IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 7.918 ⁙ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12302

Digital Footprint: An Information Atheneum for Hackers

Palash T. Sole

Department of Computer Engineering, Universal College of Engineering and Research, Pune, India

Abstract: The personal information which we post/share online is called a Digital Footprint. Most of us have a digital footprint over the internet be it knowingly or unknowingly. Technology and our personal information are getting intertwined as we become more and more dependent on technology for everyday activities. With basic information such as names, addresses, and phone numbers; personal information also includes one's demographic location, interests, relationship status, and social media accounts that can be tracked easily. Teenagers nowadays are so engrossed with technology that they spend most of their time on social media. Relationship status, personal images, and videos are shared on an everyday basis. With a such wide variety of personal information being captured and exposed online, private life is not so "private". This study proposes how digital footprints can impact an individual by measuring the discoverability of various types of personal information.

Keywords: OSINT, digital footprint, personal data, technology, cybersecurity, awareness, social media

I. INTRODUCTION

Digital footprint is the data that is left behind when users have been online over the internet. Media, social media posts, and words are the digital footprints that have been shared on the net. It also includes passwords, demographic data, online purchases, and IP addresses associated with one's digital profile.

At times it's not obvious that you are contributing to your digital footprint. For example, many websites can track your online activity by installing cookies on your device, and apps on smartphones can collect your personal data without you knowing it. Organizations can access your information, they could sell or share your data with third parties. Worse still, your personal information could be compromised as part of a data breach.

Whatever we are doing on the internet can leave a trail of information behind us that people can use to determine our likes and dislikes, or for other less condemning purposes such as trying to hack into online accounts or trying to access passwords.

A digital footprint is left every time we:

- Visit a website
- Post to social media
- Buy something online
- Send an email
- Search for something on Google
- Text or message someone
- Stream a movie or TV show
- Etc.

Digital footprints can be both beneficial and detrimental to your privacy. Therefore, to protect yourself from the dangers of a digital footprint, it's important to be aware of the types and take steps to limit or erase them as needed.

Types of Digital Footprints:

Based on how you imprint the digital footprint, it can be categorized into two major types: Active digital footprints and Passive digital footprints.

DOI: 10.17148/IJARCCE.2023.12302

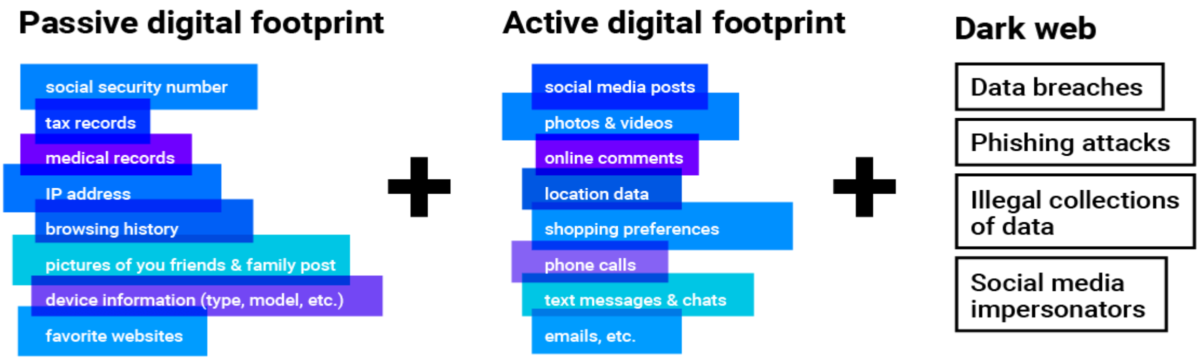
Active Digital Footprints: These footprints are created by you and are more visible. If a user is logged into a website through a registered username or profile, any posts they make form part of their active digital footprint. Other activities that contribute to active digital footprints include completing an online form – such as subscribing to a newsletter – or agreeing to accept cookies on your browser. Some types of active digital footprints can be:

