New Communication and Privacy Violation in Virtual Communities A Foresight Approach toward Ethical Duty in Interaction

Selami Saidani
Mohamed Boudiaf University of M'Sila, Algeria,
salami.saidani@univ-msila.dz

Received: 27/08/2025 Accepted: 23/11/2025

Abstract:

The interactive world has enabled us to communicate anytime and anywhere on the globe, thus reshaping the concept of proximity among peoples through interactive communication. Privacy, in this context, refers to the individual's right to live alone, to retreat into solitude, or to associate with those they are familiar with, free from external interference. It also entails protection from surveillance and intrusion. When privacy is violated, it opens the door to a significant issue known as legal crimes of privacy violation.

Such topics and perspectives fall within recent research trends in monitoring the performance of new media, particularly regarding the essence of their content and the extent of intrusion into the privacy of interactive communities. Therefore, this research paper attempts to explore ways of establishing interaction ethics in order to preserve the privacy of every user on new media platforms, mainly represented by social networking sites.

key words*: New Communication, Privacy, Violation, Virtual Communities.*

Introduction

The information revolution began as a result of the convergence of communication technologies on one hand, and information technologies on the other. This revolution represents the scientific and technological leap we are witnessing today, to the point where this era has come to be called the "Age of Information." Information has always been one of humankind's most valuable assets throughout history: it was collected, recorded, and preserved on progressively evolving media — starting with the walls of temples and tombs, then papyrus, and later the invention of paper in its various forms, until it finally reached electronic magnetic disks.

Traditional interests that have long been protected by legislation and legal systems are now facing new forms of assault due to modern technology. Whereas theft once targeted property in traditional ways or through fraud, and written documents were compromised through forgery, now financial assets are attacked via hacking into information networks and conducting electronic transfers across the globe within seconds. Similarly, legal rights once preserved in paper-based records are now being violated in their electronic formats by breaching information systems without the need to tamper with physical documents.

Just as private life was once intruded upon through eavesdropping or unauthorized photography, today privacy is violated through hacking into personal email, personal computers, and sensitive databases in healthcare, hospitals, credit institutions, and social security systems. This is the core concern of our study, which highlights the key challenges facing the interactive individual across the digital network.

1.The Core Challenges to Interactive Identity in New Communication Media

Mahmoud Alam El-Din identifies that information and communication technology encompasses three main dimensions:[1]

- **The Information Revolution:** a massive explosion of knowledge across numerous disciplines and languages, which technology attempts to organize and utilize.
- **The Communication Revolution:** embodied in wired and wireless communication technologies, from television and broadcast programs to satellites and optical technologies.
- **The Computer Revolution:** which has permeated every aspect of life, merged with communication technologies, and expanded through the rise of the Internet. This has led to two processes:
    - Transnationalization: the crossing of commercial borders.

- Informationalization: the crossing of informational borders.

In his 1995 book Electronic Dialogue: Reshaping Democracy in the Age of Media, Lawrence Grossman former head of Public Broadcasting and NBC television — argued that as the world approached the 21st century, the United States was transforming into an "electronic republic." He envisioned a new political environment in which citizens would have a stronger daily influence on state decisions.

Two major factors were driving this democratic transformation:[2]

1. A 200-year-long movement toward greater political equality for all citizens.
2. The enormous growth of long-distance communication technologies and the integration of television, telephony, satellites, cable, and personal computers.

Developing countries, meanwhile, have become vulnerable to international communication intrusions. Communication channels particularly television are not merely informational tools; they represent a shift toward a borderless world. This has weakened the traditional notion of national sovereignty, which once relied not only on physical authority and barriers but also on control over information. With the current revolution in information and communication technologies, along with the global nature of media and the increasing use of satellite broadcasting, most states have lost much of their ability to control information flows.

