**Forum:** Human Rights Council

**Issue:** Measures to preserve the right to privacy in a digital age

**Student Officer:** Tia Ching

**Position:** President of Human Rights Council

---

## Introduction

With rapidly developing technology and network, issues concerning privacy, such as cyber-crime and personal data exploitation, began to emerge. Most individuals in the world have shared information about themselves on the internet either for business or pleasure; such action inevitably leaves a digital trail consisting of personal data for everyone. Governments and companies often strive to enhance policies to gain consumer trust and maintain privacy for internet users.

Most internet users lack the information they require to make informed decisions about providers. Users are constantly tracked with their preferences, information, or movement without their consent or awareness. User's personal information is often used to manipulate them. In a data-driven society associated with ubiquitous corruption, privacy becomes crucial and hard to preserve.

Businesses tackle such problems by providing users with transparency and data protection on how they use and collect data. Governments have also created legislation in attempt to safeguard the sensitive data of users. Examples include the Privacy Commissioner's Guidelines for Online Consent by the Canadian Parliament, and the "Internet Bill of Rights" in Brazil. These legislations establish oversight with internet providers and users, also regulating user consent.

## Definition of Key Terms

### Cybercrime

Cybercrime is any criminal activity that is done using computers or the internet. Cybercriminals generally generate profit from cybercrime. Certain cybercrimes are done to devices directly to disable or damage them.

### Digital Privacy

Digital privacy is the protection of internet users' personal information. Digital privacy is also defined under the categories of individual privacy, information privacy, and communication privacy.

### Digital Property

Digital property is any information created by or about the internet user in digital form. Examples of digital property include social media pages, website domains, website hosts, and google analytics.

## Background Information

In 2012, United Nations (UN) created its first-ever resolution to assert that human rights and privacy must also be protected in the digital realm. Since 2012, dramatic revelations regarding state surveillance regimes, including the mass surveillance of private communication through online platforms, have provoked international debates about the perseverance of rights in the digital world. Users' private information became at risk of being sold or used for illicit purposes. Mentioned in a study, over half of the internet users in the United States (US) feel insecure about their internet privacy, where most users have significant fear of cybercrime.

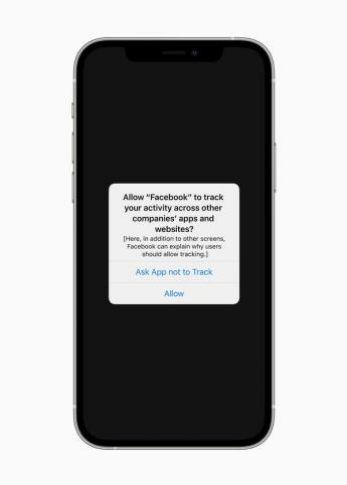
### Advertising

There was an upheaval in the advertising industry in the digital realm more than 20 years ago. Digital advertisement suddenly became the main way firms choose to advertise. Nowadays, countless brands splash ads across all kinds of websites. Digital advertisements accelerated Facebook, Google, and Twitter's growth, in which they are able to offer free social networking to people. In exchange, users were tracked for their personal data by technologies like "cookies". Their data are used to target them for relevant marketing.

Companies depend heavily on digital ads, but to achieve that, they continue to exploit access to users' personal data, violating their privacy without their knowledge. Since iPhone and Android app stores were created in 2008, advertisers have planted invisible trackers in apps for more specific trackings and targetting. Tiktok is another example of an app that flourished with this function. Personal data became the currency supporting online services and content.

#### *Actions to tackle information exploitation for advertisements*

In recent years an increasing number of firms have tried to ask for clear consent on any tracking actions in their app or website. An example is Apple's pop-up notification, which addresses tracking activities on users' phones. If the user refuses to track, then the app stops all monitoring and sharing data actions with other third parties.




