Welcome to Digital Footprints, module two. In this module, we will try to understand how it is that we started leaving such big footprints.
Meet Daniel. He is an avid internet user. He surfs the internet for almost anything. He likes to pay all his bills online. He is always sharing his updates on Facebook, Twitter and other social networking sites.
Is it possible for someone to follow Daniel around in the virtual world of the Internet, tracking his digital footprints, tracing the impressions he leaves?
The answer is “yes.”
Digital footprints are the records and traces we leave behind us as we use the Internet.
Your visits to different service providers generate data about you that piles up at each location. Service providers and other third parties exchange data about customer profiles and transaction statistics. This industry is a massive economic engine powering (and funding) much of the internet...

Over time, the technology to create profiles of Internet users has become increasingly sophisticated. Few users realize how extensive their digital footprints are, or how many third parties make up the complex ecosystem of data sharing and data monetization.
Digital footprints should be a significant privacy concern for Internet users, because they can be used to track user actions and are a basis for “profiling” by online service providers and others.
The explicit footprints we leave as we participate in Internet conversations can be obvious to us, if we pay attention to them.

For instance, if you Tweet that you have just arrived in Sydney and the sunset is spectacular, those are quite explicit disclosures about where you are and when (assuming you’re telling the truth). But what about the implicit footprints?
Each time you visit a web site, you reveal some information about yourself to the owner of the web site: your IP address, which may include your geographic location, your web browser type and operating system, and, often, the last web site you visited. These bits of information seem relatively innocuous and even fairly anonymous. If these are footprints, they are fairly light ones.
In fact, these footprints are “too” light for the purposes of some online service providers.
Internet services such as online commerce, social networking, and web mail require that a web site be able to link up multiple interactions, such as putting a book in a shopping cart, and later clicking “Pay Now”.

They need to know when the person doing something now is the same person who did something previously – and often this is in the user's direct interest, too.
IP addresses won’t do the trick, because several people might be using the same IP address at the same time: something more is required.
One solution to this problem is the cookie. Well, not exactly this type of cookies!
A cookie is one way of tying multiple actions by a single user into one connected stream.

A cookie is an arbitrary string of letters and digits - something without any inherent meaning - that a web site sends to your web browser.

Digital footprints in the form of cookies are used to make the Internet more usable, and can also help make individual transactions more secure.

Transaction security decisions rely on a combination of factors, including cookies. Web developers have settled on cookies as one of the most convenient ways to add persistence and security to your web experience, which is why they are everywhere.

Click the arrow to view an example of a cookie.
Here’s a typical cookie. As you can see, it looks pretty meaningless. But, like any cookie, if you know how to interpret it, it contains useful and valuable data.
Web sites generally set a cookie in your browser at the instant when you first visit the site. The web site can store profile and preference information in the cookie.
Your web browser stores the cookie when requested, and then every time you revisit the web site, the web browser sends the cookie back to the web server. The browser stores the cookie behind the scenes, and then sends the cookie back to the web site every time you click.
One result is that the web site can stitch together your actions to improve your user experience—even if they’re separated by days, weeks, or months. Most users don’t think about it, but by default, their web browsers contain thousands of cookies, placed there by each web site they visit. However, this also means you’re leaving bigger and bigger footprints. Cookies don’t just link up transactions; they enable web sites to keep track of you every time you visit.
If a service provider holds account information for you,...
...such as your email address, payment details, purchase history or other personal information, the cookie can be used to link this information and everything else you subsequently do on that service provider's site.
The concept of linkability is a key one in any analysis of online privacy, because linkability does more than almost anything else to erode users’ ability to keep personal data within a single context, and thus to manage their own privacy.

Incidentally, you can learn more about linkability, contexts and privacy from our Identity and Privacy tutorials.

http://www.internetsociety.org/manage-your-identity
Each individual footprint is small, but when linked they can form a surprisingly complete profile about us. When web sites decide to share this information with each other, it becomes possible to build a profile for you, using raw data such as the web sites you've visited, the products you've bought or searched for, your address, and any other bit of information you've given to any cooperating web site: age, sex, health, marital status, employment, financial information … the list is as long as everything you've ever shared on the Internet.
In fact, it is longer – because based on the raw data, profiling companies make inferences….
......about your habits, preferences, values, aspirations, and even your intentions and future behaviour.
Congratulations! You have completed Digital Footprints module two, Why did we Start Leaving such Big Footprints.

Remember, you can always find more information, whitepapers and other training modules via the Internet Society’s Identity and Privacy pages.