- Social Media Footprints
- Email Footprints
- Blog posts and comments
- Download Files
- Photo and videos footprints
- Online purchases
- Web search footprints

Passive Digital Footprints: A passive footprint would be defined as the unintentional traces that an individual creates on the internet, For example, this occurs when websites collect information about how many times users visit, where they come from, and their IP address. This is a hidden process, which users may not realize is taking place. Other examples of passive footprints include social networking sites and advertisers using your likes, shares, and comments to profile you and target you with specific content, such as:

- IP addresses
- Location data
- Data collected through cookies.
- Surveillance footprints
- Biometric data
- Telecommunication footprint

How Data can be used by Hackers



Why do Digital Footprints matter in the 21st century?

- Digital Footprint determine a person's digital reputation, which is now considered as important as their offline reputation.
- Words and photos which you post online can be misinterpreted or altered, causing unintentional offense.
- Cybercriminals can exploit your digital footprint – using it for purposes such as phishing for account access or creating false identities based on your data.
- Employers can check their potential employees' digital footprints, particularly their social media, before making hiring decisions.

How Hackers use your Digital Footprints:

- **Residence address** - A rogue Wi-Fi access point (AP) can be placed outside of your residence impersonating a legitimate Wi-Fi network. Once your personal devices are connected to the AP, your network traffic can be seen by the hacker.

DOI: 10.17148/IJARCCE.2023.12302

- **Family members' personal information** - Your family members' personal information (for example your mother's name) may be the answer to the security questions. A hacker can use this information together with other information to get access to your account in some cases.

- **Breached Passwords** - A hacker could easily reuse the breached password to gain access to your other accounts.

- **Hobbies** - Your hobbies can be used to tailor a targeted phishing attack scenario to compromise your laptop or even your company's network.

The proliferation of Digital Footprint into Everyday Practice
Behavioral Advertising

An excellent example of the above-mentioned collection of a user's digital footprint for marketing purposes is behavioral advertising. Behavioral advertising is a technique based on tracking users when they use the Internet. Digital service providers collect and process personal data to provide users with advertising matching their interests. This topic was comprehensively researched by the Working Party set up under Article 29 of Directive 95/46/EC in its Opinion 2/2010 on online behavioral advertising. Behavioral advertising comprises many different methods that all have a common feature - observation of the characteristics of a user's behavior over time through their actions. This data tracking is possible usually due to cookies or similar technology and it results in detailed user profiles.

The reason behind behavioral advertising is to compensate for the free content of the website in return for precisely targeted advertisements. The efficiency of this business model has been measured in several papers (Scott, 2013). One study has shown that behavioral targeting increases the efficiency of an advertisement by 242 % - non-targeted ads generated 2.8 percent buyer-yield efficiency whilst targeted ads attracted 6.8 percent of users to purchase a product from a merchant's website (Network Advertising Initiative, 2010). By collecting an enormous volume of personal data from a significant portfolio of users (data mining) the effect of ad targeting is even amplified by using predictive software4 (Article 29 Working Party, 2014). Therefore, it can be concluded that the more complete a personal profile containing a user's preferences is available to advertising companies, the harder it is to resist the offer.

Smart Household Appliances and Wearable Computing

To provide the most complete picture of how a digital footprint is rendered into everyday life, let's look at the new-born concept of the "Internet of Things" (IoT). The IoT has been receiving a lot of attention in recent years and was also researched in Article 29 Opinion 8/2014 on Recent Developments on the Internet of Things. As described here, the concept of IoT is based on an infrastructure of sensors, cameras, microphones, or transmitting chips embedded in common, everyday things. This does not mean users cannot trust their toasters anymore, but more likely it sets a brand-new challenge with respect to possible intrusions into their private lives.

