United States Securities and Exchange Commission
Washington, D.C. 20549

NOTICE OF EXEMPT SOLICITATION
Pursuant to Rule 14a-103

Name of the Registrant: Walmart, Inc.
Name of persons relying on exemption: Clean Yield Asset Management
Address of persons relying on exemption: 16 Beaver Meadow Rd, Norwich, VT 05055

Written materials are submitted pursuant to Rule 14a-6(g) (1) promulgated under the Securities Exchange Act of 1934. Submission is not required of this filer under the terms of the Rule, but is made voluntarily in the interest of public disclosure and consideration of these important issues.

PROXY MEMORANDUM

TO:	Shareholders of Walmart. Inc.
RE:	Proposal No. 10 (“Report on Reproductive Rights and Data Privacy”)
DATE:	May 16, 2023
CONTACT:	Molly Betournay, molly@cleanyield.com

This is not a solicitation of authority to vote your proxy. Please DO NOT send us your proxy card; Clean Yield Asset Management is not able to vote your proxies, nor does this communication contemplate such an event. Clean Yield Asset Management urges shareholders to vote for Proposal No. 10 following the instructions provided on management's proxy mailing.

Clean Yield Asset Management urges shareholders to **vote YES on Proposal No. 10** on the 2023 proxy ballot of Walmart, Inc. (the “Company”). The Proposal’s “resolved” clause states:

Shareholders request the Board issue a public report detailing known and potential risks and costs to the Company of fulfilling information requests relating to Walmart customers for the enforcement of state laws criminalizing abortion access, and setting forth any strategies beyond legal compliance the Company may deploy to minimize or mitigate these risks. The report should be produced at reasonable expense, exclude proprietary or privileged information, and be published within one year of the annual meeting.

Why a YES Vote is Warranted: Rationale in Support of the Proposal

1. Walmart handles sensitive consumer data that may be vulnerable to prosecutions concerning abortion access.
2. Walmart does not offer transparency reporting on law enforcement data requests, exposing the Company to financial and reputational risks.
3. Walmart's data sharing practices are vague and unclear to consumers and investors.
4. Regulatory and legal compliance is insufficient to minimize privacy risks related to reproductive healthcare.
5. Production of the requested report would be cost-effective and a good use of resources.

About Clean Yield Asset Management

Clean Yield Asset Management is an investment firm based in Norwich, VT specializing in socially responsible asset management. We have filed this shareholder proposal on behalf of our client, Julie Kalish, a long-term shareholder in Walmart, because the Company amasses large amounts of sensitive consumer data but lacks transparency as to how such data may imperil access to reproductive healthcare. In a time when abortion access is criminalized or severely restricted by half of the states, greater understanding about the Company's data handling practices is warranted.

Background on the Proposal

Reproductive rights are under siege in the United States. State lawmakers have enacted more than 1,380 restrictions on abortion access since *Roe v. Wade* – the U.S. Supreme Court ruling in 1973 that legalized the procedure.[1] Following the reversal of *Roe v. Wade* in June 2022, twelve states have banned most abortion services outright.[2] The Supreme Court is likely to rule on a case in the coming weeks that will decide the future of medication abortion in the United States.

[1] https://tinyurl.com/4az3pce3

The overturning of constitutional protections for abortion access elevates the need for the report requested in this Proposal. Law enforcement in abortion-restrictive states have relied on consumer data to investigate and prosecute individuals who have sought abortions or have provided aid to those who have and are expected to continue to do so.

A digital reproductive health footprint can be easily accessed by law enforcement and lead to criminal or civil charges. Meta recently received significant negative press after complying with a data request from a local Nebraska police department for private Facebook messages between a mother and daughter, who were both subsequently charged with felony crimes related to the alleged illegal termination of the daughter's pregnancy (for additional examples, see Addendum A).[3]

As a nationwide business, the Company amasses large troves of consumer data. Walmart is America's leading brick-and-mortar retailer,[4] with 90% of the U.S. population living within 10 miles of its stores.[5] In fact, just one Walmart store in the U.S. serves an average of 10,000 customers every day.[6] Walmart is also the second largest e-commerce company and the fifth largest pharmacy by prescription drugs market share in the United States.[7] Notwithstanding, **Walmart has been largely silent on the issue of data privacy following the revocation of constitutional abortion protections**.

