What even might actually manage to have more geeks than Comic-Con? PrivacyCon!

Ok, probably not, but on July 21, 2020 the FTC hosted their fifth annual PrivacyCon event, and for the first time it was entirely online. This event is designed to provide researched information on various important privacy topics. The FTC curates the event content based on submitted materials and moderates each session. This year’s topics were (1) health apps, (2) artificial intelligence, (3) Internet of Things devices, (4) privacy and security of specific technologies such as digital cameras and virtual assistants, (5) international privacy, and (6) miscellaneous privacy and security issues.

If you have the time, you’re able to view all six sessions and the opening and closing remarks from the FTC here.

Recognizing you might not, we’ve highlighted some key takeaways below. As you’ll quickly see, these topics are intense, complicated, and everywhere in our world.
these days. The issues that were discussed at PrivacyCon raise questions about potential new privacy and security laws and present compliance and risk considerations when implementing current laws and requirements. Overall, these are important discussions as technological uses of personal information continue to grow.

**Sharing is Caring**

Looking for solutions to the technical complications of getting medical records in electronic format, one study looked at the ability for apps to make obtaining, reviewing, and sharing medical records much easier. This arises from recent guidance from the Secretary of Health and Human Services that mandates an API to allow for such sharing. This is an important, albeit complex, step towards giving people access to their personal information in a digital age, and hopefully in turn better healthcare. That said, it leaves open questions on evenly implementing this technology and with any new technology comes questions on the security of the underlying personal information.

**AI Has Real Life Implications**

An entire session at the event was focused on bias in the use of AI. The bias that may occur in the eventual processing of personal information originates in the underlying formatting, training, and considerations built into the AI. It’s amazing how much data like a zip code can accidentally – or from a more cynical perspective, purposefully – impact the decisions made about an individual based on their personal information. One example demonstrated how people might not get the appropriate healthcare options provided to them by a healthcare provider by virtue of biases that were in AI programs that yielded discriminatory results due to the impact of a few data points. Yikes.

**The Walls Have Ears**

The session on cameras and smart speakers looked at how it isn’t that hard for unassuming individuals to have their voice recordings captured and used without their understanding due to arguable gaps in the review and approval process for 3rd party apps on these technologies. Voice-recordings are a hot topic right now as more and more interactions with technology can occur by voice command. While we once may have felt ridiculous talking to our car, TV, small inanimate object sitting on a table, etc., it’s now the easy way to get the music to stop, or to call a friend, or to recite a text message explaining a health problem.....ok that quickly became quite personal! Moreover, these issues align with many definitions of biometric information, raising questions on implications of such practices for BIPA and other current laws.

**Labelling Privacy**

The complexities of privacy notices aren’t new. The balance between transparency and meeting layered and detailed legal requirements is intense. This can result in companies really trying, but struggling to provide concise and comprehensible
information in an easily accessible location. Recognizing this gap in user approachability, one creative research project proposed privacy and security labels for products. Just like you can pick up a food item and see what percent of fat it has, you now could look at privacy uses and information at a glance. This wouldn’t replace privacy notices, but would provide a digestible amount of information that might also force entities to be more transparent in a concise fashion. We have to say, this really demonstrates thinking outside the box.

**Options for Presenting Options**

The GDPR and e-Privacy Directive create requirements to provide users with options to opt-in to the use of cookies, and otherwise to manage their cookie preferences. While the focus here is the EU, the fact is that cookie consent tools have become commonplace in many jurisdictions around the world. In the US there has been discussion on whether something similar to cookie consent tools might be used for providing consumers with choices they have under current (i.e., CCPA) and future US privacy laws. Sticking their hand in the cookie jar, one study looked at the factors that impact the success and engagement of users with these notices. Whether a banner, a pop-up that will go away after a certain time or when a user clicks elsewhere on the screen, a box that blocks the whole screen, or a variation on these themes, there’s a lot of formatting options. Mix in factors such as the intuition of individuals who read from left-to-right or vice versa to gravitate towards one side of the page with their eyes and focus, and you get some interesting considerations for placement and formatting. As companies continue to look at how to best meet legal requirements this type of analysis may become important to optimize practices.

**(Un)securely Buy that Sweater**

Looking to go online shopping? You might not want to after learning that one study determined that there was a massive gap between examined commitments to the Payment Card Industry Data Security Standards (PCI-DSS) and actual practices. This is despite PCI scanners being used to assess compliance by an outside vendor. In fact, NONE of the six scanners that were evaluated were compliant, meaning the tools used to determine compliance are themselves a problem. Because PCI-DSS is an industry standard and not a law, this may lead to questions on whether reliance on this long-standing practice is sufficient, and the research outright suggested doing away with the standards due to their ineffectiveness.

© Copyright 2020 Squire Patton Boggs (US) LLP

National Law Review, Volume X, Number 211

**Source URL:** [https://www.natlawreview.com/article/key-takeaways-ftc-s-privacycon](https://www.natlawreview.com/article/key-takeaways-ftc-s-privacycon)