**Estrangement from the familiar:**

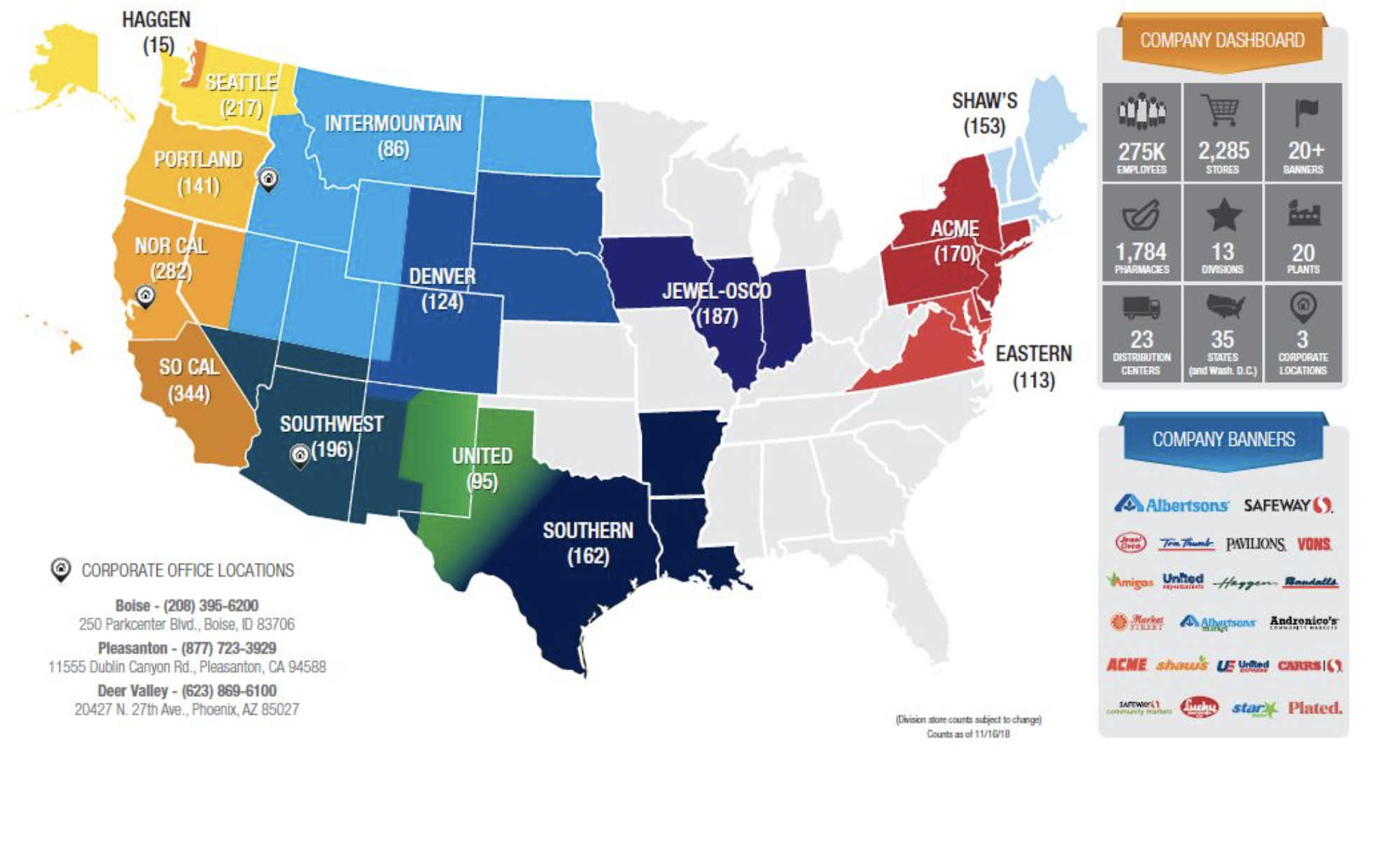
**Privacy Policy Assignment for Albertsons**