***Caption #1: Apple's pop-up notification***

## Location Tracking

Admittedly, location tracking technology is helpful in everyday lives, but it is also debated to be putting users' privacy at risk. GPS and BlueTooth allow smartphones to know people's location and even which people we are with. Certain apps exploit these data and collect or profit from them without having users' clear consent. Governments and companies tried to tackle this issue, but COVID-19's outbreak slowed down this process. Location-tracking technology slowed the COVID-19 spread by alerting people where COVID is serious and predicting tracks of the virus' spread. In fact, the increasing usage of location tracking technology during COVID created a positive correlation with the exploitation of this location information.

The main usage of location tracking is also to deliver more direct and relevant content to users. However, the consequences are an expanded digital footprint and a higher risk of data breaches. Although apps have privacy policies, such privacy policies are also questioned to be not transparent. Therefore people must tackle the problem, by keeping the conveniences that location tracking technology has brought and reducing the consequences of such technology.

## Privacy Policies

In most apps, users are required to accept a privacy policy before they enter the app. Privacy policies became an excuse for companies where they claim that their data is fair and have undergone consent. Nonetheless, explanations of the privacy policies are often misleading, incomplete or confusing. For example, the app might ask for the permission on location tracking to give them traffic information but will bypass the fact that the data will be sold and shared. Such disclosure is hidden in vague privacy policies.

In addition, the majority of privacy policies exceed college reading levels. Reading comprehension became a major issue, where users can't ~~even~~ understand the descriptions. The lengthy and dense texts also make the privacy policies difficult to read. The European Union (EU) general data

protection regulation demanded concise policies, prompting many firms to shrink their policies. However, companies often choose to include data collection process information in their descriptions and not address to users how much they are exposed.

The aforementioned reasons are what often lead to users providing consent without full comprehension of what they are consenting to. This also gives firms more power to information exploitation and violate user privacy.

## Major Events

In recent years, increasing number of firms have been reported to have privacy violation actions. With rapidly developing technology and weak data protection regulations, major internet firms have chosen to exploit the privacy of users in order to achieve profit. For example, in 2020, Zoom was accused of sharing users' information to third parties without users' knowledge. It performed an undisclosed data mining in user conversations. Google's education platform was said to have illegally collected biometric data from minors, violating the Children's Online Privacy Protection Act (COPPA). WhatsApp's flawed system protection was hacked by a group of hackers in 2019. This issue led to over 1400 users' phones being hacked within less than two weeks. These examples reflect the seriousness of digital privacy in our current society, and how firms should be more strictly regulated in their data protection functions.

### *Facebook Cambridge Analytica Scandal*

US and British lawyers sued Facebook, Cambridge Analytica, and other companies for breaking the states' policy by exploiting users' biometric data through functions like facial recognition. Cambridge Analytica was accused of interfering with Brexit with their user data, though an official investigation claimed that no significant illegal actions exist. In 2019, the Federal Trade Commission fined Facebook $5 billion for privacy violations. These data privacy breaches sparked movements such as the #DeleteFacebook movement.

### *State of Arizona Sued Google*

In 2022, Arizona filed a lawsuit against Google for violating location privacy policies and advertisement information. Google was accused of deceiving users with confusing location tracking settings. The judge allowed proceeding with the claim that Google is involved in deceptive practices, but he rejected the argument that google takes location data for ads. In past years, there have also been several similar cases regarding Google's privacy settings and how they misled consumers. Due to such cases, users have been worried about their internet usage, leading them unable to trust Google as a whole. With this fear, users became reluctant to use location apps, or grant access to their information on google. What should've been useful services for users, became tools to exploit information.

## Major Countries and Organizations Involved

### People's Republic of China

China heavily relies on mass surveillance; this raises public resistance and concern about privacy protection. Some of the largest information breaches took place in China, all involving the personal information of over one billion people. Furthermore, information exploitation became concerningly easy for Chinese firms due to flawed digital privacy protection regulations.

### Electronic Frontier Foundation (EFF)

EFF is a nonprofit organization that aims to defend digital privacy formed in 1990. EFF has made an impact on litigations, where their attorneys protect user privacy in the digital realm. EFF also collaborates with several largest companies in the world, to strive for a digital environment with human rights.

