IT Social and Professional Issues

Group 5 Report Manuscript

Topics:

Sex and Technology
Technology and Privacy

Submitted by:

Aguila, Jessie Vincent R.
Arce, Christian Jay D.
Nietes, Kristel Joy E.
BSIT-SJ 4-2

Submitted to:

Prof. Marivill Sanchez

November 2022

Sex and Technology

Technology advancements and unregulated Internet usage have made men's sexual exploitation and abuse of women and children a global phenomenon. Modern technology, including live video chat, has made it possible for pimps to market a variety of sexually exploitative and harmful entertainment. The Internet allows perpetrators to share their experiences, justify their behavior, and advise and mentor less experienced males through an online network of support.

Human culture has always evolved in tandem with technological developments. And that includes sexuality. Robots, virtual reality, and telecommunication tech are all just beginning to be repurposed to fulfill sexual needs.

What is Sex Technology?

- Sex technology, often known as sex-tech or sextech, refers to technological advancements and technology-driven businesses that aim to improve, innovate, or in some other way alter human sexuality and/or the sexual experience.
- Sextech is technology, and technology-driven ventures, designed to enhance, innovate, and disrupt in every area of human sexuality and human sexual experience.

Impacts of Sex Technology

1. Pornography
2. Pleasure
3. New kinds of sex
4. New Ways To Meet Partners
5. New Kinds Of Partners
6. New Ways To Coordinate Hook Ups

Criticism of Sex Technology

→ Risk of addiction
→ Cyber-risk
→ Unnecessary or unlawful collection and use of sensitive personal data
→ Potential for harm and inequality caused by sex robots

References:

Froats, L. (2018). Digisexuality: Merging Sex and Technology. Discover Magazine. https://www.discovermagazine.com/mind/digisexuality-merging-sex-and-technology

Wikiwand Authors. (n.d.). Wikiwand - Sex technology. Wikiwand. https://www.wikiwand.com/en/Sex_technology

Child Pornography

- Child pornography is a form of **child sexual exploitation**.
- Child pornography refers to **any representation**, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, **of child engaged or involved in real or simulated explicit sexual activities**.
- Federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor *(persons less than 18 years old)*.
- Images of child pornography are also referred to as **Child Sexual Abuse Images**. Child pornography images are readily available through virtually every **Internet Technology**, including:
  - ✓ social networking websites,
  - ✓ file-sharing sites,
  - ✓ photo-sharing sites,
  - ✓ gaming devices, and
  - ✓ even mobile app

Laws Prohibiting Such Act

- **RA 9775**, otherwise known as the **Anti-Child Pornography Act of 2009**.
  - It prohibits the production, offering, distribution and possession of "child pornography.

> ***Section 2. Declaration of Policy***. - *The State recognizes the vital role of the youth in nation building and shall promote and protect their physical, moral, spiritual, intellectual, emotional, psychological and social well-being. Towards this end, the State shall:*
>
> *(a) Guarantee the fundamental rights of every child from all forms of neglect, cruelty and other conditions prejudicial to his/her development;*
>
> *(b) Protect every child from all forms of exploitation and abuse including, but not limited to:*
>
> *(1) the use of a child in pornographic performances and materials; and*
>
> *(2) the inducement or coercion of a child to engage or be involved in pornography through whatever means; and*
>
> *(c) Comply with international treaties to which the Philippines is a signatory or a State party concerning the rights of children which include, but not limited to, the Convention on the Rights of the Child, the Optional Protocol to the Convention on the Rights of the Child of the Child on the Sale of Children, Child Prostitution and Child Pornography, the International Labor Organization (ILO) Convention No.182 on the Elimination of the Worst Forms of Child Labor and the Convention Against Transnational Organized Crime.*

Related Recent News: Watch here https://youtu.be/5Qmh9488uHk

Philippines declares 'war' against Online Child Pornography

- New technologies, lax rules on foreign travelers, and pandemic lockdowns have been attributed as causes of the surge.
- A **2022 study by UNICEF, Interpol, and Ecpat International**, a global network of organizations against the sexual exploitation of children, also said that around **20 percent** of Internet users in the Philippines who are **between 12 and 17 years old** had been **sexually abused online**.

Cases of Child Pornography in the Philippines

→ In **2018, Australian sex offender Peter Gerard Scully** was jailed for life in the Philippines.
  - For running a cybersex den exploiting Filipino minors from the regional island of Mindanao.
  - He would record himself as he sexually abused the children, **even a one-year-old baby**
  - Then sell the videos to his clients in Europe.