[**https://www.albertsonscompanies.com/about-us/our-policies/privacy-policy.html**](https://www.albertsonscompanies.com/about-us/our-policies/privacy-policy.html)

**W231 | David Linnard Wheeler | 9.20.2020**

Most of us purchase the necessities of life. We buy food, drinks, cosmetics, drugs, and other personal items from virtual and brick and mortar businesses. These transactions are an universal part of life for most of us in developed countries. They seem domestic, mundane and trivial. They are, it seems, of no apparent consequence. Is this intuition true, or is there more at stake than meets the eye when we engage in these daily transactions?

To answer this question let’s focus on a paragon of the neighborhood grocer: Albertsons Companies, Inc. and its subsidiaries and affiliated entities. With supermarkets, pharmacies, hardware stores, and gas stations in over 2,000 locations, Albertsons Cos. operates retail stores in 35 states (Albertsons Cos., 2018) (**Figure 1**). They are, therefore, in a position to collect personal data from a large proportion of the US population. Should Albertsons Cos.’ patrons be concerned?



**Figure 1.** Distribution of Albertsons Cos. in the United States.

From first glance it seems as though us customers need not be concerned. While personal information of the type shown in **figure 2** is collected, it can’t be the source of concern since every other retailer is collecting the same data, right?

A picture containing diagram, text

Description automatically generated

**Figure 2.** Albertsons Cos. collects a diversity of data from custumers in person, online, and over the phone.

Indeed, this was the reaction of the three users from UserTesting. Personal information is “collected to improve the [customer] experience”, said one of the users who captured the attitude of the others. This potentially wide scale data collection must be harmless. After all, most of us are populating these databases weekly without consequence. This reaction, however, fails to consider unanticipated future events, like the time when Target *predicted* the pregnancy of a patron before her father (Duhigg, 2012). This is the “problem with induction” (Hume, 1779). That which happened before need not happen again - the past need not predict the future. Just because overt breaches of privacy have not yet occurred, it does not follow that they will not occur.

To rigorously address the sources and risks of harm, the Privacy Policy for Albertsons Cos. Iis analysed below. Questions about the collection, use, and risks of harms are addressed through conceptions of privacy presented by Solove (2006), Nissenbaum (2011), and Mulligan et al. (2016). For contrast, Albertsons Cos. Privacy Policy will be compared with those from the California Online Privacy Protection Act of 2003 (CalOPPA) and the Federal Trade Commission (FTC). Ultimately, I will argue that potential risks of harm are introduced during the data collection, use, and sharing phases of Albertsons Cos. pipeline.

**What data does Albertsons Companies collect?**

Patrons interface with Albertsons Cos. in-person, virtually, and or over the phone. When patrons purchase an item(s) or use any of the available online services (e.g. customer loyalty programs) or mobile applications, consent for Albertsons to collect and use personal information is implicitly granted. In Nissenbaum’s (2011) and Mulligan et al.’s (2016) language, *subjects* automatically opt-in. Their personal information, the *target* of privacy, is now ripe for picking. These *fruit*, however, are not without their blemishes.

One issue with this model of consent, where users automatically opt-in and *mechanisms* to opt-out are not clearly available, is that customers, at least the three I surveyed with UserTesting plus myself, fail to recognize that they automatically opted-in. They think, even after reading the Albertsons Cos. Privacy Policy, that they consented, by clicking a button or signing a form (**supplemental document 1**). Albertsons Cos. could perhaps take a lesson from the FTC and provide simplified choices, at least *a* choice, to customers.

Further, rights for recourse, erasure, to object, to access information held by data brokers, or to not be tracked (recommended by FTC and the CalOPPA), are nowhere to be found. To confirm or refute the ability to opt-out or remove data I contacted a representative from Albertsons Cos. She informed me that patrons in Nevada and California are able to opt-out of data collection, but the rest of us must implicitly opt-in to use the desired services or “reach out to the privacy office”. To remedy this issue and improve transparency, another principle recommended by the FTC, Albertsons Cos. should consider a simple but transparent policy that enables users to understand the collection, use, and sharing practices.

