Module Objectives

Each year, we live more of our lives online, and this trend is not going to change. When your only connection to another person or organization is your digital footprint, then your footprint will determine how they see you and treat you. It is important to understand who is examining your footprint, and how you can take charge of where it leads them.

On successfully completing this module, you will be able to:

* **describe your digital footprint and digital trail.**
* **discuss online privacy issues, including privacy protection.**
* **explain how businesses use your digital footprint.**
* **examine a website for safety.**
* **assess online content for authenticity and validity.**
* **discuss the ethics of creating a false online identity.**

Digital Footprints and Digital Trails

Earlier, you googled your name to get some idea of a **digital footprint**. If your search returned any hits, then you began to see what your footprint tells people. The results you found, however, are only a part of your digital footprint (all the information you left behind from interactions with digital environments). Search engines like Bing and Google cannot find all the data you leave behind in the digital environment, though it is all accessible to someone. Consider the following list of typical interactions with the digital environment, and some of the information they can leave behind:

* a post on a Facebook page
* an image texted to friends
* a Google search
* an online purchase
* walking past a security camera on a busy street
* logging in to a website

Below is an example of the trail of digital information one person can leave during a single day. The example shows how rapidly a digital trail can grow. Notice that the **digital trail**, or footprint, can grow without your knowledge or consent.

|  |  |
| --- | --- |
| **7:30** | **Text a friend –** even if you delete the text, it still leaves a digital “print” (and also remains on your friend’s device if they don’t delete it) and could still be accessible and tracked down. |
| **8:15** | **Download an app to your mobile device –** online technologies take note of information like your e-mail address, credit card information and what kind of apps you like. Apps can collect all sorts of information about you, including your location and contacts in your address book.  |
| **8:42** | **Late for soccer game** – call coach to let team know. Cellular phone calls can easily be intercepted; mobile phone technology signals your whereabouts to satellites to deliver calls. |
| **9:11** | **Play a shift in game –** people could be recording videos and taking pictures of your game with their mobile phones. They could post these on their favorite social networking sites, tagging your name. |
| **10:37** | **Send personal e-mail to mom at work –** this can be read by mom’s employer; simple deletion does not erase it from the computer’s hard drive or the company’s network. |
| **10:40** | **Drive car to coffee shop –** your geo-location device plots your route and records your vehicle location at all times. |
| **10:43** | **“Check in” in at coffee shop –** you do this on your favourite social networking site, so all your friends know where you are. Anyone with access to your profile can see where you are (and where you aren’t) and, later, you receive personalized marketing recommendations that are based on that particular location. |
| **10:47** | **Use bank machine at coffee shop –** system records details of transaction, cameras overhead or in machine record your behavior. |
| **10:55** | **Log onto Internet from computer at coffee shop –** Your choice of chat groups and your messages can be monitored and a profile assembled by anyone, including police; some web sites keep track of your visits. Coffee shop could also be monitoring your traffic.  |
| **11:00** | **Post pictures from the party last night on your favourite social networking site –** pictures and comments you post can be accessed long into the future, possibly by future college and job interviewers. If the geo-tagging features are enabled on your device, your photo will be tagged with your location. Anyone who can see your photo – and anyone they share the photo with – will know your location. If they know that location is your house, they will know where you live. |
| **11:30** | **Return some jeans you bought yesterday –** for the return you are required to give your driver’s license for the clerk to scan and to fill out a form that asks for your phone number and home address. |
| **11:53** | **Buy a birthday gift for a friend –** credit card records details of purchase, retailer’s loyalty card profiles purchase for points and directed discounts; banks may use spending patterns to help assemble complete customer profile. |
| **1:00** | **Buy a fast-food meal –** security cameras record your arrival, your debit card purchase is recorded, loyalty card tracks selections for marketing and targeted discounts. |
| **2:12** | **Realize you forgot your mobile phone at fast-food place –** if your device isn’t password-protected anybody could pick it up and gain access to any and all personal information on it. If they choose to text or e-mail from it, they could even pretend to *be* you. |
| **2:32** | **Return to fast-food place –** security cameras record your return.  |
| **4:30** | **Listen to phone messages –** your phone has recorded callers’ phone numbers and displays your number when you call others, unless you enter the code to block the display.  |
| **5:13** | **Accept someone you don’t know that well as a “friend” online –** if you haven’t set up different privacy settings for different lists of friends, you may be giving that person access to a treasure trove of your personal information. |
| **7:30** | **Play a videogame online with some virtual people you have never met –** many types of personal information can be collected through online gaming: everything from names, addresses and credit card information for billing purposes, to email addresses and IP addresses, down to feedback rankings from others, digital images and personalized profiles. |
| **9:05** | **Order some clothing and books online –** company records personal details and credit card number and may sell the information to database-list-makers. Next time you visit that company’s web site you may see ads tailored directly to your interests, based on what you purchased at this visit. |