### Norway

Norway has the best digital privacy among all the countries in the world achieving a 90.1 privacy score. Most data exchange online is encrypted, and the Norway government has high respect for internet privacy. The government claims that they value privacy rights over the entertainment industry's businesses.

### Payment Card Industry Security Standards Council (PCI)

PCI is a non-governmental organization (NGO), managed by the Federal Trade Commission (FTC). The PCI created the Payment Card Industry Data Security Standard (PCI DSS), consisted of requirements aimed to regulate firms take responsibility of user privacy. PCI DSS ensures that all companies process, accept, store, and transmit data in a moral and secure manner. These requirements allow for the protection of user's privacy in transactions, offering users reassurance to their privacy. Since credit card information and privacy remains as a top concern for users, the PCI DSS was an efficient method to regulate and formalize the protection of privacy in all businesses.

## Timeline of Events

| Date | Description of event |
|---|---|
| 1981 | The Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data (Convention 108) was created to guard internet privacy. |
| 1984 | The Data Protection Act was passed in the United Kingdom. |

| | |
|---|---|
| 1994 | Cookies were invented, and for the first time, users began being tracked for the websites they visited. |
| 1995 | The Data Protection Directive was passed by the European Union due to increasing concern about internet privacy. |
| October 28th, 2000 | Google launched AdWords, where it uses cookies to provide personalized ads to users. |
| 2004 | Facebook was created, but it was also charged with security breaches, privacy, and copyright violations by the Harvard administration. |
| 2009 | Facebook was accused of its flawed privacy policy. Campaigners were outraging about the privacy settings that expose more information about people online. |
| 2011 | Google Buzz was accused of privacy violations. Google settled for $8.5 million and promised that it will be independently audited for the next 20 years. |
| 2012 | European Commission starts the plan to craft the General Data Protection Regulation (GDPR). |
| 2014 | iCloud was being cyber attacked as hackers released private pictures of certain celebrities, harvested from their iCloud accounts. |
| 2018 | GDPR was put into action, regulating online information and privacy. |
| 2021 | Due to COVID-19, mass surveillance technology was put into use, but people started to question whether their privacy is protected in such mass surveillance. |

## Relevant UN Treaties and Events

- The Right to Privacy in the Digital Age, 26 September 2019 (A/HRC/RES/42/15)
- General Data Protection Regulation, 25 May 2018 (European Union)

## Previous Attempts to solve the Issue

### Norway

Norway's personal data act categorizes most personal data as sensitive information. This allowed the privacy of users to be largely protected. Norway achieved outstanding digital privacy protection by implementing strict regulations on all users' information. Norway established the Norwegian Data Protection Authority, an independent supervisory authority to protect users' information, making significant effort regarding digital privacy. Apart from Norway's participation in GDPR, Norway already has a robust Personal Data Act. The regulations stated in the Personal Data Act are extremely detailed

and careful. For example, any form of collection of user data, requires users to be informed on the collectors' name, address, purpose of data collection and whether the data will be shared to third parties. The level of detail in the Personal Data Act, the enhancement of GDPR and the supervision of the Norwegian Data Protection Authority, all contributes to the success of Norway in protecting users' privacy and rights.

### Raising awareness

A number of countries and organizations have made attempts in raising awareness of digital privacy. Organizations such as the EFF and Privacy International have hosted speeches and created sophisticated websites to raise awareness. Such organizations promote ways to enhance security on devices and teach users how to protect their privacy. By raising awareness, users of the internet can more seriously acknowledge the problems existing with internet safety and security and protect their own rights accordingly.

### Business efforts for the protection of privacy

As the issue of digital privacy becomes increasingly prevalent in human rights and the current society, major companies such as Google, Instagram, Apple, and Facebook have taken action to enhance their privacy protection measures. Companies strive to earn users' trust, which is an essential reason why they work hard to improve protection. As aforementioned, Apple's launch of the consent pop-up notification is an improvement to gaining clear and full consent of tracking from users. Its forced stop on tracking when the user clicks reject, also notes how users are having more power to manage their information and activities on the internet. The shortened privacy policy of these companies also marks a development in making all users clearly aware of where and how their private information is being used.