→ In **2021, 4 convicted for online sexual exploitation of 11 kids in Cebu**
  - Four women were convicted after they pleaded “guilty” to online sexual exploitation of children in two separate cases in Lapu-Lapu City, Cebu.
  - The **first case** involved nine minors, two boys and seven girls, who were rescued in an operation conducted by the Women and Children Protection Center Visayas Field Unit (WCPC-VFU) on **March 21, 2019**.
  - The **second case** originated from a case buildup by the WCPC-VFU **on Feb. 26, 2018**, after “Annie” (not her real name) was caught offering her three-year-old son and a five-year-old girl for online sexual exploitation in exchange for money.

Definition of Terms

- **Child** – refers to a person below eighteen (18) years of age or over but is unable to fully take care of himself/herself from abuse, neglect, cruelty, exploitation or discrimination because of a physical or mental disability or condition.

- **Explicit Sexual Activity** – means actual or simulated: sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic area.

- **Internet Address** – refers to a website, bulletin board service, internet chat room or news group, or any other internet or shared network protocol address.

- **Internet Content Host** – refers to a person who hosts or who proposes to host internet content in the Philippines.

  Responsibilities of the Internet Content Host
  - ✓ *Never allow* the hosting of any type of child pornography on their website.
  - ✓ *Report any incidents of child pornography* within seven (7) days, together with the identity of anyone responsible for maintaining, hosting, disseminating, or otherwise supporting the website in question.
  - ✓ *Keep any evidence* for use in investigations and prosecutions by national authorities.

- **Internet Service Provider (ISP)** – refers to a person or entity that supplies or proposes to supply, an internet carriage service to the public.

  Responsibilities of the Internet Service Provider (ISP)
  - ✓ *Must contact* the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days of discovering facts and circumstances indicating that child pornography is being committed via its server or facility.
  - ✓ ISP *must keep any proof on hand* in case the appropriate authorities need it for an investigation or legal action.
  - ✓ *Must implement* available technologies, programs, or software to prevent access to or transmission of any type of child pornography.

- **Grooming** – refers to the act of preparing a child or someone who the offender believes to be a child for sexual activity or sexual relationship by communicating any form of child pornography. It includes online enticement or enticement through any other means.
- **Luring** – refers to the act of communicating, by means of a computer system, with a child or someone who the offender believes to be a child for the purpose of facilitating the commission of sexual activity or production of any form of child pornography.
- **Pandering** – refers to the act of offering, advertising, promoting, representing or distributing through any means any material or purported material that is intended to cause another to believe that the material or purported material contains any form of child pornography, regardless of the actual content of the material or purported material.

References:

Auto, H. (2022). Philippines declares "war" against online child pornography. The Straits Times. https://www.straitstimes.com/asia/se-asia/philippines-declares-war-against-online-child-pornography

Official Gazette of the Republic of the Philippines. (2009). Republic Act No. 9775 | GOVPH. https://www.officialgazette.gov.ph/2009/11/17/republic-act-no-9775-s-2009/

U.S. Department of Justice Author. (2020). Child Pornography. U.S. Department of Justice. https://www.justice.gov/criminal-ceos/child-pornography

Moaje, M. (2021). 4 convicted for online sexual exploitation of 11 kids in Cebu. Philippine News Agency. https://www.pna.gov.ph/articles/1132331

Prostitution has moved "from the street to the Internet," where pimps recruit young girls via Snapchat and Instagram before prostituting them in apartments rented on Airbnb.

Virtual Prostitution

- An action in which one engages in sexual activity with a partner whom one has never seen or met in person before. They **typically connect online**.
- It may also refer to obscene and indecent live shows or interactive methods **through the computer, the Internet and other electronic devices**.
- Prostitution is promoted online and men's experiences purchasing women and children for prostitution are compiled in online forums.
- **Example:** Having an *OnlyFans* is basically virtual prostitution.

Case/s of Virtual Prostitution

Apps like ***Facebook*** and ***Tinder*** are **fueling the "soaring industry" of online prostitution and sexual exploitation**, according to a worldwide study published by a French anti-prostitution group.

→ In **Israel**, dating app **Tinder** is the most popular tool to find prostitutes.
→ In **Zambia** students in cybercafes join **WhatsApp** and **Facebook groups** to connect with prostitutes and pimps in a few clicks.
→ In **France**, gangs contact underage girls from *"welfare homes and high schools"* on social networks such as **Facebook** and **Snapchat**, promising *"opportunities to make money very quickly"* before posting online advertisements and prostituting them.
→ This is happening around the world, from restrictive countries like **China**, to **Germany** where legislation is more lenient

→ In **2021**, *"Of victims and saviors: Sex work amid the pandemic"***.** Delilah, 23 years old, has been doing sex work since she was 18*. (Note: Names of sex workers interviewed for this article are pseudonyms or internet personae.)*