Given the sensitive nature of the Company's data, **Walmart will be especially vulnerable to law enforcement data requests related to abortion, particularly with respect to interstate conflicts regarding exercise of reproductive rights in states where abortion remains legal**. Idaho, for instance, criminalizes interstate travel to obtain a legal abortion under certain circumstances.[8] Yet, Americans largely oppose criminalizing abortion, thereby amplifying the risk of reputational damage that may ensue from the Company's participation in the enforcement of abortion-related criminal laws. Indeed, a May 2023 Kaiser Family Foundation national survey found that "majorities of the U.S. public oppose criminalizing women, doctors, or people who assist those seeking abortion care."[9] According to the Kaiser survey, at least two-thirds of respondents living in certain states threatened by abortion bans opposed "criminalizing doctors for performing abortions (69%), making it a crime for women to cross state lines to get an abortion (76%), making it a crime for a woman to get an abortion (74%), or allowing private citizens to sue people who provide or assist in abortions (78%)." Similarly, a January 2023 national poll from Change Research on behalf of Planned Parenthood reveals that "Americans strongly oppose law enforcement being used to enforce abortion bans."[10]

---

[2] https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html

[3] https://tinyurl.com/msazvebu

[4] https://nrf.com/resources/top-retailers/top-100-retailers/top-100-retailers-2022-list

[5] https://corporate.walmart.com/about

[6] https://tinyurl.com/yxx5syby

[7] https://tinyurl.com/79kbkkk9; https://tinyurl.com/4h85xubj

[8] https://tinyurl.com/y2a79x4c

[9] https://www.kff.org/womens-health-policy/poll-finding/kff-health-tracking-poll-views-knowledge-abortion-2022/

[10] https://changeresearch.com/wp-content/uploads/2023/01/PPFA-_-Poll-Results-January-2023-1.pdf

Shareholders have reason to be concerned about whether the enforcement of criminal abortion laws will impact the reputation and financial wellbeing of the Company. The Proposal thus calls upon management to examine the risks associated with the Company's current data handling practices, including its response to government information requests, in the face of new restrictive abortion laws.

1. Walmart handles sensitive consumer data that may be vulnerable to prosecutions concerning abortion access.

Consumers interact with the Company through various ways. They may shop in-store or via the Walmart app, browse the Walmart website to learn about products, use the Company's medical and pharmacy services, or contact customer care. By way of these interactions, Walmart collects detailed and sensitive data from consumers, including geolocation data, purchase and transaction history, demographic information, and inferences related to customers' shopping patterns and behaviors.[11] Walmart Health & Wellness and related operations also collect personal health information ("PHI") from patients who use Walmart's various pharmacy and medical services.[12]

While medical records – which the Company keeps – is one of the "most definitive proof[s]" of conduct related to illegal abortions,[13] officials who cannot get those records may search for other evidence such as information about consumer purchases (e.g., pregnancy tests or abortion medication) or searches related to abortion (e.g., searching for "mifepristone" in Walmart's search tool). Less granular consumer data may also provide evidence supporting abortion-related prosecutions, including "information regarding the payer, the payee, the payment amount, and the users' transaction labels."[14]

_____

[11] https://corporate.walmart.com/privacy-security/walmart-privacy-notice

[12] https://corporate.walmart.com/privacy-security/notices/

[13] https://www.nytimes.com/2022/06/29/business/payment-data-abortion-evidence.html

[14] https://tinyurl.com/3dp5tx2r

Given the current environment the Company is operating in following the revocation of constitutional abortion rights in the United States, consumers' digital reproductive health footprint is at risk of being obtained through law enforcement data requests with the intent to prosecute those who have received an abortion, even when the procedure is legal. We believe it is crucial that Walmart explore all options to protect users from these risks.

2. Walmart does not offer transparency reporting regarding law enforcement data requests, exposing the Company to financial and reputational risks.

A recent empirical study in the *Journal of Marketing* showed that the misuse of commercial data can generate negative outcomes for businesses, including negative abnormal stock returns and damaging customer behaviors such as negative word of mouth and switching to a close business rival.[15] These negative customer effects are due to both anxiety about the potential for data misuse and feelings of corporate betrayal, as well as actual data misuse. Corporations collecting large troves of consumer data, such as Walmart, are thus exposing themselves to higher financial and reputational risks. Apropos to the current Proposal, the study found that data transparency, among other things, can alleviate these detrimental effects.

Walmart does not publish transparency reporting on the issue of law enforcement data requests, in contrast to many other publicly traded companies. **CVS – an industry competitor – recently announced that it will publish "semiannual transparency reports on the number of legal information requests received," among other privacy-related information.[16] Amazon – Walmart's biggest e-commerce rival – as well as Meta, Google and Apple also offer such reporting semiannually**, including details on the types of data requests, compliance rates and jurisdictional information.[17] This information would be extremely helpful for investors to make determinations about the Company's risk exposure as well as serve as an accountability tool. In turn, consumers would gain more assurances that Walmart respects the privacy of their data.