## Possible Solutions

### Further regulations on privacy policies

Though many privacy policies are regulated for their lengths, the reading levels of privacy policies remain poorly controlled. The unreasonably high reading levels are the main cause of why a majority of users fail to understand privacy policies. Legislations may be set on how privacy policies may not exceed a certain reading level, and related professionals or officials may check and oversee them. This can effectively solve the problem of certain companies abusing privacy policies for privacy violations, and offer a clearer explanation to users of where their information is going and how it is being used or monitored.

### Direct communication of concerns regarding privacy

Most citizens or users are aware of the existing problems and are concerned about many apps or functions regarding their privacy. Governments or related official organizations may create a direct and simple place online where citizens can file complaints or concerns about digital privacy. Governments may create official social media accounts, email, or other methods on major platforms, so users can easily communicate their concerns to the related officials. This method can largely increase the confidence of users.

### Host bi-Annual forums discussing related issues

Major companies on the internet need constant monitoring of their breaches in user privacy. The UN or certain governments may host bi-annual forums to create a platform where officials from all three parties (governments, the UN, and representatives from major companies) can come together to discuss current progress and problems of digital privacy. Representatives from companies that constantly have privacy problems may also participate in addressing their plans on how to enhance their systems.

## Bibliography

Allstate Identity Protection. "Location Tracking Poses Serious Privacy Concerns. But Is It Key to Ending the Pandemic?" *Allstateidentityprotection.com*, https://www.allstateidentityprotection.com/content-hub/location-tracking-poses-serious-privacy-concerns. Accessed 22 July 2022.

Chen, Brian X. "The Battle for Digital Privacy Is Reshaping the Internet." *The New York Times*, The New York Times, 16 Sept. 2021, https://www.nytimes.com/2021/09/16/technology/digital-privacy.html.

"Facebook Hit with Four Lawsuits in One Week over Cambridge Analytica Scandal - Business & Human Rights Resource Centre." *Business & Human Rights Resource Centre*, https://www.business-humanrights.org/en/latest-news/facebook-hit-with-four-lawsuits-in-one-week-over-cambridge-analytica-scandal/. Accessed 22 July 2022.

"Google Cannot Escape Location Privacy Lawsuit in Arizona, Judge Rules." *Reuters*, Reuters, 25 Jan. 2022, https://www.reuters.com/technology/google-cannot-escape-location-privacy-lawsuit-arizona-judge-rules-2022-01-25/.

Litman-Navarro, Kevin. "Opinion." *The New York Times*, The New York Times, 12 June 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

Next, Carly, and Tomaso Falchetta. "The Right to Privacy in the Digital Age." *Journal of Human Rights Practice*, vol. 9, no. 1, 2017, pp. 104–118, https://doi.org10.1093/jhuman/huw026.

Qin, Amy, et al. "China's Surveillance State Hits Rare Resistance from Its Own Subjects." *The New York Times*, The New York Times, 14 July 2022, https://www.nytimes.com/2022/07/14/business/china-data-privacy.html.

*The Pop-up Notification That Apple Rolled out in April*. Apple, https://static01.nyt.com/images/2021/09/17/business/00futureinternet2-alt/merlin_186728538_1bdcfc32-64aa-4fef-8800-c66e2ce751b7-superJumbo.jpg?quality=75&auto=webp.

Valentino-DeVries, Jennifer, et al. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." *The New York Times*, The New York Times, 10 Dec. 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Walsh, Ray. "Staying Secure Online in Norway." *Proprivacy.com*, ProPrivacy, 28 Nov. 2020, https://proprivacy.com/guides/norway-privacy.

Youens, Annabel. "The Complete Data Privacy Timeline :" *AE*, Appreciation Engine (AE), 19 Feb. 2020, https://get.theappreciationengine.com/2020/02/19/data-privacy-timeline/.