> *She finds it odd to be asked what sex work means to her. "I think people mean well when they ask me that," she said, "but the thing is, we don't normally ask that question to other workers."*
>
> *While she admitted that she enjoys the work because she gets to explore her sexuality and identity, she still believes that it is just a job. "I don't think I have to feel empowered to do it," she said, "and I don't think it has to be any special."*
> *…*
> *Despite all this, she said she believes that the pandemic-induced rise in online sex work can be a good thing because more individuals get to explore their sexuality and even earn from it. "It's like experimenting in the kitchen," she said, "where you cook something, sell it, and see if people like it."*

Definition of Terms

- **Prostitution** – the act or practice of engaging in promiscuous sexual relations especially for money. The selling of sexual services is yet another controversial sexual behavior.
- **Prostitute** – a person who engages in sexual intercourse or other sex acts for money, sex worker.
- **Prostitution Solicitor** – refer to a person who invites, approaches, or communicates with the sought online and offers to pay for a sexual act.
- **Cyber Prostitution** – involves obscene and indecent acts evolving around virtual sexual stimulation and/or intercourse in exchange of money and/or profit.

Related Recent News: Watch here https://youtu.be/Jrmf0WEchKw

References:

9.4 Prostitution – Social Problems. (2016). Pressbooks. https://open.lib.umn.edu/socialproblems/chapter/9-4-prostitution/

Acosta, R. (2021). Of victims and saviors: Sex work amid the pandemic. INQUIRER.net. https://newsinfo.inquirer.net/1387176/of-victims-and-saviors-sex-work-amid-the-pandemic

Agence France-Presse. (2019). Apps, social media fuel 'booming' online prostitution – study. RAPPLER. https://www.rappler.com/technology/232336-study-apps-social-media-fuel-booming-online-prostitution/

Henion, A., & Finn, M. (2016). Prostitution has gone online – and pimps are thriving. MSUToday | Michigan State University. https://msutoday.msu.edu/news/2016/prostitution-has-gone-online-and-pimps-are-thriving

Hughes, D. M. (2004). Prostitution Online. Journal of Trauma Practice, 2(3–4), 115–131. https://doi.org/10.1300/j189v02n03_06

Cyber Sex

- Cybersex is fundamentally virtual and does not involve person-to-person physical contact.
- Cybersex is any type of sexual activity that occurs **virtually between two or more individuals** including:
  - sexting,
  - sharing sexual images or videos with a partner,
  - webcam sex,
  - chatroom sex or visiting sexually oriented chat rooms
  - reading and writing sexually explicit letters and stories
  - e-mailing to set up personal meetings with someone
  - placing ads to meet sexual partners

- **Spin-offs of cybersex activities** are phone sex with people met online, and online affairs that progress to real or offline affairs.
- Cybersex, **also called computer sex**, **Internet sex**, **netsex** and, commonly, **cyber** or **cybering.**

Different Types of Cybersex

1. **Sexting**
   - It involves sending sexually explicit messages and/or photos by phone to a partner.

2. **Phone Sex**
   - It usually entails verbally describing sexual activity over the phone to another person and listening to their descriptions.

3. **Webcam Sex**
   - It allows a person to masturbate with one or more individuals over live video, whether on their phone or on an online video conferencing platform.

4. **Chatroom Sex**
   - It is practiced by people in online chatrooms, frequently with unknown partners.
   - There are cybersex chat rooms, streams that need to be purchased, and spaces where you have one on one time.

5. **Virtual Reality Sex**
   - may increase in popularity as virtual reality systems become more affordable and widespread.
   - A **virtual reality headset** is a device that is worn on a person's head that creates a 3-dimensional virtual experience for the wearer.
   - In virtual reality sex, this experience could **utilize 3-D pornography**.

6. **Alternate Reality Sex**
   - sex that takes place between two digital avatars in an online community.
   - One of the **most popular online communities** at this time is called **Second Life**.

7. **Connected Sex Toys, or Teledildonics**
   - These are sex toys that are controlled through an internet-connected device like a smartphone and can therefore be controlled by long-distance sex partners.
   - The word **teledildonics** refers to the use of connected sex toys

How Safe is Cybersex?

- Cybersex is **considered a safe form of sex**.
- Cybersex users should be aware that sharing private sexually explicit photos or films with a partner exposes them to the possibility of that partner disclosing them to third parties.
- People who engage in cybersex with strangers online should keep in mind that they may be able to simply lie about their age, gender, and other personal details.

Three Overall Types Of Cybersex Users:

1. **Recreational Users**
   - Refers to those who occasionally engage in Internet sex.

2. **At-Risk Users**
   - Refers to those people who usually have underlying stress or unhappiness and are vulnerable to addictive distractions.

3. **Sexually Addicted Users**
   - It describes those who engage in cybersex regardless of the consequences.