---

[15] *See* Kelly D. Martin et al., *Data Privacy: Effects on Customer and Firm Performance*, 81.1 Journal of Marketing at 36-58 (2017), https://doi.org/10.1509/jm.15.0497

[16] https://tinyurl.com/5yt3xnn7

[17] https://tinyurl.com/e7j4me8u (Meta); https://tinyurl.com/y37bzv97 (Amazon); https://tinyurl.com/4bvubser (Google); https://tinyurl.com/4zbwk6bv (Apple).

A Response to Walmart's Opposition Statement

3. Walmart's data sharing practices are vague and unclear to consumers and investors.

In opposing the Proposal, Walmart states consumers may easily access the Company's privacy notices to learn how their data may be used. However, these notices seem to lack critical information as to how and under which circumstances law enforcement may access customer data.

Walmart's Privacy Notice only states that the Company may share consumer data with third parties when the Company "believe[s] sharing will help to protect the safety, property, or rights of Walmart, [its] customers, [its] associates, or other persons."[18] Pursuant to this provision, it is unclear whether conduct related to criminalized abortion would be considered a situation where the Company could share consumer data. Moreover, **Walmart has failed to clarify if a data request from law enforcement must be accompanied by a court order or if the Company could voluntarily share the data**. For instance, could the Company disclose information about purchases of pregnancy tests in response to a police department seeking evidence in connection with an illegal abortion, but without a judge having ever reviewed or approved the request?

On the other hand, the Walmart Health & Wellness Notice of Privacy Practices provides that the Company "may disclose PHI to a law enforcement official for certain law enforcement purposes, such as reporting crime on our premises or responding to legitimate law enforcement inquiries,"[19] which could include criminalized abortion investigations. While the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") would normally prohibit Walmart from sharing PHI with third parties without the individual's consent, HIPAA provides an exception for law enforcement purposes. Following the revocation of abortion rights in 2022, the U.S. Department of Health and Human Services ("HHS"), which enforces HIPAA, published guidance providing stricter HIPAA protections when it comes to the law enforcement exception, which the Company has failed to expressly adopt in its privacy policies or via other Company statements.[20] According to HHS, entities regulated by HIPAA may disclose only the PHI expressly requested by a court order, but no more. In addition, HHS provides that HIPAA generally "permits but *does not require*" a covered entity to disclose PHI to law enforcement without consumer consent if the entity believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Some have argued that this exception applies to reproductive healthcare, and even to protection of a fetus, which position HHS disavows.

---

[18] https://corporate.walmart.com/privacy-security/walmart-privacy-notice

[19] https://corporate.walmart.com/privacy-security/notices/

[20] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

In contrast, **other publicly traded companies have adopted many of the foregoing HHS or HIPAA provisions as part of their privacy notices.** Amazon, for instance, provides that it "does not disclose customer information in response to government demands unless [it is] required to do so to comply with a legally valid and binding order."[21] Meta's privacy policy contains a similar provision and further states that the company "produce[s] narrowly tailored information to respond to that request."[22] Cisco Systems similarly "interpret[s] demands to produce the least data necessary to comply."[23]

Based on the Company's vague privacy notices, Walmart consumers and investors cannot ascertain whether a judicially enforceable order is necessary for the Company to turn over user data to law enforcement in all cases, or whether an informal request on government letterhead may suffice, making it easy for law enforcement to access user data without judicial scrutiny. Clarity is further needed as to how the Company will protect PHI related to reproductive health information. The requested report could provide guidance on how to correct, update or reconcile the Company's privacy notices.

4. Regulatory and legal compliance is insufficient to minimize privacy risks related to reproductive healthcare

Data privacy laws in the United States are considered by many experts to be lacking in scope and woefully outdated. In fact, there is no single, comprehensive federal law regulating how companies collect, store, or share customer data.

As the *New York Times* reports, "[t]he data collected by the vast majority of products people use every day isn't regulated."[24] In most states, companies can use, share, or sell most data they collect about consumers without notifying them that the company is doing so. There is no federal law standardizing when (or if) a company must notify consumers if their data is breached or exposed to unauthorized parties. If a company shares consumer data – including sensitive information such as an individual's web searches or location – with third parties (e.g., data brokers), those third parties can often sell the data or share it without notifying the affected consumers. HIPAA – one of the few federal privacy laws but which only protects PHI – contains the previously mentioned loopholes, which could allow Walmart to disclose information to law enforcement seeking to prosecute abortion-related crimes.

