CHAPTER 11
THE DIGITAL SELF

I, Me, and Myself, and My User ID online

Digital self is a mask we put on to draw in the innovative world. With the digital technologies such as web pages, online games, virtual worlds, social media, smart phones, Internet, self- extension is extensive. **It is the aspect of the self that is expressed or shared to others through the use of digital technology especially the Internet and social networking.** Jones (2007) mentioned that college students view cell phones, instant messaging and the Internet as "extensions of themselves.

Objects that one's possess can truly extend the self, as when an instrument or weapon enables us to get things done of which we would somehow, or another be unable. Belonging can likewise emblematically extend self. Sartre explained that the reason we want to have something is to enlarge our sense of self and that the only way we can know who we are is by observing what we have. Belk (1988) presented the concept of the extended self: (1) Dematerialization, (2) Reembodiment, (3) Sharing, (4) Co-construction of Self, and (5) Distributed memory.

This reasonable refresh looks to renew the idea, consolidate the effects of digitization, and give a comprehension of consumer feeling of self in the present innovative condition. It is essentially a work in advance, for the computerized condition and our conduct inside it keep on evolving. Be that as it may, some vital changes are now certain. Five changes with advanced utilization are viewed as that effect the idea of self and the idea of belonging. Required alterations and increments to the extended self are laid out, and bearings for future research are recommended. The advanced world opens a large group of new implies for self-extension utilizing numerous new items to come to an incomprehensibly more extensive crowd. Despite the fact that this requires certain reformulations, the fundamental idea of the extended self stays crucial.

Belk's Summary of Digital Modification of the Extended Self

Digital Dimension	Self	Possession
Dematerialization		Attachment to and singularization of virtual possessions; almost, but not quite the same
Reembodiment	Avatars affect offline self; multiplicity of selves	Attachment to avatars
Sharing	Self revelation; loss of control	Aggregate possessions; sense of shared place online
Co-construction of self	Affirmation of self;building aggregate extended self; "Attachment to Virtual Possessions in Videogames"	
Distributed memory	Narratives of Self	Digital clutter; digital cues to sense of past

"Your online identity is not the same as your real-world identity because the characteristics you represent online differ from the characteristics you represent in the physical world." - Internet Society, 2018

Digital Literacy and Disinhibition

Digital Literacy: Capabilities possessed by individuals who are living, learning, and working in a digital society.

You might be searching and navigating everyday through all types of information. Then based on that information, you make certain decisions and you share it socially with others using a variety of tools. Let's pretend that you want to book a trip to a beach. But first,

you might research things like accommodation, food and culture, and make travel plans based on what you find out. You might even create an itinerary online and share it with your family.

Digital literacy is about using technology confidently as you live, learn, and work in a challenging digital world. It is important to be digitally literate in order to monitor and evaluate information that you often see and receive online.

- As a student, you need to find answers to your questions such as your assignments. The internet is a great source for a wide array of information but you need to be careful. You need to evaluate whether the information presented is accurate or even true.

Online Disinhibition: lack of restraint that one feels when communicating online.

Two types of disinhibition:

1. Benign Disinhibition

- Speaking about emotions, fears, and wishes
- Showing kindness and helping others
- Combating loneliness through social interaction
- Finding emotional support

These are the healthy types of disinhibition because these are some of the things that you cannot freely speak offline. Especially if the people around you are not that accepting or overly critical of your behavior.

2. Toxic Disinhibition

- Rude language, harsh criticism, anger, hatred, and threats
- Pornography and violence
- Cyberbullying
- Threatening, humiliating, spreading rumors, making fun of others
- Cyber harassment and exploitation

Managing Toxic Disinhibition

1. Be careful about sharing: be careful what to share and what to post because people may react differently
2. Do not hang with the wrong crowd online: Use your social media accounts appropriately and productively. Follow those individuals who give you inspiration and who spread positivity.
3. Consider your emotional state before posting: Avoid posting things when you are feeling angry or frustrated. You might post something that you will regret later and this might be taken against you.
4. Consider other people's reactions

Social Networking in the Philippines

- The Philippines has the fastest growing internet population in Southeast Asia.
- Majority of the Filipinos use the internet primarily for social networking.
- They mostly use social networking for communication, information and entertainment.
- The Filipino youth are the biggest users of social networking in the past few years. They usually post pictures, videos of themselves, their friends and family. Thus, adolescents are particularly susceptible to cyberbullying, gossips and stalking.
- The Church, schools and government in the Philippines make efforts to prevent and effectively manage the spread of identity theft, false information and fake news in the country.

Philippine Declaration on Internet Rights and Principles

- **Internet Access for All**

Everyone has the right to affordable and quality access to the Internet. The State must narrow the digital divide in order to provide quality universal access and ensure an enabling environment for fair competition that will benefit all stakeholders and

promote consumer protection. Consistent with the distributed nature of the Internet, community-owned and driven information infrastructure and networks should also be promoted as alternatives or complements to national-level infrastructure.