Once consent is implicitly granted Albertsons Cos. passively and actively collects a diversity of data from subjects above the age of 13. Surveillance, as conceived by Solove (2006), begins. The scope of the personal data that is collected is wide and deep. It includes, to use Nissenbaum’s language, a diversity of *attributes*. As such, Albertsons Cos. broadly defines personal information as “any information that can be directly associated with, or used to identify, a specific person”. This conception also aligns with the Organization for Economic Co-operation and Development guidelines (OECD, 2013).

With such a broad realization of personal information, Albertsons Cos. can collect information on everything from our personal location, contact information, food, fuel and drug purchase history to devices we use to interface with their services. Moreover, the depth of this personal data is penetrating and includes, but is not limited to contact information, addresses, date of birth, demographic information, social security number, financial information, employment history, purchase history, food and drink tastes and preferences, prescription drug use history, health-related information from patrons, doctors or insurance companies, and “any other information you choose to provide”.

On top of this rich collection of features with which to predict our spending habits/behaviors, Albertsons Cos. passively collects locational, navigational (e.g. browser type, history, IP address, and sites from and to which subjects navigate, time stamps, etc.), transactional, device, and video and audio data. In other words, Albertsons Cos, knows where we live; our names and sensitive identification details; what we look and sound like; our financial information and behaviors; what and how much we eat, drink, use healthcare products and prescription drugs’ our medical history; driving habits and locations; what types of devices we have, and how we interface with their services on the internet.

This seems like a lot of information.

Moreover, additional data is collected over time as Albertsons Cos. solicits purchases with coupons. One can argue that this constitutes a passive version of Solove’s interrogation, where information is recovered through *coercion*. One can imagine: “Here is a coupon for your favorite and most expensive guilty pleasure food. Use it, and give us more data.”

The complement set of data - the data they do not collect - is harder to define. To use the language from the FTC principles, Albertsons Cos. is not exactly *transparent.* Starting with the individual, they do not know anything directly about patrons under 13, however; they can certainly infer some of this information from their parents. For those patrons who shop at other retailers, they may not know exactly which products they prefer, since these patrons presumably shop at specific retailers for specific products. Moreover, Albertsons Cos.’ collection of personal data may be *contaminated* by patrons who shop for others. Examples of other personal information are abound. Some seem sensitive, some not. For example, Albertsons Cos. does not necessarily know any explicit information about our mental abilities/disabilities (although they could infer some details); they likely do not possess comprehensive DNA sequence data for most or all patrons; they do not know the exact length of my right big toe nail, etc. In short, while they do not know everything, they certainly seem to know enough to introduce risks to users.

In practice, I imagine that, while Albertsons Cos. can collect a wide diversity of data from their patrons, they probably experience customer attrition and, as a result, possess mostly high-dimensional but sparse databases. Lots of NAs. In short, I expect that the distribution of complete records in Albertsons Cos. databases is poisson-like. That is, I expect that, for most customers, they possess some but not all possible data and, for fewer and fewer customers, possess more and more data. To confirm or refute this expectation, I contacted Albertsons Cos. I await their response.

As we saw above, a potentially vast and rich amount of data can be collected by Albertsons Cos. Big databases, however, does not always mean that the entity in question is using the data for something beyond the expectations of the users. To paraphrase Metcalf and Crawford (2016), it’s not what you got, but how you use it that counts.