---

[21] https://tinyurl.com/y37bzv97

[22] https://transparency.fb.com/data/government-data-requests/

[23] https://tinyurl.com/4zs6akk6

[24] https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

As a result of this lax regulatory environment, many businesses have implemented firmer privacy practices that more fully protect consumers from nefarious data uses while increasing brand trust. One such practice is abiding by the principle of "data minimization," in which companies only collect personal data that is strictly necessary for delivering the service a user is expecting to receive, and use it for only that purpose.[25] Data minimization is already a legal requirement for certain companies doing business in the European Union,[26] and U.S.-based publicly traded companies like Apple and PayPal, to name a few, have already explicitly adopted this practice.[27] As a result of data minimization, companies amass less information that may be subject to law enforcement information requests or shared with third parties seeking to participate in the enforcement of abortion-restrictive laws. Notably, data minimization would also reduce the Company's liability, reputational risk exposure, and storage costs.[28] Walmart has nonetheless failed to disclose in its various privacy statements whether it abides by this principle.

Privacy experts further recommend that in order to protect consumers from being targets of abortion-related prosecutions, companies should employ data security measures such as data encryption, de-identification, and anonymization.[29] Encryption is the process of converting information or data into a code, especially to prevent unauthorized access. De-identification entails segregating personally identifiable data like names and addresses from PHI and other sensitive data that the company stores. Anonymization protects private or sensitive information by erasing identifiers that connect an individual to stored data.

While Walmart is legally required to apply some of these security measures before sharing HIPAA-covered PHI, it is unclear whether these measures could be applied to other consumer information contemplated in the Proposal such as data collected in its website (e.g., product searches, geolocation data). Sharing consumer data without proper security measures could expose the Company to significant risks, including the threat of burdensome litigation. In 2021, for example, the most popular fertility and period tracking app developer, Flo Health, faced legal action upon claims that the platform shared sensitive health information with third parties, including Google and Facebook, without the users' consent.[30]

---

[25] https://pirg.org/articles/do-you-know-where-your-data-is-because-facebook-doesnt/

[26] https://www.business.com/articles/how-to-apply-data-minimization/

[27] https://tinyurl.com/4npba7a6 (Apple); https://tinyurl.com/2p8er5r2 (PayPal)

[28] https://tinyurl.com/2p92fr8t

[29] https://www.securitymagazine.com/articles/98414-privacy-and-data-protection-in-the-wake-of-dobbs

[30] https://tinyurl.com/2sduk56f

Finally, most companies doing business in California, Virginia and the European Union are also required to provide consumers with "deletion rights," as contemplated by the Proposal.[31] Deletion rights generally grant consumers the ability to have personal information erased in instances where the business is not required to maintain the data. Implementing a sustainable data deletion program can help Walmart reinforce its standards and governance for data deletion, meet regulatory requirements, reduce the risk of data breaches, and improve data hygiene overall.[32]

Since Walmart already complies with data deletion requirements under California and Virginia law, applying deletion rights or other related data deletion mechanisms nationwide could be a feasible and cost-effective mitigation measure to the problems raised identified in the Proposal. Mastercard provides deletion rights to consumers nationwide.[33] Synalab Group, an international health services provider, automatically deletes or anonymizes a website visitor's IP address from the company data logs, while other remaining website-visitor data "is stored for a limited period of time" with the explicit purpose of improving the "operation of [Synalab's] website."[34] DaVita, a leading healthcare provider, gives consumers the opportunity to "amend or delete" information collected from them through the company's online platforms.[35]

The requested report would advise investors whether the foregoing data security and protection measures could indeed provide benefits to Walmart. The report would also assess whether consumers' trust in the Company could be increased by enhancing or adding new privacy safeguards, which, in consultation with reproductive rights and civil liberties organizations, may include:

- Establishing a robust policy of challenging overbroad or vague government data requests;
- Providing user-friendly and easy-to-read privacy guidelines (e.g., infographics, disclosure banners, privacy policy outlines);
- Implementing a default policy of, whenever legally permissible, notifying users whose data is requested by law enforcement; and,
- Publishing periodic transparency reporting on data privacy and government data request, with special attention to issues related to reproductive rights.

[31] https://tinyurl.com/mryrf3jc (CA); https://tinyurl.com/53s7zn5t (VA); https://tinyurl.com/3w7mek6x (E.U.)

