**EMCS2210: Privacy and Personal Data Protection**

Assignment: Privacy Policy & Terms of Use

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

PAX Privacy Policy : <https://www.paxvapor.com/privacy-policy/>

In the sections below I will note if the PAX privacy policy meets the basic requirements of each of the applicable laws and make some observations about how the policy can be improved. At the end of this paper, I will give a more in-depth assessment and highlight the major changes I recommend as a part of my analysis.

FTC Act

The PAX Privacy Policy does not make any direct reference to the FTC Act, but it does check many of the FTC Act’s Privacy Mandates ( mainly the ones that overlap with GDPR ).

The FTC summarizes its Privacy and Security regulations with these commonsensical statements ( not the complete list ) :

* Don’t collect personal information you don’t need.
* Hold on to information only as long as you have a legitimate business need.
* Don’t use personal information when it’s not necessary.
* Restrict access to sensitive data.
* Limit administrative access.
* Store passwords securely.
* Guard against brute force attacks.
* Protect against authentication bypass.
* Keep sensitive information secure throughout its lifecycle.

Since the FTC Act is wide ranging I don’t expect the PAX Privacy Policy to address the law point by point, however, it seems there are some pretty important high-level issues it should address that it does not. The policy is so spare it only seems to address the basic parts of GDPR. There is no mention of how long data is kept, the steps that the company takes to ensure that access to sensitive data is restricted or standards as it relates to encryption. While I don’t a security roadmap in the privacy policy, the policy should relate to the user the company’s standards, and not if a generalized “we are doing our best” way but in a here are the types of things you can expect from us as it related to XYZ way. There is some of that, but it just feels incomplete when you compare it to this partial FTC summarization.

CalOPPA

To be considered in compliance with CalOPPA, the website’s privacy policy must contain the following:

* A list of the categories of personally identifiable information the operator collects;
* A list of the categories of third parties with whom the operator may share such personally identifiable information;
* A description of the process (if any) by which the consumer can review and request changes to his or her personally identifiable information as collected by the operator;
* A description of the process by which the operator notifies consumers of material changes to the operator’s privacy policy; and
* The effective date of the privacy policy.

This is a pretty low bar, nevertheless, the PAX Privacy Policy meets all these requirements.

ADA

The PAX privacy policy does not directly address ADA at all.

TCPA

The PAX privacy policy does not directly address TCPA at all.

CCPA

To be considered in compliance with CCPA, the company must::

* Implement processes to obtain parental or guardian consent for minors under 13 years and the affirmative consent of minors between 13 and 16 years to data sharing for purposes (Cal. Civ. Code §1798.120(d)).
* “Right to Say No to Sale of Personal Information” link on the home page of the website of the business, that will direct users to a web page enabling them, or someone they authorize, to opt out of the sale of the resident’s personal information (Cal. Civ. Code §1798.102).
* Designate methods for submitting data access requests, including, at a minimum, a toll-free telephone number (Cal. Civ. Code §1798.130(a)).
* Update privacy policies with newly required information, including a description of California residents' rights (Cal. Civ. Code §1798.135(a)(2)).
* Avoid requesting opt-in consent for 12 months after a California resident opts out (Cal. Civ. Code §1798.135(a)(5)).

The PAX privacy policy addresses the collection of data from minors.

There is no “Right to Say No to Sale of Personal Information” link on the homepage. There is no disclosure on whether on not PAX sells User’s Personal Information to 3rd Parties. However, it does state: “We do not sell any Product Usage Data to third parties for advertising purposes.”

There is no toll-free number to submit data access requests.

The privacy policy makes no mention of the CCPA.

**Assessment**

Overall the PAX Privacy is pretty minimalistic and doesn’t address all of the applicable privacy laws especially the new enacted ones. While there are some laws that like TCPA and ADA that may not apply to PAX, it would be advisable to make it clear in the privacy policy that PAX as a business does not collect any information that is under the domain of these laws.

The PAX privacy policy does not disclose whether or not the company sells private information. This type of disclosure is very important and is probably the biggest gaping hole in the Privacy Policy. While there is a statement about not selling Product Usage Data, there should be a clear intentional statement about whether or not the company sells Personal Data to third parties.

The PAX Privacy policy does not disclose how long we keep Personal Data. Even if the length of time that we keep Personal Data is forever, we should disclose that. It would be advisable that the Privacy Policy set forth a timeframe for keeping Personal Data along with a description of the practices used to destroy personal data after the prescribed timeframe has expired.

**Conclusion**

The PAX Privacy Policy should be something that makes users safe and is not overly complicated. While the PAX Privacy policy is easy to read and not overly complicated, when compared to the applicable laws is lacks details. A user reading the policy, trying to find a specific mention CalOPPA will not find it. In my professional opinion, the policy needs to address these laws even if they are deemed inapplicable.