Advantages of Cybersex *(Tanimoonwo & Hassan, 2013)*

- ✓ Cybersex allows real-life partners who are physically separated to continue to be sexually intimate.
- ✓ Since cybersex can satisfy some sexual desires without the risk of a sexually transmitted disease (STD) or pregnancy, it is a physically safe way for young people *(such as with teenagers)* to experiment with sexual thoughts and emotions.
- ✓ Cybersex allows for sexual exploration.
  - It takes less effort and fewer resources on the Internet than in real life to connect to a person like oneself or with whom a more meaningful relationship is possible.
- ✓ Cybersex allows each user to take control.

Disadvantages of Cybersex *(Jones & Tuttle, 2012)*

- **Possibility of Cyber Sex Addiction**
  - Unlike other forms of addictive behavior, such as gambling disorder and substance disorders, **cybersex addiction is not an officially recognized disorder** and therefore mental health professionals would not give a diagnosis to people who show the signs of this kind of addiction.

  - **Compulsive Cybersex** use can be labeled an addiction because it often contains the **main components of most addictions**:
    - salience,
    - mood modification,
    - tolerance,
    - withdrawal symptoms,
    - conflict, and
    - relapse

- **Privacy concerns** are a difficulty with cybersex, since participants may log or record the interaction without the other's knowledge, and possibly disclose it to others or the public.

Related Recent News: Watch here https://youtu.be/M7m6whRA5mw

References:

Black, J. (152 C.E.). Cyber Sex. prezi.com. https://prezi.com/dyxsxtedwis4/cyber-sex/?frame=b7a21c44a68f211c7048d87f2902edf3e0491d67

Boskey, E. (2020). Cybersex: Types, Benefits, and Risks. Verywell Health. https://www.verywellhealth.com/cybersex-pros-cons-4800752

Delineation of Responsibilities in the Fight Against the Occurrence and Proliferation of Cyber Pornography / Cyber Prostitution. (2006). dswd.gov.ph. https://www.dswd.gov.ph/issuances/mcs/mc_2006-005.pdf

Shoengold, MD, S. (2020). What Is Cybersex?: Center for Female and Male Sexual Medicine: Urologists. Center for Female and Male Sexual Medicine. https://www.njsexualmedicine.com/blog/what-is-cybersex

VanBuren, K. (2021). Cybersex: Types, Benefits, How to Do It Safely. Marriage Advice - Expert Marriage Tips & Advice. https://www.marriage.com/advice/intimacy/what-is-cybersex/

Action Taken by the Local Government for both Cybersex and Virtual Prostitution

- **Republic Act No. 10175** or this Act shall be known as the **"Cybercrime Prevention Act of 2012".**
  - This Act was signed by the former President of the Philippines *Mr. Benigno Aquino* on **September 12th of 2012**.
  - The **original goal** of this Act was to penalize acts like cybersex, child pornography, identity theft etc.

- **January 16, 2017**, former President Duterte loathes the **proliferation of porn websites**.
  - **Republic Act No. 9775**, often known as the **Anti-Child Pornography Law**, was violated by websites, according to Information and Communications Technology Secretary Rodolfo Salalima.
  - On **January 15, 2017**, visitors of the popular *pornhub.com* and *xvideos.com* were surprised that they **were prohibited from accessing both porn sites**. It began a few days after *pornhub.com* indicated that Filipinos were its top site users, consuming an **average of 12 minutes and 45 seconds watching sex movies**.

References:

Garg, R. (2022). All you need to know about the Cybercrime Prevention Act in the Philippines. iPleaders. https://blog.ipleaders.in/all-you-need-to-know-about-the-cybercrime-prevention-act-in-the-philippines/

Official Gazette of the Republic of the Philippines. (2012). Republic Act No. 10175 | GOVPH. https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Ramos, M. (2017). Shutdown of websites part of drive vs child porn – Palace. INQUIRER.net. https://newsinfo.inquirer.net/862592/shutdown-of-websites-part-of-drive-vs-child-porn-palace

---

Technology and the Internet have changed a lot of things in our world, including human communication and relationships.

Online relationships are now widely utilized in a world dominated by smart phones and the internet, where everyone is connected to one another. In addition to articles concerning cybercrimes, we frequently read news stories about couples who met online and were married.

Online Relationships

- Online romantic relationships, also known as **internet relationships.**
- It is a way of **starting a romantic relationship on the internet**, by giving information about yourself or replying to someone else's information.
- In online relationships **people can be partially or fully anonymous**: people can conceal their true identity or important aspects of it.

    - **Anonymity** in online relationships **facilitates self-disclosure** as it reduces the risks involved in disclosing intimate information about oneself.
        - **People can express themselves more freely since they are more anonymous, less accountable, and hence less vulnerable**.
        - In the **anonymity (or semi anonymity) of cyberspace**, it is much easier to disclose one's true feelings.

- People can start an online relationship for any reason. The internet creates a convenient atmosphere were busy people can meet those with common interests and lifestyles.
- The relationship may be for friendship, companionship, romance or even business.