For citizens, the impact of the "info-communication revolution" is largely negative. The importance of the people does not lie merely in their legal definition as a population, but rather in their cohesion, loyalty, and faith in their state. With digital networks reshaping perceptions of time and space, and transcending geographical boundaries, new forms of belonging have emerged in the shape of "electronic communities." However, this can weaken people's loyalty to their political systems and their states.[3]

Such changes in the traditional concepts of state, authority, and security, alongside the rise of new concepts such *as cultural security*, are primarily due to the pressing features of information and communication technology, which can be summarized as follows:

1. **Interactivity:** the degree to which participants influence communication roles and exchange them (interactive practice). Interactivity refers to the degree of reciprocal communication and mutual influence between users and a medium, system, or environment. It goes beyond one-way information transfer by enabling users to actively participate, respond, and shape the flow of communication. Scholars in communication and media studies view interactivity as a defining characteristic of digital technologies, distinguishing them from traditional mass media.
2. **Demassification:** messages can be directed to individuals or specific groups rather than massive audiences. Demassification refers to the process by which mass

communication and media shift from addressing large, undifferentiated audiences to targeting smaller, more specialized groups. With the rise of digital technologies, audiences are no longer treated as a single homogeneous entity but as fragmented communities with distinct needs, interests, and identities.

3. **Asynchronicity:** the ability to send and receive messages at convenient times without requiring simultaneous participation. Asynchronicity in communication refers to the separation of time between the sending and receiving of messages. Unlike synchronous communication, where interaction happens in real time (e.g., phone calls, live chats), asynchronous communication allows participants to engage at different times.
4. **Mobility :** communication technologies can be used on the move (e.g., mobile phones). Mobility in communication refers to the ability to access, create, and share information anytime and anywhere through portable digital devices such as smartphones, tablets, and laptops. It removes spatial and temporal restrictions, enabling constant connectivity and interaction.
5. **Convertibility :** the ability to transfer information across media (e.g., converting spoken messages into written text). Convertibility in digital communication refers to the capacity of media content to be transformed from one format, platform, or medium into another without losing its essential meaning. It allows text, audio, video, and images to be adapted, repurposed, and circulated across different digital environments.
6. **Connectivity :** the capacity of communication devices to connect with diverse systems regardless of manufacturer or country of origin. Connectivity refers to the capacity of digital technologies and networks to link individuals, groups, and systems across spatial and temporal boundaries. It enables constant interaction, access to information, and participation in social, economic, and cultural activities. Connectivity enhances collaboration, facilitates real-time communication, and supports the integration of global communities. However, it also raises concerns about digital divides, dependence on technology, and privacy issues. Ultimately, connectivity represents the backbone of the digital environment, shaping how societies function and interact in the information age.
7. **Ubiquity :** the widespread global reach of communication systems. Ubiquity refers to the omnipresence of digital technologies and media in everyday life, allowing individuals to access information, communication, and services at any time and from any location. This constant availability transforms how people work, learn, and socialize, fostering a seamless integration of the digital and physical worlds. Ubiquity enhances efficiency, personalization, and immediacy of interaction, but it also introduces challenges related to information overload, surveillance, and the erosion of personal boundaries. In essence, ubiquity underscores the pervasive nature of technology in shaping contemporary human experience.

8. **Globalization :** the new communication environment has become global, allowing information to follow the same complex pathways as international capital flows. Globalization refers to the increasing interconnectedness and interdependence of societies, economies, and cultures across the world, facilitated by advances in communication, transportation, and digital technologies. It enables the rapid flow of information, goods, services, and ideas beyond geographical boundaries, fostering cultural exchange and economic integration. In the media and communication context, globalization amplifies the reach of content, shaping global public opinion and creating a shared cultural space. However, it also raises concerns about cultural homogenization, digital divides, and the dominance of powerful global actors over local voices.

