Museum-Partner Observation #3

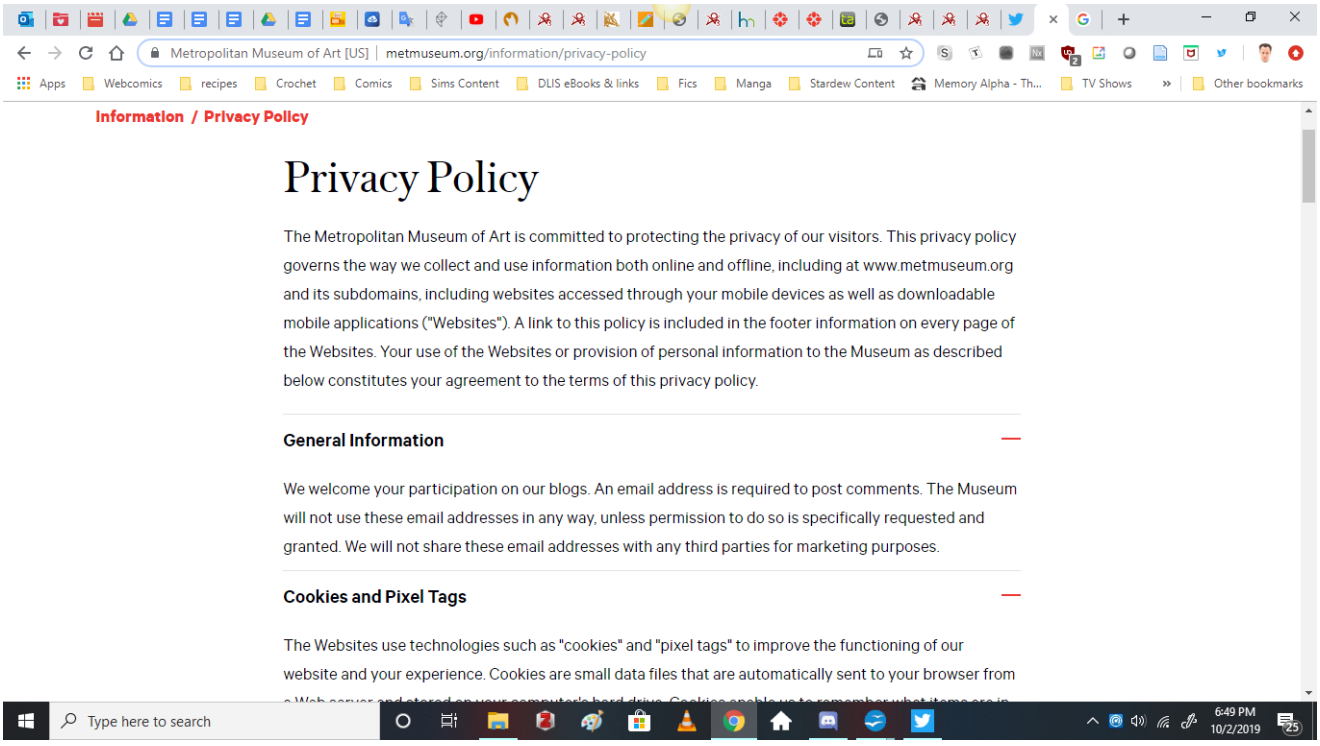
AJ Lent

LIS 258

Dr. Christine Angel

2 October 2019

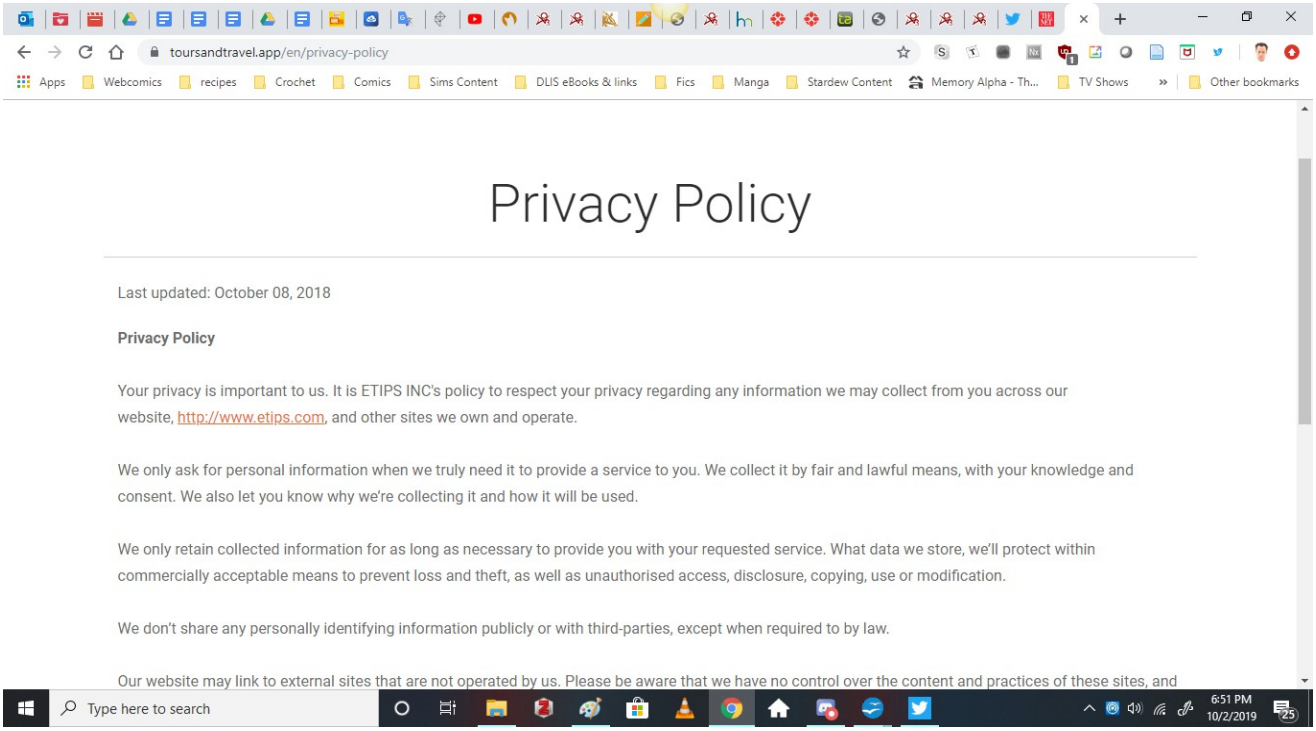
The Metropolitan Museum of Art is a large, internationally known museum, which means it has the funding and ability to have a detailed privacy policy – which it does. The policy is included on the museum's main website and goes into detail concerning each of the ways the museum protects patron information. There is a section for each method of online transaction a patron may have with the museum, as well as one that focuses on how information is collected by the website using tools such as cookies and pixel tags, what third party vendors the museum is affiliated with and the information they send to said vendors, and continuous reference to the fact that patrons can opt out of having their information shared by following instructions provided in emails sent by the museum or, if they are a MET member, through their online preferences.



Screenshot of the MET website's privacy policy page

Not only that, but even through the MET app, data security and privacy concerns are addressed, even if the museum adheres to the privacy policies of the third party affiliates who are connected to the app. For instance, when looking up the MET app in the Apple store, one can click to find a separate

privacy policy that relates to the program used to create the MET app. The MET then adheres to the privacy policies of other websites and social media they work with to allow users to share information about their visits to the museum with their peers.



Screenshot of the ETIPS INC privacy policy for the MET app

When it comes to data security specifically, the MET provides a section of their privacy policy that is completely dedicated to detailing how they protect patron data when performing online transactions. As stated in the NMC Horizon Report (2016), it is extremely important to make sure the personal information of patrons is protected accordingly, or hackers and viruses may obtain important financial details about patrons. For instance, a third party company called Service Systems Associates suffered from a malware that stole such credit card data "from 10 zoos and science centers across the US" (p. 33). While it is convenient for many to use online services to perform transactions, such as purchasing tickets or merchandise, there always comes the risk that vital information could be stolen and used against a patron.