Types of Online/Virtual Relationships

1. **Online Dating**
    - The **most common type of virtual relationship**.
    - Today finding someone to get into a virtual or real relationship is as easy as finding a red dress on an e-commerce website.
    - **People used common apps and websites** like:
        - Tinder,
        - Bumble,
        - Hinge,
        - Muddy Match,
        - Raya,
        - HER,
        - JSwipe,
        - Omegle, etc., among others for online dating.

- **Advantages of Online Dating**
  1. **Saves Time**
     - The dating app lets you talk and get to know the person before actually going on the date.
     - If you see any obvious red flags, you can cancel the date and save your precious time.

  2. **Access to Plenty of Options**
     - Online dating gives you access to more options than you will ever find in real life along with a chance to get to know their personality traits.
     - The **biggest advantage** is that you can talk to multiple people at the same time.

       Examples:
       - If **you want to date someone who likes travelling a lot**, dating apps will give you a bunch of options.
       - If **you are not looking for long term relationships**, dating apps will give you the chance to connect with people who want the same.

  3. **Narrows Down Options**
     - Online dating helps you to narrow down your options from a hundred to five in as little time as possible.

       Examples:
       - You have the option to erase a person from your life with one swipe in the other direction has to be the best thing about online dating.
       - You can talk to a person, get to know them, and unmatched with them if you don't like them or find it uncomfortable to talk to them.

     - However, you will have to be upfront about your intentions and expectations to make it work.
     - You can be honest and experiment to figure out what you want.

  4. **You Can Go Slow**
     - The advantage of online dating is that you are not expected to stick to a timeframe.
     - The getting-to-know-each-other phase can be as long as you want.
     - You can talk to the person you are interested in every day or once a week.

- **Disadvantages of Online Dating**
  1. **Weak Grip On Reality**
     - The photos you see on a dating app can be far from how the person looks in real life.

       Example:
       - People may put up old, younger photographs or edited versions.
       - Even if the photos are not edited, you cannot assume their body language or mannerisms from a photo.

     - If you are someone who cares a lot about physical appearance, photos can be deceiving.
     - If you are someone who cares about body language and mannerisms, photos leave you with nothing

  2. **Hard To Detect The Truth**
     - The possibilities are endless in online dating. In a good way and a bad way.
     - In the realm of online dating, you **could potentially run into your**:
       - ✓ Perfect Match,
       - ✓ Serial Killer, or
       - ✓ Sexual Predator.

     - You may be fooled if the individual is skilled at lying.
     - It's likely that your perfect match isn't very good at texting, and you'll perceive him or her as uninterested.

  3. **Hard to track down the other user**
     - When you become Ghosted/Scammed/abused and blocked by a person in online dating, it's impossible to track down the other user since the platform won't share any details even if you contact their helpdesk due to privacy restrictions.

2. **Social Networking**
   - In a time like today, when people don't have time to make new friends in person or meet up with their friends and catch up on old times, people depend on **social networking sites** like:
     - Facebook,
     - Twitter,
     - Instagram,
     - LinkedIn, etc. to **make new friends and interact with old ones**.

3. **Online Gaming**
   - People who love gaming tend to play games on the net and end up meeting many anonymous gamers.

4. **Chatrooms & Forums**
   - There are many chatrooms & forums where people post their issues and get responses from random strangers on the internet.
   - **Forums** not only are a very good platform for discussion, but they're also a very good platform to **get reliable information and guidance**.

5. **Business Partnerships and Professional Relationships**
   - Companies and institutions that have partnerships or dealings with people who are in a different city or country **use the internet in an efficient way to connect** with them when a face-to-face meeting isn't possible.
   - These institutions and companies maintain healthy and professional virtual relationships with people via the internet.

Gen Z and Millennial Dating Terminologies that's Commonly Used on Online Platforms

- **Breadcrumbing** – when you flirt with someone and make them feel like they have a chance of going on a date with you, when in reality, you know you are staying single and just need them for an ego boost.

- **Ghosting** – his is when someone cuts off all communication with you without warning. One day they're holding your hand, the next you don't even know if they're still in the same country as you.

- **Pink flag** – a trait your partner has that's a bit weird but not bad enough to be a red flag yet. It deserves more investigating. For example, if your partner has never posted you on social media, it's a pink flag if he never posts on social - but a red flag if he constantly updates his feed.

- **Green Flag** – coined to describe positive qualities in potential partners in relationships, such as kindness, loyalty, patience, supportive, and a good sense of humor.

- **Red flag** – a warning sign that appears during a date that could indicate a problem, miscommunication, or challenge in the future.

- **Benching** – the act of keeping someone interested but not really following through.
  How it's done: they'll flirt with you online, maybe even in person, but all those plans to go out never actually happen. You're just kept "on the bench."

- **Fading** – the act of gradually disappearing from a person's life.
  How it's done: the dm's, texts, and calls that were once frequent start to slowly trickle down to nothing.