- ***The Main Challenges of New Media Interaction :***

1. Technical Challenge: remaining consumers rather than producers of technology, failing to use it effectively.
2. Professional Challenge: lack of trained technical and programming specialists who can localize culture and knowledge.
3. Stylistic Challenge: weak rhetorical consistency and lack of engaging, distinctive presentation in media content.
4. Content Challenge: poor prioritization of messages — sometimes rushed, sometimes delayed.
5. Internal Challenge: lack of confidence and hesitation in presenting what we have to offer.
6. Acceptance of Others: impatience in communicating messages, leading to difficulty in gaining acceptance.
7. Philosophical/Methodological Challenge: swinging between complete openness and complete isolation, instead of adopting a balanced approach.
8. Specialization and Methodology Challenge: the need for media work to become a highly professionalized and specialized industry.
9. Role Integration Challenge: the necessity of coordination between media and security as complementary forces.
10. Pace Challenge: the rapid evolution of science and technology forces constant adaptation and immediate application to avoid falling behind.[4]

2. Interactive Media

Since the mid-20th century, the world has witnessed tremendous technological leaps, the most important of which are communication systems. This gave rise to the **Information Society**, resulting from the convergence of satellite communication technologies with their immense ability to transcend the boundaries of time and space and computer technologies capable of storing vast amounts of data and retrieving them within seconds. This development enabled the emergence of information networks through instant

communication tools on Earth or via space, adding an important dimension to human capacity to expand knowledge, store it, organize it, produce information, broadcast it, and interact with it immediately.[5]

. What Do We Mean by Interactive Communication?

Researchers define interaction as involving both sender and receiver. One of its key characteristics is **responsiveness**. Interactive communication extends beyond interpersonal communication to include interaction with the medium itself, not just between the individuals involved in the communication process :[6]

- The term interactive communication is often used as a substitute for "computer-mediated mass communication."
- Interactive communication allows for the exchange of communicative roles.
- It implies equality among participants in communication and symmetry in communicative power, leading to group consensus through the free exchange of opinions without interference from external sources or forces.
- It fosters open democratic participation, such as real-time online discussions in chat rooms and online email exchange platforms.

Dr. Mahmoud Alam El-Din outlines seven levels through which newspapers benefit from the Internet:[7]

1. **First Level:** The Internet as a source of information and a tool to support news coverage, urgent events, and awareness of new books and publications.
2. **Second Level:** The Internet as a means of communication with external sources, correspondents, and in conducting meetings.
3. **Third Level:** The Internet as an interactive communication tool by expanding communication through email.
4. **Fourth Level:** The Internet as a medium for journalistic publishing by issuing newspaper copies, summaries, databases, or even full newspapers and magazines.
5. **Fifth Level:** The Internet as an advertising medium that increases newspaper revenue through online ads.
6. **Sixth Level:** The Internet as a tool for marketing and promoting services provided by the press institution, through creating websites presenting basic information about its development and achievements.
7. **Seventh Level:** The Internet as a provider of information services — transforming the press institution into a supplier of services for subscribers, such as circulars, newspapers, and bulletins on behalf of others.

3. Security Risks Threatening the Privacy of the Interactive Society

In the information age, with advanced technologies, state boundaries have become vulnerable to surveillance satellites and satellite broadcasting. The Arab and Islamic world has always been, and still is, a target — politically, culturally, and intellectually. Espionage methods have shifted from traditional means to electronic ones, particularly with the use of the Internet.

. Interactive Espionage

The danger lies not in the Internet itself but in the weakness of security measures used to protect institutional and governmental networks. Relying on foreign-made security systems is risky, as they are not entirely trustworthy.

The threat does not only come from hackers whose actions are usually limited to tampering or destroying content, which can be overcome by restoring secure backups but rather from intelligence agencies that conduct espionage to obtain state secrets and confidential information, then disclose them to hostile states or exploit them in ways harmful to national interests.[8]

Some cases of international espionage have been revealed, such as the key planted by the U.S. National Security Agency (NSA) in the Windows operating system. This was one reason why the German government announced its decision to replace Windows with alternative systems.

Additionally, a massive international electronic surveillance network, known as ECHELON, was exposed. Operated by the NSA in cooperation with intelligence agencies in Canada, Britain, Australia, and New Zealand, ECHELON intercepts phone calls and electronic messages of all types. Designed for non-military targets, it captures enormous quantities of communications and messages using keyword recognition through powerful computers. Secret monitoring stations worldwide in New Zealand, Australia, Britain, and the U.S. contribute to surveillance of global communications.

Modern espionage techniques also include information hiding within information (steganography). Sensitive data is embedded within ordinary files, making it harder to detect, even if the carrier is caught red-handed.