**How does Albertsons Companies use personal data from customers?**

Albertsons Cos. uses its patrons personal information “for a variety of business purposes”. After reviewing their Privacy Policy several times, I am struck by the scope but mostly by the ability of the framers to flip the valence of what otherwise appears to be potentially exploitative use cases. The policy is readable, as recommended by CalOPPA. However, through some impressive rhetorical sleights of hand and framing bias, the authors of Albertsons Cos.’ Privacy Policy frame the uses of personal information through the lens of beneficence- to maximize benefits and minimize harm to us, it’s customers. In some cases, their “customer first” facade seems to be aligned with their actual business operations. In other cases, we are left to assume the worst.

For example, Albertsons Cos. uses customer data for what seem like harmless, helpful, or even mundane services: provide customer services, process orders and job applications, share coupons, validate identification (which, although mostly positive, can limit customers’ request for anonymity), and alert customers about product safety. These use cases seem typical but, as cautioned above, sometimes innocuous data can be aggregated, as described by Solove 2006, in such a way as to reveal sensitive and penetrating information.

Moreover, other uses seem a little more exploitative. For example Albertsons Cos. uses personal information from customers for: market research; aggregation of anonymized information for analytical and statistical purposes; and “[i]mproving our Services such as the way offers are made for our Services based on the purchasing decisions of our customers and improving the interactions visitors have with our Services”. To me, this just sounds like a euphemistic translation of what, in practice, might mean: “we use your data to optimize the efficacy of our marketing campaigns such that, every time we offer you a product, you buy it”. If my intuition is correct, then one candidate *object* of privacy might be the ability to *choose* what we buy without the overbearing and persuasive influence of advertisements.

My interpretation, however, appears to be too critical and unrealistic. The three users from UserTesting were not concerned and more charitable (**supplemental document 1**). They imagined that, under worst-case scenarios, their data would be stolen by hackers, not used by Albertsons Cos. to predict and exploit purchasing behaviors. The object of privacy for them was likely the control over their personal data, wrongful disclosure, or breaches of confidentiality. In other words, they were worried about unrestricted flow or *transmission* of sensitive information to potentially malicious *actors*. We need not invoke hackers, however, to imagine how things can go downhill within the walls of Albertsons Cos. All violations of expected data flow aside, it is very possible that any entity with sufficient resources, such as Albertsons Cos., could build and deploy algorithms that know our preferences *better* than we know them ourselves. Under these conditions, there is no marketing. We would just wait for the Albertsons Cos. to send us our grocery list.

These practices, if implemented, by businesses at scale would not simply represent potential harms from information processing - they could represent intrusions, in the Solovian sense, since customers lives could be interrupted with coercive ads against which they posses no immunity.

Fortunately, we do not yet live in that reality. Moreover, the time between now and then might be longer for Albertsons Cos. than for other companies, considering they do not sell or rent our personal data - they just give it to their subsidiaries, service providers, and legal teams, and when companies merge, to the relevant entities. This practice seems admirable to me and deserves praise for, if nothing more, not selling our data to, for example, health insurance companies who might issue penalties for those of us who drink too much wine or eat too much sugar.

Even if our data does not leave Albertsons Cos., they still have to store and protect it. According to Albertsons Cos. Privacy Policy, they store our data in the “United States and other countries”, some of which may have “different data protection laws” than the resident country of the customer. Moreover, data is passed back and forth, *transmitted*, between countries. One does not need too vivid an imagination to see how this could constitute inappropriate flow of information under draconian conditions. A nightmare for Nissenbaum. Imagine, for example, that you buy something in country A that is illegal in country B. While traveling in country B, the authorities recover a digital receipt - proof that you broke law X, they might say.

Fortunately, Albertsons Cos. protects our personal information with “various physical, electronic, and procedural measures”. They use “encryption when transmitting” our data. While these safeguards are laudable Albertsons Cos. acknowledges that data security systems are not impervious to unwanted visitors and, insofar as we *give* them our data, we “do so at [our] own risk”.

At this point I discussed the collection, use/abuse, transmission, storage, and protection of customer personal data. In most cases, I stoked the pessimistic arguments and smothered the optimistic ones. Returning to the original question and more moderate expectations about the motivations of large corporations like Albertsons Cos., should we actually be concerned?