- **Democratizing the Architecture of the Internet**

The Internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion and equal opportunity for all.

Recognizing the fundamental distributed, decentralized and diverse nature of the internet, everyone shall have universal and open access to the Internet and its content, free from discriminatory prioritization, filtering or control for political or commercial purposes, while allowing for legitimate technical traffic management. The Internet should continue to evolve via open, permission-less innovation and the voluntary adoption of standards through inclusive multi-stakeholder processes, with due regard for the diversity of human abilities.

- **Freedom of Expression & Association**

Everyone should have the right to freedom of expression, opinion, and association without interference online and offline. State and non-state actors should refrain from infringing upon the universal right to receive and impart information, opinions and ideas. Any restrictions on online activity should conform with necessary and proportionate principles. Attempts to silence critical voices and censor social and political content or debate on the Internet should be stopped.

Everyone should also be free to use the Internet to organize and form associations, and to engage in protests.

- **Right to Privacy & Protection of Personal Data**

Everyone has a right to privacy on the Internet and the right to control how their personal data is collected, used, disclosed, retained, and disposed. Everyone should be able to communicate free from the threat of surveillance and interception. Targeted surveillance for the protection of public health and safety should always provide safeguards for human rights and be governed by transparent rules and oversight mechanisms.

Everyone should also have the right to communicate anonymously on the Internet and should be free to use encryption technology to ensure secure, private and anonymous communication.

- **Gender Equality**

Everyone should have an equal right to learn about, access, define, use, and shape the Internet regardless of sex, sexual orientation, gender identity and expression. Efforts to increase access must recognize and redress existing gender inequalities. In particular, there must be full participation of women in all areas related to the development of the Internet to ensure gender equality.

Gender-based violence involving the use of technology is growing, and the harms and violations perpetrated through and with ICTs are in need of serious attention. There must be concrete programs and mechanisms to prevent violence in cyberspace by promoting human rights for all and harnessing the potential of ICTs to promote women's empowerment. The Internet must promote diversity and social justice, and should be a transformative space to challenge and dismantle social injustice and patriarchy.

- **Openness and Access to Information, Knowledge, and Culture**

Everyone should have the right to access information on the Internet and be free from restrictions on access to knowledge. Copyright and patent regimes must not disproportionately restrict the capacity of the Internet to support public access to knowledge and culture. The State must ensure an enabling environment where linguistic, religious, and cultural diversity are encouraged as it enriches the development of society.

It should also promote the development of local content and the production and use of free, *libre*, and open source software (FLOSS).

- **Socio-Economic Empowerment and Innovation**

  Everyone should be free to use the Internet for socio-economic empowerment and innovation. Innovators should be encouraged to design, develop, and implement information and communication technologies that respect human rights and that contribute to socio-economic empowerment and sustainable development. The State shall also foster an enabling environment for the growth of innovators and start-ups.

- **Education and Digital Literacy**

  Everyone should have the knowledge and skills that enable them to use and shape the Internet. Everyone should have access to online resources, materials, and knowledge. Digital literacy is fundamental to children's capacity to use the Internet competently and exercise their human rights. Digital literacy will facilitate more active, responsible, and productive citizen participation in political, social and economic spheres. The State should promote open educational resources and enable open access to research and data, as well as the use of free and open source software.

- **Liberty, Safety, & Security on the Internet**

  Everyone has the right to liberty and security on the Internet. Security measures, devised and implemented in a consensual manner, must be consistent with international human rights laws and norms. Everyone has the right to enjoy secure connections to and on the Internet, including protection from malware and fraud, as well as services and protocols that threaten or impair the current technical functioning of the Internet. Digital security measures should be commensurate with the threats they seek to address, taking into consideration and relative to the benefits of the social, economic and democratic activity they seek to protect.

- **Internet and ICTs for Environmental Sustainability**

  Sustainable use of the Internet must be encouraged and enabled. E-waste should be minimized and recycled or otherwise disposed of in a manner that is protective of the environment. Sustainable use of the Internet that minimizes its impact on resources should be encouraged.

Selective Presentation and Impression Management

Self-presentation is behavior that attempts to convey some information about oneself or some image of oneself to other people. These behaviors are activated by the evaluative presence of other people and by others' knowledge of one's behavior. In new situations, many people would like to impress and become self-conscious. People behave in ways designed to create a favorable impression or even to one's ideals. Humans are social animals and regulate our behavior to fit in world or adjust it to impression that we desire. People monitor their behavior, observe how others react and adjust their performance to create a desired impression.