[32] https://www.grantthornton.com/insights/articles/advisory/2020/how-data-deletion-empowers-data-protection

[33] https://tinyurl.com/yck8twbp

[34] https://www.synlab.com/privacy-policy

[35] https://www.davita.com/privacy-policy

5. Production of the requested report would be cost-effective and a good use of resources.

In opposing the Proposal, the Company notes that staff resources would be better used on "upholding and enhancing its robust processes and responding to requests than in preparing the requested report." We wholeheartedly disagree with this statement.

The requested report would provide an opportunity for Walmart to fully consider the risks of becoming a target of abortion-related law enforcement requests so that it may mitigate future controversies and increase investors' trust in the Company. The scope of research involved in the production of the report is narrow and limited to the risks associated with the Company's fulfillment of information requests relating to Walmart customers for the enforcement of state laws criminalizing abortion access. Furthermore, production of the requested report would be cost-effective and feasible. Interpublic Group Companies recently conducted an assessment of its reproductive health data with respect to state laws criminalizing abortion,[36] showing that the type of analysis contemplated by this Proposal could be done. As such, we believe that the requested report could be produced by current Walmart staff in consultation with outside experts and groups, thus satisfying this Proposal without incurring substantial cost.

In sum, we believe that implementing the requested report will help ensure that Walmart does more to monitor its data handling practices, reducing consumer exposure to serious risks stemming from abortion-related criminal prosecutions. Failure to do so may erode shareholder value by diminishing the Company's reputation, consumer loyalty, brand, and values.

Vote "Yes" on Shareholder Proposal No. 10.

For questions, please contact molly@cleanyield.com.

The foregoing information should not be construed as investment advice.

[36] https://tinyurl.com/mvrmfj2x

ADDENDUM A:

Examples of harms from companies sharing reproductive health-related data with third parties without consumer consent

Aaron Sanderford, ***Facebook data used to prosecute Nebraska mother, daughter after alleged abortion*****,** Nebraska Examiner (Aug. 10, 2022), https://tinyurl.com/2etavr8t

> In 2022, Meta complied with a data request from a local Nebraska police department for private Facebook messages between a mother and daughter, who were both subsequently charged with felony crimes related to the alleged illegal termination of the daughter's pregnancy.

Cynthia Conti-Cook, ***Surveilling the Digital Abortion Diary,*** University of Baltimore Law Review (Oct. 2020), https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2/

> In 2017, a woman in Mississippi experienced an at-home pregnancy loss. A grand jury later indicted her for second-degree murder, based in part on her online search history, which recorded that she had looked up how to induce a miscarriage.

Drew Harwell, ***Is your pregnancy app sharing your intimate data with your boss?****,* The Washington Post (Apr. 10, 2019), https://tinyurl.com/57mrfs3n

> A 2019 report revealed that pregnancy app Ovia Health sold user health data to their employers, without user consent.

Patel v State of Indiana**, 60 N.E.3d 1041 (Ind. App. 2016),** https://tinyurl.com/yc6v27f9

> In 2013, a woman was sentenced to twenty years in Indiana prison for "neglect of a dependent and feticide" after taking abortion pills she purchased online. Evidence presented against her at trial included online research she conducted, the email confirmation she received from an online mail order pharmacy, and unencrypted text messages to a friend about her relationship, becoming pregnant, and the abortion medication she purchased.

Shoshana Wodinsky & Kyle Barr, ***These Companies Know When You're Pregnant—And They're Not Keeping It Secret***, Gizmodo (Jul. 30, 2022), https://tinyurl.com/mthv8jzc

In 2022, *Gizmodo* identified 32 brokers selling data on 2.9 billion profiles of U.S. residents pegged as "actively pregnant" or "shopping for maternity products."

Jennifer Gollan, ***Websites Selling Abortion Pills Are Sharing Sensitive Data With Google,*** ProPublica (Jan. 18, 2023), https://tinyurl.com/3ty8cb45

A 2023 investigation by *ProPublica* found online pharmacies that sell abortion medication such as mifepristone and misoprostol are sharing sensitive data, including users' web addresses, relative location, and search data, with Google and other third-party sites — which allows the data to be recoverable through law-enforcement requests.

Federal Trade Commission v Kochava, Inc. (Aug. 29, 2022), https://tinyurl.com/ywbffb4b

In 2022, the Federal Trade Commission sued Kochava – a data analysis platform primarily used by companies for marketing purposes – for selling data that tracks people at reproductive health clinics, places of worship, and other sensitive locations.

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, E-MAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY. PROXY CARDS WILL NOT BE ACCEPTED. PLEASE DO NOT SEND YOUR PROXY TO CLEAN YIELD ASSET MANAGEMENT. TO VOTE YOUR PROXY, PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.