**Should we be concerned?**

The most salient risk of harm introduced in Albertsons Cos. Privacy Policy is, in my opinion, not the risk of a digital Panopticon for large scale surveillance. Although terrifying and easy to imagine, deeper ethical questions are invoked by the confluence of rich datasets and well trained algorithms. As mentioned above, the risk of algorithms that can predict our behaviors better than ourselves are more pernicious and devastating than simple surveillance.

Although there is no evidence that supports the existence of such algorithms at Albertsons Cos., the absence of evidence is not the evidence of absence. Market forces and the incentive structures of most businesses are pointed towards profits, not necessarily ethics. If technological advancements continue as per usual and ethical boundaries remain porous, it seems likely that algorithms with better and better predictive performance will be deployed throughout commerce.

While Albertsons Cos. does not explicitly discuss such analyses, I doubt they would want to be left in the dust. Moreover, they do not discount such algorithms. This is perhaps a more fundamental problem with this policy. It is nebulous. The vagaries translated, for myself and the users from UserTesting, into a very broad scope. That is, my expectations were broadened and deepened by reading the policy. Thus, the breadth and depth of the data collection and use were alarming.

How can Albertsons Cos.,as a privacy *provider*, resolve this issue?

One solution is to take some lessons for FTC and revisit their design. Rather than confronting users with a wall of text that most won’t read, Albertsons Cos. could dramatically simplify their interface, be more transparent about data use and collection, and integrate privacy into the data lifecycle. Although not good for sales, I think a description of a worst-case scenario of privacy infringement would introduce a healthy dose of sobriety into the *provider* and *subject* relationship.

Clearly, my proposal will not land as intended. After inspecting other privacy policies from similar retailers, like Whole Foods and the National Co+op Grocers, I noticed that most policies share similar structure and content. An exceptional example was Trader Joe’s. They present a humorous page of “Legal Stuff” <https://www.traderjoes.com/privacy-policy> where they state that “we will NEVER sell your personal information”. Such a strategy, where transparency and humor are used as a Trojan horse to motivate customers to read the policy, seems *effective*.

But what does an effective privacy policy even mean? Effective for who? From the analysis above, I learned that, if nothing more, using vague language leaves the details up to the reader. If the reader is skeptical and cynical, like myself, then we impute what might be unlikely harms to fill in the gaps. To resolve this issue, I again propose that Albertsons Cos. and similar entities are transparent about how they collect, use, store, and protect data. Since, most or all policies are likely not perfect, lets just be honest, try our best, and update our policies to satisfy all parties.

**References**

1. Albertsons, 2018: <https://bis.onenetwork.com/web/albertsons>
2. Duhigg, C. 2012. <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&ref=charlesduhigg>
3. Hume, D. 1779. An enquiry concerning human understanding. In D. Hume, Essays and treatises on several subjects, Vol. 2. Containing An enquiry concerning human understanding, A dissertation on the passions, An enquiry concerning the principles of morals, and The natural history of religion (p. 3–212). Unknown Publisher. <https://doi.org/10.1037/11713-001>
4. Metcalf J. And Crawford K. 2016. Where are the human subjects in Big Data research? The emerging ethics divide. Big Data and Society. Doi:
5. Mulligan, Deirdre K., Koopman, Colin and Doty, Nick (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of The Royal Society A: Mathematical Physical and Engineering Sciences*, 374(2083):20160118 (December 2016). <http://doi.org/10.1098/rsta.2016.0118>
6. Nissenbaum, Helen F. (2011). A Contextual Approach to Privacy Online. *Daedalus* 140:4 (Fall 2011), 32-48. <https://ssrn.com/abstract=2567042>
7. Organization for Economic Co-operation and Development. 2013. <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>
8. Solove, Daniel J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review,* 154:3 (January 2006), p. 477. <https://ssrn.com/abstract=667622>