that participate in these practices, and customers can opt out of this sharing.

Data Usage: Aggregate and anonymized customer data provides us with insights to improve our services and products. There are also some instances where individually identifiable customer data is used to enhance these insights or provide our customers with a more personalized experience. For example, we use such insights to better communicate with our customers through email, social media, and responses to surveys. Additionally, we use data about our customers' purchases to make it easier for them to quickly reorder frequently purchased items and personalize product recommendations.

Customer Access: Customers who have an online account can view the information they have provided to us online and also a record of their recent online transactions and purchases made in-store using Walmart Pay. Since the ability for the customer to view this information is tied to accessing the profile for the online account, customers without online accounts with us are unable to view similar information. Patients of our pharmacies, vision centers, and clinics have the ability to request copies of their medical records and may also request an accounting of how their Protected Health Information has been disclosed in accordance with applicable law. Beginning in January 2020, we will provide California residents with additional ability to request access to their personal information as specified under CCPA.

Advertising: Walmart uses customer information to offer advertising services to third parties. However, Walmart does not share individual customer's personally identifiable information as part of this business. We also allow third-party cookies on our website in order to permit our advertisers to provide our customers with a more personalized experience, where their products are presented through more relevant advertising.