- **Zombieing** – refers to an ex who comes back into your life, most often after ghosting you.

Benefits of Online Relationships

1. **Meet and connect with new people**
   - You can meet with new people that you would otherwise not otherwise meet.

2. **Get to know someone before you meet in person**
   - You can get to know someone and form a deeper connection with them before you meet in person.

3. **Online relationships can rise above everyday stresses**
   - Connecting with someone online can be a great way to create positive connections and relieve stress.

4. **Collaborate and work with other people**
   - You can share a joke with a colleague on the other side of the world and work more effectively with them.

5. **Less Conflict**
   - People tend to fight less when in a virtual relationship as they don't get complete and verified information.

Risks of Online Relationships

1. **People may not be who they say they are**
   - It can be easier for someone to pretend to be someone else in order to abuse, scam or extort money from you.

2. **Tactics such as trickery and flattery**
   - People can use tactics to get you to do things you would otherwise not do.

3. **Messages and images may be shared or copied without your consent**
   - The person you are in an online relationship with may share your messages or images without your permission.

4. **Unwanted contact or contact from strangers**
   - You could receive unwanted communication or communication from people you do not know.

5. **Addictive**
   - People get so used to it that it becomes difficult for them to meet & communicate with people in real life, and they tend to get uncomfortable with physical contact and lose confidence. Sometimes it also becomes impossible for them to handle a real-life relationship.

Reasons for relationship formation often differ between the genders.

- **For example:**
  - Cooper and Sportolari (1997) and Cooper (1998) hypothesized that **men** are attracted to online relationships because they develop in a less pressured way where sexual intimacy occurs due to emotional attachment rather than sexual connection. An alternative explanation is that the anonymity on the internet may allow men to express their sexual selves more openly or compulsively.
  - **Women** on the other hand tend to meet people in chat rooms or newsgroups and have started internet relationships for networking or emotional support.

According to McKenna, Green, and Gleason (2002) found that relationships are most successful when participants are able to show aspects of their “true self” to their partner. In face-to-face interactions, a person's "real self" may not always be apparent to others, but it is thought to be the fundamental qualities that they believe define them. It is believed that the “true self” may be easier to express in computer-mediated communication because of the lack of social cues that often distract people from these characteristics.

References:

BP World Bureau. (2019). Advantages And Disadvantages Of Online Dating - Beyond Pink World. Beyond Pink World. https://www.beyondpinkworld.com/featurestories/relationship/advantages-disadvantages-onlin-7905

eSafety Authors. (n.d.). Online Relationships. eSafety. https://www.esafety.gov.au/key-issues/esafety-guide/online-relationships

Manchanda, J. (2016). Relationships Over The Net. Youth Incorporated Magazine. https://youthincmag.com/virtual-relationships

Online Relationships. (2015). Science Direct. https://www.sciencedirect.com/topics/social-sciences/online-relationships

Rohan, L., & Reitsma, B. (2022). Gen Z v Millennials: The Gen Z sex and dating terms you probably don’t know. NZ Herald. https://www.nzherald.co.nz/lifestyle/gen-z-v-millennials-the-gen-z-sex-and-dating-terms-you-probably-dont-know/TXVAJRAEOPBR6V72YYXTC6EGRE/

Savoie, G. (2022). Best Dating Apps. Brides. https://www.brides.com/best-dating-apps-5105328

The Dynamics of Online Relationship Formation. (n.d.). webspace.ship.edu. http://webspace.ship.edu/jacamp/psyberpsych/dating/Subtopic2.htm

Technology and Privacy

Technology and privacy have undergone a transformation over the past few years, resulting in an environment that is both risky and promising. And human beings value their privacy and the protection of their personal sphere of life. They value some control over who knows what about them. They certainly do not want their personal information to be accessible to just anyone at any time. However, recent developments in information technology have put privacy at risk, decreased the level of control over personal data, and increased the risk of access to confidential data, which may have several effects.

What is Privacy?

- Privacy is a **fundamental right**, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.
- Privacy **helps us establish boundaries to limit** who has access to our bodies, places, and things, as well as our communications and our information.

What is Data Privacy?

- Data privacy, also called **Information Privacy**, is an aspect of data protection that addresses the proper storage, access, retention, immutability, and security of sensitive data.
- Data privacy is **not a single concept or approach**. Instead, **it's a discipline involving** rules, practices, guidelines, and tools to help organizations establish and maintain required levels of privacy compliance.
- Data privacy is typically **associated with the proper handling of personal data** or **Personally Identifiable Information (PII)**

    - **Personally Identifiable Information (PII)** uses data to confirm an individual's identity. It can be sensitive or non-sensitive.