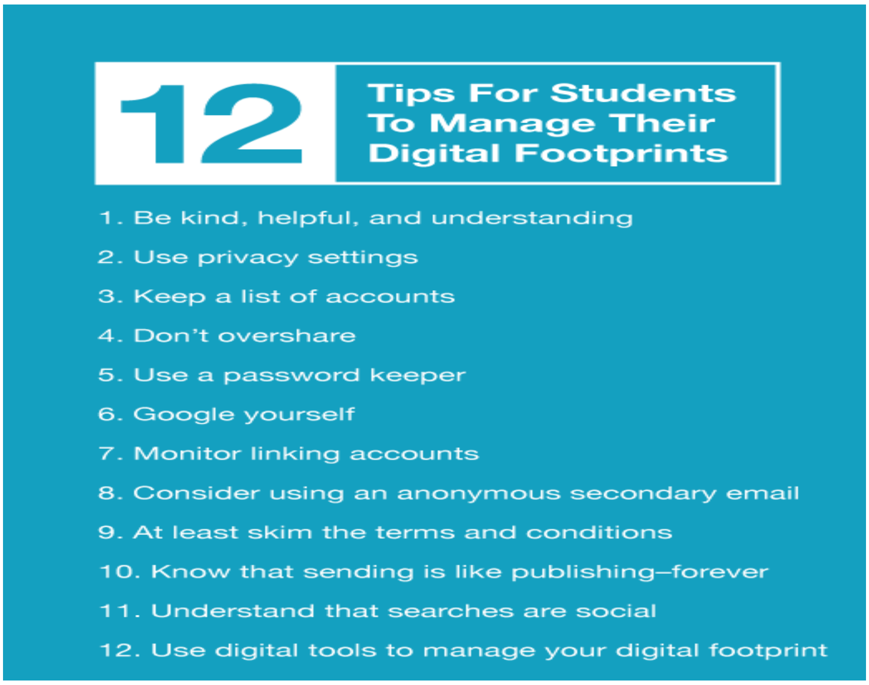
Risks

The leaking of personal data could hardly be considered harmless. Regulation 2016/679 enumerates a long list, with varying likelihood and severity, of possible consequences of misuse of personal data. The list begins with "physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage (...)". Unfortunately, the common denominator of these categories is their abstractness. The precise calculation of total economic losses made to an individual's rights is almost unquantifiable. Nevertheless, Acquits deduced that the estimated economic losses of consumers reached billions of dollars. Acquits also concluded that the total net effect on privacy remains an open question because many breaches of personal data were not subsequently abused to gain profit (Acquits et al., 2006: 1565).

Protecting your Digital Footprints: Because employers, colleges, and others can look up your online identity, it's a good idea to be mindful of your digital footprint. Here are some tips for protecting your personal data and managing your online reputation. Following are some remedies:

- Use search engines to check your digital footprint.
- Reduce the number of information sources that mention you.
- Limit the amount of data your share.
- Double-check your privacy settings.
- Avoid oversharing on social media.

- Avoid unsafe websites.
- Avoid disclosing private data on public Wi-Fi.
- Delete old accounts.
- Create strong passwords and use a password manager.
- Keep an eye on your medical records.
- Don’t log in with Facebook.
- Keep software up to date.
- Review your mobile use.
- Think before you post.
- Use a VPN.



12 Tips For Students To Manage Their Digital Footprints

1. Be kind, helpful, and understanding
2. Use privacy settings
3. Keep a list of accounts
4. Don’t overshare
5. Use a password keeper
6. Google yourself
7. Monitor linking accounts
8. Consider using an anonymous secondary email
9. At least skim the terms and conditions
10. Know that sending is like publishing—forever
11. Understand that searches are social
12. Use digital tools to manage your digital footprint

Steps parents should take for youngsters’ digital safety:

- Explain the dangers of posting content that you feel might be inappropriate or controversial and the trail that can be left behind.
- Ensure that they know the dangers of posting content and personal details including pictures.
- Encourage them not to divulge any personal details such as age, address, or contact details to anyone online.
- If they feel they might have put themselves in danger, or feel in danger remember to reassure them that you are always there to support them.
- Many people want to share the fact that they are going on holiday and how long they are going for – think about the impact and danger this could be placing your family in.
- It is a criminal offense to use the internet to threaten or harass people.

