

# Societal Safety and Preservation in the Digital Era

**Dylas Gudoshava**

*Zimbabwe Open University, Zimbabwe*

## INTRODUCTION

Personal privacy is being eroded from various directions as modern technologies bring numerous threats towards personal privacy. People are often unconscious about it and accept violation of privacy to a great extent without questions. Technological advancement has been embraced by all nations including developing countries. Today, the world is like a village where people share information at the same time but in different parts of the world over the internet.

Developing countries venture into new technologies without understanding the implications and the legal frame works under which the technologies operate. According to the 40th International Conference of Data protection and Privacy commissioners (2019), the technological pace keeps accelerating while the legal pace remains particularly slow. For this reason, developing countries may not effectively deal with crimes committed over the internet or in the office work environment. Spammers for instance, may send spam over the internet with little or no knowledge of users in developing countries. Although these countries may have laws on data protection, these laws are general in character and may not apply in crimes like spamming. Palfrey (2005) explained that, some countries use existing laws of general application to fight crimes like spam. Unfortunately, an observation made in 2005 still stands in 2019 as these laws miss their target.

## BACKGROUND

Privacy and security are related, hence go hand in hand. The major difference being between legitimate and illegitimate uses of data. An illegitimate use of data is one that is unauthorised, that is, when data is stolen, altered, or viewed by the wrong party. This is the domain of security, which protects data from being inappropriately accessed, modified, or shared. Legitimate uses of data are those that have been authorised. However, in a discussion of privacy, there are plenty of legitimate data uses that may be problematic or harmful. For example, in countries where companies can collect individuals' data with only nominal notification, requiring users to search for ways to opt out, personal data can be used in ways that people did not expect or knowingly give permission to. This is the domain of privacy, which is broadly concerned with how people control and manage data about themselves. In essence, just because something is legal doesn't mean it is constructive.

Today's Internet age is marked by tremendous technological developments which allow for the collection and processing of an indistinct number of personal data. Before the advancement of technology, these data would have simply elapsed. However, with the advent of limitless capacity to store information, such as the cloud, google drive as well as digital space, there has been an increase in capacity of analysing and processing personal data. Personal information of daily life that is isolated does not necessarily

DOI: 10.4018/978-1-5225-9715-5.ch050

endanger personal privacy, however, put together, all this information allows for the creation of profiles of one's personality and such digital biographies increase vulnerability with regard to a variety of dangers. The right to privacy and the right to data protection have thus become two of the most important fundamental rights of modern society. Developments in the field of privacy require an innovative legal and political framework which can guarantee that the technological implications are correctly understood and regulated accordingly.

The Editorial Board (2017) describe Internet privacy as “involving the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet”. It has to be noted that Internet privacy is a subset of data privacy.

Wheeler (2017) noted that “Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behaviour on a website. PII refers to any information that can be used to identify an individual. Age and physical address alone, for example could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person. Some experts such as Steve Rambam, a private investigator specialising in Internet privacy cases, believe that “privacy no longer exists”. He notes that “Privacy is dead – get over it” (Rambam, 2015).

While illegitimate uses of data must be contested with security, legitimate but harmful uses of data must be interrogated through the lens of privacy preservation

The penetration of Internet throughout the world is bringing an increase in volume of user information online. Developing countries such as those of Africa are included as contributors and consumers of this voluminous information. Concerns have been shown from different parts of the world regarding Internet user privacy and security. For Southern African region, very little is known regarding how Internet users are concerned with their online privacy and security. This chapter aims to compare Internet user awareness and concerns about online privacy and security between users in a developing country and users in a developed country, and to determine any common attitudes and differences between these user groups.

Retreating to one's home, closing an office door, or hanging up a phone may have previously allowed a person to feel a measure of control over who might be listening or watching, but the presence of network-connected devices in private spaces can remove this sense of control and privacy (Rosner and Kenneally, 2017). In an article by Fick and Akwagyiram (2019) in the Nairobi/Lagos Reuters, it was noted that “in Kenya, there is a large and fast growing population of internet users”. At the same time, there are no specific laws or regulations to protect the privacy of those individuals. Recent revelations about British analytics firm Cambridge Analytica, which Facebook says improperly accessed personal data of about 50 million of the social networks users in the 2016 U.S. presidential election, have also touched the African continent.

Fick and Akwagyiram (2019) noted that “Kenya is not alone in Africa, which as a region has clocked the world's fastest growth in internet use over the past decade”. Unlike in Europe and the United States, where data-privacy laws provide a level of protection to consumers, many Africans have little or no recourse if a data breach occurs because often legal and regulatory safeguards don't exist. In an article by Kshetri (2019), he observed that there were 24 million malware incidents that targeted Africa in 2016. In a survey conducted in Ghana, it was noted that “in 2016, Ghana's financial institutions were reported to experience more than 400,000 incidents related to malware, 44 million related to spam emails”.

Some economies in the continent are becoming attractive to cybercriminals, thanks to the high degree of digitisation of economic activities. For instance, 86% of South Africans regularly use online banking services. This proportion is higher than many countries in the Middle East and Turkey.

The chapter seeks to answer research questions that follow:

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/societal-safety-and-preservation-in-the-digital-era/248081](http://www.igi-global.com/chapter/societal-safety-and-preservation-in-the-digital-era/248081)

## Related Content

---

### Slave Patrols: The Precursor to Police Brutality

(2023). *Analyzing Black History From Slavery Through Racial Profiling by Police* (pp. 59-73).

[www.irma-international.org/chapter/slave-patrols/321626](http://www.irma-international.org/chapter/slave-patrols/321626)

### General View for Investigative Interviewing of Children: Investigative Interviewing

Elif Gökçearslan Çifciand Huseyin Batman (2018). *Social, Psychological, and Forensic Perspectives on Sexual Abuse* (pp. 54-69).

[www.irma-international.org/chapter/general-view-for-investigative-interviewing-of-children/197819](http://www.irma-international.org/chapter/general-view-for-investigative-interviewing-of-children/197819)

### Case Study: Australia

(2023). *Comparing Black Deaths in Custody, Police Brutality, and Social Justice Solutions* (pp. 96-120).

[www.irma-international.org/chapter/case-study/323586](http://www.irma-international.org/chapter/case-study/323586)

### Also, Victims of Expectations: The Double Bias Complexity of Drugs and Sexuality

Sílvia Ribeiro (2024). *Investigating and Combating Gender-Related Victimization* (pp. 1-24).

[www.irma-international.org/chapter/also-victims-of-expectations/342070](http://www.irma-international.org/chapter/also-victims-of-expectations/342070)

### The Normative Basis for Victims' Rights and Their Status in the Criminal Justice Process

(2019). *Sexual Violence and Effective Redress for Victims in Post-Conflict Situations: Emerging Research and Opportunities* (pp. 57-113).

[www.irma-international.org/chapter/the-normative-basis-for-victims-rights-and-their-status-in-the-criminal-justice-process/222361](http://www.irma-international.org/chapter/the-normative-basis-for-victims-rights-and-their-status-in-the-criminal-justice-process/222361)