Saal:	17:15	01:00	Day: 1	Track: Security & Hacking	nA
Simulacron-3					

Title: **Privacy Badger**

Subtitle: Stop being tracked online

Speaker: **Noah Swartz, Cooper Quintin**

Short: *In this talk EFF Technologist Noah Swartz will present Privacy Badger, EFF's new browser extension that automatically blocks both invisible trackers and spying ads. It is intended to be a minimal or zero-configuration option that most Internet users can use to prevent non-consensual third party collection of their reading habits from their everyday browser. Privacy Badger couples the recently developed HTTP Do Not Track opt-out header with a number of heuristics for classifying the behavior of third parties, to automatically determine which should be blocked, which are needed but should have cookies blocked, and which are safe from a privacy perspective. They will also talk about the current state of non-consensual tracking on the web, what methods are currently being used to track people and exploring what alternatives we can pursue.*

Long: In this presentation I will address the state of online tracking. I will discuss the prevalence of tracking online, describe who is participating in it, explain the adverse effects for common web users, and then discuss what can be done to protect yourself from being tracked. Websites have long ceased to be simple static html pages, and are now made up of many different resources distributed across the web. Over the course of a day of browsing the web, even if the number of sites we visit is small, we often broadcast information about the sites we go to to hundreds of third parties. These third parties have the ability to aggregate information about our browsing across many first party domains, enabling them to track what we read on the web. To many Internet users these third parties are invisible, and just as invisible are the ways in which they can uniquely identify you as you browse. As these forms of tracking become more ubiquitous and as data resellers grow in prevalence users need to have ways to protect themselves and their privacy. In this talk I will cover the technical details of how third parties determine your identity on the web, and how they aggregate that information across websites. I will talk about the implications this has for web users' privacy and security. Additionally I will talk about the legal and policy work that has been done to rein in this sort of tracking. Finally I will discuss the Privacy Badger project, and how it protects users as they browse the web. The talk will cover the following issues in detail: Ways in which advertising companies track users, how spy agencies and other bad actors piggyback on this info, and how to stop them. Specifically IP addresses, 'tracking' cookies, super cookies, and browser fingerprinting. How you can protect yourself from these forms of data collection and how Privacy Badger works. Why other kinds of privacy plug-ins and features fail to protect users from tracking Ways that the EFF is working to rein in browsing tracking through law and policy. After this talk you will be informed about the types of tracking that occur online and feel empowered to do something to protect yourself from it. You will know how to follow future issues and understand current efforts to protect users and shape law.