



Society for Computers & Law
The leading educational charity
for the tech law community
www.scl.org

SCL Tea & Tech: "Staying Away from the Cookie Jar"

Simon Forrester was the guest speaker at this week's Tea & Tech session and gave a fascinating overview of cookies, how they track website users and the issue arising in trying to create a "cookie-less" website. He was asked by SCL to create the [Remote Courts website](#) without cookies.

The issue is very topical in light of the EU's proposed E-Privacy Regulation as well as recent [EDPB guidance on cookie walls and consent under the GDPR](#), as well as [ISBA/DMA guidance on privacy within programmatic advertising](#).

Why you need to stay away from the cookie jar

Simon pointed out that cookies can be very useful, e.g. in relation to log-in mechanisms. However, once you use cookies, you need to be concerned about regulation and privacy statements.

Using Google incognito mode, he gave a demonstration of where cookies "hide" by showing people how they appear in the developer tools in Google Chrome, which shows the separate elements of a website. Cookies come in two forms – permanent cookies which stay on your computer and session cookies which, as the name suggests, are just for that session and expire quickly.

Simon explained that websites are "stateless", so each page of a website has to give a request and cookies give the website "state" and allows them to adapt to the user. Websites do not all sit on the same server, a website may link to items such as Google fonts or images, so cookies are also served from other websites. Websites are effectively decentralised – and advertisements come from (lots of) other servers.

Simon used his local newspaper website as an example. It has its own cookies but because it has so much advertising the cookie section of the developer tools soon filled up with third party cookies and Simon pointed out that every single one of these cookies will track the user. He then went to the Halfords website and the same cookie reference came up and so the organisation serving the cookie knew in which county he lived from the newspaper site and that he had visited the Halfords website. In addition, a Twitter cookie was served called "personalised ID" which tracked Simon to an even greater extent. Simon said cookies know exactly what you are doing.

Simon also expressed the opinion that cookies have changed from being something useful to being something dangerous, with thousands tracking each individual for the sake of advertising revenue.

Remote courts

Simon was tasked with creating the Remote courts website without using cookies. This proved to be surprisingly difficult and he had to take the following steps:

- Tell the server not to issue session cookies

www.scl.org



Society for Computers & Law
The leading educational charity
for the tech law community
www.scl.org

- Host everything locally including fonts, pictures/images, icons etc. Simon built a caching system for images, so they were held locally and no cookies were served.
- Statistics – cookies are usually used to collect statistics eg to find out what the most popular pages on a website are.

Effectively every piece of content you link to serves a cookie, so you have to ensure that everything is locally held. The website was eventually created in such a way that it only needed to ask about cookies when people came to register and log in.

Questions

There were some questions about whether there were tools you could use to combat the tracking – Ccleaner and Malwarebytes were mentioned with the latter being more effective.

There were also questions about cross-device tracking where cookies are shared between devices. However, Simon pointed out that when you eg sync your devices you are effectively doing the tracker's work for them.

Some apps do not pass on data, but others do, if they are stand-alone they usually do not but if they work within a browser they will.

Cookies will collect any data, including keystrokes. However, they cannot pass that data onto other websites, key stroke data can only be used by the domain which issued the cookie concerned.

IP addresses can be used to track people but because they are created at router level, not person level, they are not as specific as cookies which are shared between a person's devices. Also, for most people a new IP address is generated every time they reboot their router.

Pixels can track people - everything on a website can serve its own cookies.

Simon mentioned that Firefox is the best mainstream browser to stop cookies, although Tor will stop them all. However, if you do not allow any cookies at all, websites will just not work, and it is very difficult to stop third party cookies talking to each other.