Online Tracking and Cookies
Investigators and IRBs may want to consider adding language to informed consents to describe online tracking and cookies. The web includes elements that may not be evident to the average user, such as tracking cookies or web beacons. Connections between a site visited and third party services are not always obvious (e.g., as a user moves from one site to another, third parties may “watch” the activity to collect marketing research important to their clients’ business). In fact, some people may be unaware that many third-party sites sometimes have the ability to monitor and track our activity on the sites we visit. This is rarely transparent to users, despite the fact that it may carry privacy risks to them. The challenge is how to communicate this to participants, many of whom will lack understanding of how relationships among various online sites work. It is important to explain those risks as clearly as possible to research participants. (To learn more, watch former Mozilla CEO Gary Kovacs’s TED talk about exposing online tracking).

When browsing the web, the browser retains certain pieces of information, such as a history of the sites visited (also known as ‘tracking’). Tracking is often accomplished with “cookies,” small files that are stored on the user’s computer and hold a modest amount of data specific to a particular website and the device used to access it. These files can be accessed either by that online service or that device itself. Cookies allow the online service to deliver an experience to a particular user (e.g., remembering the kinds of books or music a user enjoys), or enable a site to sustain information from one visit or site to the next (e.g., maintaining a ‘shopping cart’ for items previously put in that cart, but not yet purchased). ¹

Some cookies are temporary only, and are deleted when the browser is closed. These “session cookies” are commonly used to keep a user logged in to their online account as s/he navigates within the site. Other cookies persist indefinitely and may track the user’s browsing behavior across sites or provide customization, such as remembering preferred page layout on a particular site. Familiar experiences based on persistent cookies include websites welcoming users back by name or sites displaying advertisements drawn from other sites visited. ²

Investigators and IRBs should consider privacy risks created by tracking technologies and recommend suitable privacy safeguards before directing participants to online research data collection sites. Such safeguards may include browser privacy settings or comprehensive anonymization mechanisms. ³ [https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2012/6/No-need-of-informed-consent-for-authentication-and-session-ID-cookies/]

Most web browsers offer privacy settings designed to enable “Do Not Track” and/or “Private Browsing”. Such settings will not make the participant entirely anonymous, however, as their Internet service provider (ISP), employer network, or the individual websites themselves can still track what pages that they visit.

Below is a model statement investigators may adapt to describe online tracking and cookies for web interactions.

Sample: Online Tracking

Although every reasonable effort has been taken, privacy and anonymity during Internet interactions cannot be guaranteed. It is possible that additional information beyond that collected for research purposes may be captured and used by others not associated with this study. The web includes elements that are not always evident, including online tracking mechanisms. As you move from one site to another, third parties not involved in this research, may “watch” your online activity, including your visit to our research site. That third party may employ security and privacy policies different than ours, over which we have no control.

<<We can provide some recommended tools and practices to prevent online tracking mechanisms and improve your online privacy. For practices, first check your web browser’s privacy settings to enable “Do Not Track” and/or “Private Browsing.” Please note such settings will not make you entirely anonymous however as your Internet Service Provider (ISP) or employer network can still track what pages you visit. For tools, we recommend XYZ>> (Only include this sentence if you or your institution has tools and practices to share with the research participant. For recommendations on how to improve online privacy go to: privacyrights.org/online-privacy-using-internet-safely).