In our digital world, information seldom just goes away. Data sits on servers and in databases, generally being used, but often simply forgotten until someone looks for information, possibly years later. In this way, a long-forgotten part of a digital footprint can come back to haunt a person in future years. Something that a person posts online today could contribute to their success in finding a job tomorrow, or even lead to them losing their employment years from now. Even posts that you might think are temporary—like a Facebook post you delete after a couple of days, or a Snapchat image that automatically deletes in 10 seconds or less—can be copied or captured in a screenshot by viewers and shared in other ways.

Footprints and Privacy

The information you add to your digital footprint might remain "out there" forever. In this case, "out there" does not even mean that it remains in the same web site or on the same server that first collected it. Personal information may be shared, copied, sold, stolen, altered, used and abused by whoever can access it. In some cases, information like this comes back to haunt people in future years.

When this information can be used to identify you as an individual, or to affect you or the people you care about, it becomes a **privacy** issue. Privacy is a legal concept that is defined by laws. Each country has its own privacy legislation, and there may be significant difference from country to country in how privacy is defined and protected by law.

In Canada, privacy is defined by two federal laws. Read a brief description of each:

**Privacy Act**

Since July 1, 1983, Canada's **Privacy Act** has limited how **federal government departments and agencies** can collect, use and disclose our personal information. The Act gives us the right to access and request corrections to any personal information about us that those organizations might have.

**Personal Information Protection and Electronic Documents Act (PIPEDA)**

The **PIPEDA** sets ground rules for how **private-sector organizations** may collect, use or disclose personal information about us in the course of their commercial activities. The Act gives us the right to access and request corrections to any personal information about us that these organizations might have collected.

In New Brunswick, privacy is defined and protected within **provincial government departments and agencies** by the **Protection of Personal Information Act** and the **Right to Information Act**.

While our privacy is clearly defined, and our laws provide some effective protections for our privacy, they only apply to businesses, organizations and governments within Canada. The difficulty in protecting privacy on the Internet is that the Internet spans countries. If an online business in The United States, Taiwan or Russia collects and uses your private information, who is going to protect you?

The answer is: **You must protect your own privacy!**

Click the following links to visit and explore a few websites that can help you educate yourself about your privacy rights and risks. You can use information you find there to support your comments and thoughts for your next journal entry.

* [**MediaSmarts**](http://mediasmarts.ca/privacy) – This is a good website for developing your general media literacy. You can use it as a starting point to learn about privacy and the Internet.
* [**My Privacy Everyday**](http://www.priv.gc.ca/youth-jeunes/fs-fi/day-quotidien_e.asp) – This scenario is an effective example of how much information one person can add to a personal digital footprint in a single say.
* [**Gaming consoles and personal information: playing with privacy**](http://www.priv.gc.ca/information/pub/gd_gc_201211_e.asp) – An in-depth question-and-answer page about data collected from gamers and its privacy implications.
* [**Canada's Privacy Act**](http://laws-lois.justice.gc.ca/eng/acts/P-21/) – This is the law that defines and protects Canadians' rights to privacy.