In its privacy policy under the subheading “Data Security”, the MET website provides an explanation as to how the museum works to keep such information safe and secure. The museum uses technology that encrypts visitor information, called Secure Socket Layer (SSL), and keeps its main website and online store VeriSign Secure and GeoTrust Secure, respectively. Both sites are also compliant with the Payment Card Industry Data Security Standard (PCI DSS), further protecting sensitive information from potential virus attacks or leaks (Privacy Policy, 2017). This section makes a point to note that these measures against information loss are within United States law, but may not be up to the standard of the European Union, and that there is a separate disclosure for patrons who make online purchases from the EU (Privacy Policy, 2017).

The most important part of this method of securing data, in my opinion, is that the MET's privacy policy, throughout the different sections, continuously states that credit card information is only stored temporarily in secure servers provided by these third party organizations. The data is used for the purchase and then is no longer stored by the museum, which certainly lowers the risk of said information being available if the servers are compromised somehow. And, as stated before, the MET gives patrons the ability to opt out of having any of their other information shared, such as their name, address, and email address, which allows patrons the freedom to engage with the MET's websites at their level of comfort.

While the MET does not yet have digital pens or similar devices, like the Cooper Hewitt Smithsonian Design Museum (Museum Horizon Report, 2016, p. 32), for the digital resources it does have – social media, the websites, online transactions, and its app – the privacy policy seems adequately equipped to provide data security for the patrons who engage with the museum online. However, the museum will need to begin revising its policy when and if it begins to implement new digital technologies into its organization, rather than simply relying on tools and third party companies that are most useful at keeping someone's credit card information from being stolen after they have

made a purchase of something from the MET's online gift shop.

References

Privacy concerns. (2016). *NMC Horizon Report: 2016 Museum Edition*, pp. 32-33. Retrieved from https://bbprod.stjohns.edu/bbcswebdav/pid-1898521-dt-content-rid-13200640_1/xid-13200640_1

The MET. (July 25, 2017). Privacy policy. Retrieved from https://www.metmuseum.org/information/privacy-policy

Tours and Travel. *(*October 8, 2018). Privacy policy. Retrieved from https://www.toursandtravel.app/en/privacy-policy