        - **Sensitive** personal information includes legal statistics such as:
            - Full name
            - Social Security Number (SSN)
            - Driver's license
            - Mailing address
            - Credit card information
            - Passport information
            - Financial information
            - Medical records

- **Non-sensitive** or indirect PII is easily accessible from public sources like phonebooks, the Internet, and corporate directories.
  Examples of non-sensitive or indirect PII include:
  - Zip code
  - Race
  - Gender
  - Date of birth
  - Place of birth
  - Religion

Definition of Terms

- **Big Data** – is being collected, analyzed, and processed by businesses and shared with other companies.
- **Data Privacy** – focuses on the rights of individuals. It focuses on how to collect, process, share, archive, and delete the data in accordance with the law.
- **Data Security** – includes a set of standards and different safeguards and measures that an organization is taking in order to prevent any third party from unauthorized access to digital data, or any intentional or unintentional alteration, deletion, or disclosure of data.

References:

Agre, P. (Ed.). (1997). Technology and Privacy. The New Landscape. https://pages.gseis.ucla.edu/faculty/agre/landscape.html

Bigelow, S. J. (2022). data privacy (information privacy). SearchCIO. https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy

Data Privacy Manager Author. (2022). 5 things you need to know about Data Privacy. Data Privacy Manager. https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/

Frankenfield, J. (2022). What Is Personally Identifiable Information (PII)? Types and Examples. Investopedia. https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp

Privacy International Authors. (2017). What Is Privacy? Privacy International. https://privacyinternational.org/explainer/56/what-privacy

Stanford Encyclopedia of Philosophy. (2019). Privacy and Information Technology. https://plato.stanford.edu/entries/it-privacy/

Identity Theft / Impersonation

- **Identity Theft** in social networks refers to accounts that use the name, image, or other identifying elements of a person, company, or organization for fraudulent purposes.
- Generally speaking, **Impersonation** is the **act when a person pretends to be someone else** on social media platforms.
- Identity theft is when someone uses another person's financial or personal data, usually for monetary gain.
- **Social Media Impersonation** differs from other legitimate uses of a brand or person, such as:
  - Fan Accounts,
  - Parodies or Criticism, and
  - Information Pages

5 Common Types of Identity Theft / Impersonation

1. **Financial Identity Theft**
   - Financial identity theft is when one person uses another's personal data for financial benefit.
   - This is the **most common form of identity theft**.
   - Financial identity theft can take **Multiple Forms**, including:
     - **Fraudsters may use your credit card information to buy things.**
       - We all love to shop online — even criminals. Unfortunately, this issue has become especially prevalent thanks to online shopping during the COVID-19 pandemic.
     - **Hackers may steal funds from your bank account.**
       - Sometimes, the amount might be so small that it seems inconsequential, totaling just a few dollars. However, criminals can rack up millions in damages if they target enough people in this way.
     - **Criminals may open new accounts using your Social Security number and other data.**
       - For example, a person may use your data to open a new line of credit. They then run through the credit line, leaving you to foot the bill.
   - The **good news** is that it's easy to protect yourself against financial identity theft by checking your bank accounts, credit card statements, and bills.
   - **If you see an unexplained charge**, contact your credit card company or bank immediately to report it.

2. **Medical Identity Theft**
   - This might not seem like a real form of identity theft, but it happens.
   - Medical identity theft is when a **criminal poses as another person to obtain health care services**.
   - In fact, **fraudsters may use your name and insurance information to**:
     - **Get prescriptions for drugs**.
     - **Access medical services**, from checkups to costly surgeries.
     - **Obtain medical devices and supplies**, such as wheelchairs or hearing aids.
   - This can result in you having bills for prescriptions, services, or devices you didn't need, ask for, or even receive. Your health care and insurance records may even have these things added to them.
   - An **inaccurate medical record** can make it harder for you to get the care you need in the future and even impact insurance coverage.

- You can help minimize the risk of medical identity theft by **regularly reviewing your medical claims**.
- **Contact your insurer** if you see unfamiliar procedures, prescriptions, or services.

3. Criminal Identity Theft

- Criminal identity theft occurs when **a person arrested by law enforcement uses someone else's name** instead of providing theirs.
- They might be able to pass this off by **creating a fake ID or using a stolen ID**, like your driver's license, to show to the police.
- This type of fraud can be difficult to detect until the **Consequences are Evident**, like:
    - **You receive a court summons.**
        - For example, the courts may issue a summons if a criminal uses your ID for unpaid parking tickets.
    - **A bench warrant is issued for your arrest.**
        - Unresolved problems like unpaid parking tickets can also result in a judge issuing a bench warrant. You may then be taken into custody at any time, even during a routine traffic stop.
    - **A background check is issued.**
        - Sometimes, police will keep an identity theft victim in their database, noting it as an alias for the real criminal.
        - This can result in a false criminal record showing up on your background check. This can cause problems with potential landlords and employers.
- You can help protect yourself against criminal identity theft by **safeguarding your ID**.
- If your license or state-issued ID is lost or stolen, report it to the local Department of Motor Vehicles (DMV) and law enforcement.

