Product is You

We are living in the information age, but what does that mean from a business stand point? Imagine all the free stuff you use. You play free games on your phone, free e-mail, free social networking, free search… Looking at it, one might wonder if humanity was wrong to ever invent money. The thing is money is still exchanging hands, you just are not paying for it.

Everything you do, leaves a digital footprint. Paying for the snegls at the corner bakery, checking your social media feed, even walking somewhere with your phone in your pocket generates information. This information is worth money. You pay for the free stuff with your information. Then somebody pays the owner of the service to buy that information. This is the world we live in…

Cut in Schneider Video Here

First Party or Third Party Tracking

Every web site, every app, every network you interact with collects information about you. Some of this information may seem innocuous by itself. Perhaps you post Harry Potter fan-fic on a forum, and your interactions on the forum don't seem sensitive.

That is the first party data that the forum has on you. The data a vendor gleans through your interactions with their product. Facebook knows who your friends are, what kinds of stuff you like, and what you read on your feed. Google knows what you search, which sites you visit after, where you go using Google maps. Amazon knows what you bought last summer. These are all first party data.

Then there is the third party data. Very often companies like Facebook or Google will track you across web sites, often as part of their advertisement placement service. Google can even track you walking into a brick and mortar store thanks to the location data from your phones. Thousands of data brokers, advertisers and other trackers lurk in the background of your daily life, secretly collecting data…

Show them cookies: Use Privacy Badger

What They Know

Allude to Das Leben Der Anderen, and government surveillance. Talk about how easy it is now to scale what authoritarian regimes tried to do in the past. GPS tracker, microphone, camera all in one device and the best part is we pay to carry it on our person. Here is the rub though:

With trackers collected from across the web, they don't need to listen to us to spy on us. They already have better information through much more mundane stuff we do.

The traces we leave going about our lives creates an immense accumulation of data points about us. Our browsing history, app usage, purchases, geolocation… Trackers assemble data about our clicks, impressions, taps and movement into behavioral profiles. Behavioral profiles that reveal our political affiliation, religious belief, sexual identity, race, ethnicity, education, income, purchasing habits, physical and mental health…

Show them google assumptions

How do They Know It?

Trackers use identifiers like the software or the devices you use and try to link it to a single person. So your web browser, or your cellphone hardware, or your credit card number may be used to create a profile for a person. Then this profile is used to accumulate all your behavior tracker can see. Things like what you searched for, what you read, where you click… Even if the particular tracker doesn't know your real name it is not hard to trace it to you.

Some of identifiers trackers use like browser cookies are features, others like browser fingerprints or device identifiers are an artifacts of the underlying technology. We will talk more about specific identifiers in a separate module.

The key point here is a tracker uses several identifiers to track you. So even if you change your phone number, it doesn't take long for the tracker to figure out its you using the same iphone with a different number.

Who Is Tracking You?

Ad networks

Each web site or app that serves you apps includes a small snipped of code from the ad network to choose and deliver the ad to you. Each time you visit the web site or open the app, it asks the ad network for an ad, giving away your interactions on the web site.

Often each app or website has multiple ad networks competing for your attention. Therefore your visits may expose you to a larger audience.

Analytics Services

Sometimes the trackers offer data in exchange for your data, as is the case with Google Analytics. The web site owner allows tracker access to your behavior on their site, and in exchange tracker provides insights into who is visiting their web sites.

When an app uses ready made code offered by trackers, the app may end up sharing your data. Sometimes even without realizing it is sharing your data. For example a local chat app that uses Google's location services to match chat partners in your area, is sharing your location with Google. This saves the developer from developing their own location service, in exchange for your data.

Others

There are many others that are tracking you but Ad Networks and Analytics services are the biggest two. Just realize this, when you are served an embedded video, or music on a web site, your information gets shared with the streaming service that hosts the video/music. When you use single sign on to use facebook to log in to anything, your information gets shared with Facebook.

Data Sharing

Most trackers don't have all pieces of information on people they track. That is why they often join forces and share the information with each other.

Real-time Bidding

The web sites often load in a fraction of a second and it is hard to believe that within that fraction, advertisers learn about you loading a web site, hold an auction on who gets to place their add on your web browser, then sending the winning advertisement your way. Yet this is a mundane reality of today's internet.

The add network receives the request for an add from your web browser. Based on the information the network has on you it creates a bid request. The advertisers look at the personal information and make a bid to show advertisement. Add network goes through matching bids such as young female interested in first person shooters and pick the highest bid to serve the add to you. Then you get served the add for Call of Duty MXVII.

The advertisers place bids for their targeted customers: An insurance company may be interested in people looking to buy cars, a make up company may be interested in women with a high purchasing power, a gym may be interested in young professionals in a certain neighborhood for example.

Data Brokers

Who Is Buying?

Targeted Advertisement

Political Campaigns

Debt Collectors

Law Enforcement

Its funny, in US law enforcement's data collection is somewhat limited by law. The corporations are not… So the law enforcement buys the data on the free market.

What GDPR Does?

Informs the user on what is being collected, and what purpose.

Gives the user the option not to allow some cookies.

Regulates how user data is stored and transmitted.