Two Types of Self Presentation

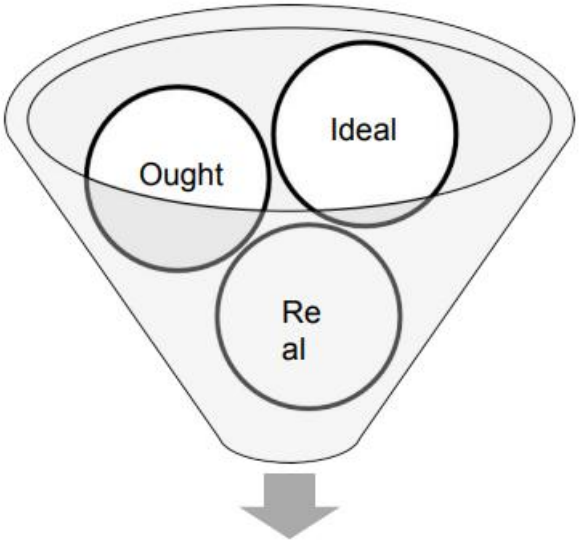
1. **Pleasing the audience** – This type of self-presentation which try to match self to the audience's expectations and preferences.
2. **Self-construction** – This type of self-presentation tries to match oneself to one's own ideal self. The expression of the audience-pleasing motive varies across situations.

Multiple Aspects of the Self

Higgins (1987) argues that there are three domains of the self: the actual self, the ideal self and the ought self.

1. **Actual self** – this refers to the attributes an individual possesses.
2. **Ideal self** – this refers to the attributes an individual would ideally possess.
3. **Ought self** – this refers to the attributes an individual ought to possess.

According to Higgins, the discrepancies between the actual self and ideal self leads to feelings of dejection. Our sense of self helps organize our thoughts, feelings and behaviors. Our overall self- evaluation influences our cognitive processes. For instance, when people with high self- evaluation fail, they sustain their self-worth by looking at others failure.



Multiple Aspects of the Self

Impact of Online Interaction on Self: Computer-Mediated Communication

Computer-mediated communication encompasses human communication involving several exchanges through various platforms such as text, audio, and/or video messages. A CMC interaction occurs through various types of networking technology and software, including email, Internet Relay Chat (IRC), instant messaging (IM), Usenet and mailing list servers. An interesting discussion can stem from a comparison of how we construct our identity in the “real world” versus how we construct it in the online world. As Dutton (1996) points out, that technology can work two ways – open or close social choices. Individuals shape the impact of technology has on their lives by choosing which technology to use and how to use it.

Boundaries of Self Online

The line between offline and online self has become blurred. Since people nowadays are becoming more connected digitally, self-identity is becoming more fashioned in transmedia paradigm. In the present culture of constant connectivity, the Internet is coordinated into our lives with the end goal that the experience of being on the web is subjectively not quite the same as before.

Types of Cyber Crimes

- **Phishing Scams** - Phishing scams are attempts by scammers to trick you into giving out your personal information such as bank account numbers, passwords and credit card numbers.
- **Online Scams** - basically scams that happen online.
- **Malware/Virus Dissemination** - Malware is the contraction of malicious software onto your system. It’s a piece of software written with the intent of causing harm to data and devices.
- **Email Bombing** - Email bombing is an overload of emails directed to one email address, this will cause the person receiving the emails server to become sluggish or even crash
- **Theft** - The aim of internet theft is to steal your personal information and use it to then steal money out of your bank account or make purchases using your details.
- **Social Media Hack & Spamming** - Social media spamming comes when a person makes a fake account and becomes friends or followed by the average person. This then

gives the fake account the freedom to spam inboxes with bulk messaging, this can be done for spreading malware. Spamming can also spread malicious links created with the intent to harm, mislead or damage a user or their device. Clicking on the malicious link, which may be advertising a new iPhone or weight loss treatment, means you could be downloading malware which can lead to the theft of personal information. Another dark side of social media is the ability for malicious accounts to spam your output by constantly replying with negative messaging. A form of trolling.

- **Sales & Investment Fraud** - By sourcing the contact details and available account information for savings or investment account holders, fraudsters can adopt the persona of an investment broker.
- **Eavesdropping & Surveillance/Cyber Stalking** - Eavesdropping without the consent of the parties is a crime and can be done online or over the phone.
- **Data Diddling** - The action of skewing data entries in the user's system.
- **Identity Theft** - Criminals usually steal identity information of others such as credit card information, addresses, email addresses and more. With this information they can pretend to be someone else and create new bank accounts.
- **Child Soliciting & Abuse** - Child soliciting and abuse online is a type of cybercrime where criminals solicit children via chat rooms for the purpose of pornography. It can also come in forms of material that shows or describes sexual abuse towards children. A child is regarded as someone who is under the age of 18.
- **Software Piracy** - Software piracy is the unauthorized use and distribution of computer software.

How to address these crimes?

- **Cybercrime Prevention Act of 2012 otherwise known as Republic Act of 10175.**

The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting electronic commerce, and data processing, in the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

Privacy and confidentiality should be a major concern, especially for adolescents who may not be entirely aware about the consequences of sharing private information to the public.

- **Data Privacy Act of 2012 otherwise known as Republic Act 10173.**

It was created to protect people from invasion of privacy. The Act states that "It is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected. Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Be careful what you post, whom you interact with, and what you do online for it can create an impact on your presentation of yourself and to other people.