After the September 11 attacks in the U.S., surveillance satellites were ordered to focus on Afghanistan, searching for Osama bin Laden and his groups. Specialized satellites intercepted wireless and mobile phone communications, while others captured high-resolution images. The ECHELON system was also used to analyze signals, even weak or encrypted ones.[9]

. Piracy (Website Theft)

Piracy here refers to the unauthorized use or copying of operating systems and software. With the rise of the Internet, piracy has expanded, with many websites offering pirated software freely or for sale. Software piracy has caused massive financial losses, prompting software companies to form alliances such as the Business Software Alliance (BSA) to monitor and analyze the software market.[10]

BSA reports indicate that Internet piracy will surpass other forms. Companies proposed countermeasures such as scanning users' hard drives for pirated programs but faced strong opposition from privacy advocates. Instead, some companies collaborated with Internet Service Providers (ISPs) to identify and shut down piracy websites.

In the Arab world, piracy is widespread, often exacerbated by weak or absent intellectual property protection and lax enforcement of existing laws.

. Crimes Against Personal Privacy

In the contemporary digital age, the concept of personal privacy has acquired unprecedented significance. The rapid evolution of information and communication technologies, particularly the proliferation of the Internet, social media platforms, and data-driven economies, has created both opportunities and threats to individual rights. Among the most pressing challenges is the rise of crimes against personal privacy, a category of offenses that target one of the most fundamental human entitlements: the right to control one's personal information and to live free from unwarranted intrusion.

Crimes against personal privacy encompass a broad range of il licit acts, including unauthorized access to personal data, unlawful surveillance, identity theft, interception of private communications, and the misuse of digital traces such as browsing histories, cookies, and geolocation data. These practices not only violate legal protections but also undermine trust in digital systems, erode social cohesion, and compromise individual dignity. The issue becomes more complex when considering that individuals often disclose personal information voluntarily in online environments, without fully comprehending the potential consequences or the hidden mechanisms of data collection and exploitation.[11]

The legal and ethical dimensions of crimes against personal privacy are particularly critical. From the perspective of legal systems, both international conventions and domestic laws attempt to strike a balance between safeguarding privacy and ensuring other societal needs such as security, public order, and technological advancement. Ethically, privacy is tied to human dignity, autonomy, and freedom, and any violation is not merely a technical infringement but a moral offense against the very essence of personhood. Moreover, with globalization and the borderless nature of cyberspace, crimes against privacy often transcend jurisdictions, posing serious challenges to regulators, law enforcement agencies, and policy-makers.[12]

Another important dimension is the technological sophistication of these crimes. Cybercriminals exploit vulnerabilities in computer systems, mobile devices, and communication networks, often leveraging advanced tools such as malware, phishing techniques, artificial intelligence, and big data analytics. In addition, corporations and governments themselves may engage in practices that compromise privacy, blurring the line between legitimate data collection for service improvement and invasive surveillance that infringes on individual rights.

Therefore, the study of crimes against personal privacy requires an interdisciplinary approach that integrates law, ethics, technology, and sociology. It is not sufficient to merely identify the legal breaches; rather, there is a need to contextualize these violations within broader debates on digital rights, democratic governance, and the social contract in the information society. Protecting personal privacy must be understood as a collective responsibility, requiring awareness from individuals, accountability from corporations, and commitment from states.

Ultimately, crimes against personal privacy represent a defining challenge of the twenty-first century. Addressing them demands a proactive vision that combines robust legal frameworks, ethical standards, and technological safeguards, while fostering a culture of digital literacy and respect for human rights. Only through such a holistic perspective can societies mitigate the risks of privacy violations and ensure that technological progress does not come at the expense of fundamental freedoms.[13]

These crimes cannot be addressed adequately by traditional legal provisions. Technology has stripped behaviors of their material form, creating challenges in applying conventional laws.

The right to privacy is complex and multifaceted, encompassing:[14]

- the sanctity of the human body,
- the home,
- images,
- conversations and correspondence,
- and professional life.

With the rise of databases, privacy concerns have intensified. These databases, used for scientific, cultural, military, and commercial purposes, have become repositories of human secrets, easily accessible in ways unimaginable under traditional storage systems.