II. CONCLUSION

In this article, we looked at the concept of Digital Footprint and the mechanism behind it. Steps were also discussed on how teenagers should surf safely over the web without being tracked. Digital footprints as an emerging dimension of digital inequality connect to the broader societal and academic discourse on the mutual dependency of society and technology. While digital inequality scholarship has addressed this nexus by analyzing the mechanisms between life chances and the purposeful use of ICTs, we have argued for the inclusion of digital footprints in the analysis of what ultimately concerns informational and social justice.

Disregarding the result of the initiative mentioned above, future proposals will have to find a balance in the matter of protecting and empowering users. As a proximate to the consumer protection idea, there is an ongoing trend to switch to

DOI: 10.17148/IJARCCE.2023.12302

user protection. This approach follows the traditional objection that it should not be the user's responsibility to protect his or her privacy. It should be the responsibility of commercial subjects not to violate users' rights (Albert, 2002).

REFERENCES

[1] Abidin, C. (2015), "Communicative intimacies: influencers and perceived interconnect-ends", Ada: A Journal of Gender, New Media, and Technology, Vol. 8, available at http://adanewmedia.org/2015/11/issue8-abidin/
[2] Andrejevic, M. (2014), "The big data divide", International Journal of Communication, Vol. 8, pp. 1673-1689.
[3] Baruh, L., Secinti, E. and Cemalcilar, Z. (2017), "Online privacy concerns and privacy management: a meta-analytical review", Journal of Communication, Vol. 67 No. 1, pp. 26-53.
[4] Beer, D. (2017), "The social power of algorithms", Information, Communication & Society, Vol. 20 No. 1, pp. 1-13.
[5] Blank, G. (2013), "Who creates content? Stratification and content creation on the Internet", Information, Communication & Society, Vol. 16 No. 4, pp. 590-612.
[6] Blank, G., & Lutz, C. (2017), "Representativeness of Social Media in Great Britain: Investigating Facebook, LinkedIn, Twitter, Pinterest, Google+, and Instagram", American Behavioral Scientist, Vol. 61 No 7, pp. 741-756.
[7] Bucher, T. (2017), "The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms", Information, Communication & Society, Vol. 20 No 1, pp. 30–44.
[8] Büchi, M., Just, N. and Latzer, M. (2017), "Caring is not enough: the importance of Internet skills for online privacy protection", Information, Communication & Society, Vol. 20 No. 8, pp. 1261-1278.
[9] Casemajor, N., Couture, S., Delfin, M., Goerzen, M. and Delfanti, A. (2015), "Non-participation in digital media: toward a framework of mediated political action", Media, Culture & Society, Vol. 37 No. 6, pp. 850-866. Cath, C., Zimmer, M., Lomborg, S., and Zevenbergen, B. (2018). Association of Internet Researchers (AoIR) Roundtable Summary: Artificial Intelligence and the Good Society Workshop Proceedings. Philosophy & Technology, Vol. 31 No. 1, pp. 155-162.
[10] Cavoukian, A. (2009), "Privacy by Design – Take the Challenge", Information and Privacy Commissioner, Toronto, Ontario.
[11] Clarkson, P. J., Coleman R., Keates S., and Lebbon C. (2013), Inclusive Design: Design for the Whole Population, Springer Science & Business Media.
[12] Couldry, N., Fotopoulou, A. and Dickens, L. (2016), "Real social analytics: a contribution towards a phenomenology of a digital world", The British Journal of Sociology, Vol. 67 No. 1, pp. 118-137.