For instance, personal data provided voluntarily during transactions with banks, credit institutions, insurance companies, or social security agencies can be easily accessed. Internet protocols (such as HTTP) can reveal a user's device number, location, and email address. Some websites install programs like cookies on hard drives to collect user data.

Moreover, everything written online even emails is archived and retrievable decades later. Many users mistakenly believe that pseudonyms or fake email addresses protect their identities, but ISPs can access all their information and track their browsing activities.[15]

Conclusion

Divine legislations and secular systems alike agree on the necessity of respecting individual privacy. Even the mere intrusion into such information whether stored on a computer, in an email account, or elsewhere is considered a violation of personal privacy. With the widespread use of the Internet, many users have found their privacy compromised, either intentionally or accidentally. For instance, when an Internet user visits a website, the site issues two copies of a "cookie." Cookies are small text files sent by many websites to be stored on the visitor's device for various purposes, such as identifying repeat visitors or other tracking functions. One copy remains on the server of the website, while the other is stored on the visitor's hard drive in a file where other websites may also have deposited cookies without the user's awareness or consent.

Immediately, a unique identifier is generated to distinguish that visitor from others, and the cookie begins collecting information and transmitting it back to its source or to data-gathering and analysis companies, often advertising agencies. Each time the user revisits the website, the information is updated, and the browser continues executing these functions unless the user changes the browser settings. However, some suspicious websites may exploit these cookies by copying and misusing such files. Website owners may also obtain personal information voluntarily, as users tend to be less hesitant to disclose personal details to a computer system than to another human being.

Although certain tools exist to protect privacy while browsing the Internet, it remains very difficult to control what happens to data once it leaves the user's computer. Therefore, privacy protection must begin at the source: first by determining the types of data that should never become public, and then by restricting access to such information.

Bibliography List **:**

[1] Hisham Farid Rustum (1999), Criminal Law and the Risks of Information Technology, Modern Machines Library, Assiut, p.51.

[2] Bouhania Koui (2006), Media and Communication and the Inevitability of Socio-Cultural Change, Journal of Human Sciences, University of Batna, Algeria, No. 14, June, p.230.

[3] Mohamed Laakab (1996), Muslims in the Civilization of New Media, Dar Al-Ummah, Algeria, p.20.

[4] Bouhania Koui (1998), Modern Communication Technology and the Reality of Arab Media Discourse, The Third Scientific Conference of the Faculty of Arts, Philadelphia, Jordan.

[5] Abdel Fattah Bayoumi Hegazy (2007), The Conflict of Computers and the Internet – In the Model Arab Law, Dar Al-Kutub Al-Qanouniya, Cairo, p. 609.

[6] Badr al-Din Ahmed Ibrahim (2013). New Media: Its Impact and Role in Security Awareness, Security Awareness Conference, Center for Knowledge Enlightenment and the Higher Military Academy in cooperation with Naif University for Security Sciences, p. 15.

[7] Mahmoud Alam al-Din(2014), The Internet and Social Work, Al-Majdi Publishing and Distribution House, Cairo, p. 114.

[8] Abd al-Rahman Arabi (2013), Interactive Communication: A Theoretical Introduction, Ibn Salem Publishing House, Laghouat, p. 82.

[9] Mostafa Ahmed Mounir (), The Communicative Risks of the Internet. For further information, http://www.startimes.com/?t=30327235., (consulted on 15/10/2016, 21.30).

[10] http://www.startimes.com/?t=30327235. (consulted on 16/10/2016, 22.30).

[11] Saber, Mahmoud. (2007). Privacy in the Age of Computing. Al-Warsam Publishing and Distribution, Egypt, p126.

[12] Al-Alwani, sabrine (2004), Smart Devices and Independent Data. University of Sulaymaniyah Publications, Iraq, pp 133,134

[13] Saber, Mahmoud, Previous reference, P128.

[14] Mamdouh Khalil Omar (1993), Protection of Private Life and Criminal Law. Dar Al-Nahda Al-Arabiya, Cairo, p. 207.

[15] Ibid., p. 208.