4. Synthetic Identity Theft

- Synthetic identity theft is a type of fraud in which a **criminal combines real (usually stolen) and fake information to create a new identity**, which is used to open fraudulent accounts and make fraudulent purchases.
    - Fraudsters may use data like birthdates, addresses, and Social Security numbers from real people, blending them to create a fake profile.
- Synthetic identity theft allows the criminal to steal money from any credit card companies or lenders who extend credit based on the fake identity.

- The **most important thing** about synthetic identity theft is **knowing the signs and acting fast**.
- Keep an eye out for any mail with your address on it but addressed to a different name and phone calls or mail about new credit accounts. You can further protect yourself by regularly checking your credit reports for unexplained changes and placing a security freeze on them.

5. **Child Identity Theft**
   - When someone **uses a child's identity for various forms of personal gain**.
   - This is common, as children typically do not have information associated with them that could pose obstacles for the perpetrator.
   - This is often easier than targeting an adult because most kids don't have credit reports or financial accounts, making them a clean slate.
   - By this point, the issue may have been escalating for years. So, it's important as a parent to be aware of child identity theft. The best way to do this is to check whether your child has a credit report with any of the three big credit bureaus *(TransUnion, Equifax, and Experian)*. If so, review the report and report any fraudulent activity. You can also place a freeze on your child's credit report to help minimize the risk of future fraud.

Some of the Most Common Ways Scammers have been Impersonating Brands

1. Phishing
2. Counterfeiting
3. Fake News
4. Scams

How do you know if you're a Victim of Identity Theft?

- Anyone can be a victim of identity theft. **Children and the elderly** are particularly vulnerable to identity theft as they may not understand specific situations, bills, and their care and finances are handled by others.
  1. You get a fraud alert from a financial institution.
  2. There are unexplained changes in your credit score.
  3. There are changes to your financial accounts.
  4. A loan or credit card application is denied.
  5. You get phone calls from debt collectors.
  6. You get unfamiliar mail.
  7. You experience tax return

Laws Prohibiting Such Act

- The Philippines enacted in **2012 Republic Act No. 10175**, or otherwise known as the **Cybercrime Prevention Act ("RA 10175")**, which enumerates cybercrimes and provides for their penalties.
  - **RA 10175** penalizes any person found guilty of computer-related identity theft with imprisonment of:
    - **prison mayor (6 years and 1 day to 12 years)** or
    - a fine of at least **Two hundred thousand pesos (PhP200,000.00) up to a maximum amount** commensurate to the damage incurred or both.
  - Under **RA 10175**, **Computer-related Identity Theft** is the intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right.

Related Recent News: Watch here
https://www.youtube.com/watch?v=qaLVIYaSF90
https://www.youtube.com/watch?v=N1TNdTiVjTE

References:

Hussain, A. (2022). What Is Identity Theft? Definition, Types, and Examples. Investopedia. https://www.investopedia.com/terms/i/identitytheft.asp

McAfee Authors. (2022). 5 Common Types of Identity Theft. McAfee Blog. https://www.mcafee.com/blogs/privacy-identity-protection/5-common-types-of-identity-theft/

Nicolas & De Vega Law Authors. (n.d.). Computer-related Identity Theft is a Serious Cyber Crime. Nicolas & De Vega Law. https://ndvlaw.com/computer-related-identity-theft-is-a-serious-cyber-crime/

Social media impersonation: What is it? How to stop it. (2022). Red Points. https://www.redpoints.com/blog/social-media-impersonation-what-is-it-how-to-stop-it/

Monitoring vs. Intrusion to Privacy

1. **Monitoring**
   - **Monitoring Technology** means any hardware, software, or application utilized in conjunction with an electronic device that **can cause the electronic device to capture**, **monitor**, **record**, or **report information about user activities** with or without the user's knowledge.
   - Monitoring technology equipment **includes tools** such as:
     - alarms,
     - sensors,
     - remote monitors and other devices.

- **Back in 2007**, it would have been hard to imagine the revolution of useful apps and services that smartphones ushered in. But they came with a cost in terms of intrusiveness and loss of privacy. As computer scientists who study data management and privacy, **they find that with internet connectivity extended to devices in homes, offices and cities, privacy is in more danger than ever**.

- **Internet of Things**
  - Online or offline, Smart devices collect a wide range of data about their users.
  - To do their magic, they need the internet to reach out for help and correlate data.
    - **For example**, some Wi-Fi routers can collect information about users' whereabouts in the home and even coordinate with other smart devices to sense motion.
  - Workplaces, malls, and cities are also becoming smarter, and the smart devices in those places have similar requirements.
  - In fact, the **Internet of Things (IoT) is already widely used** in transport and logistics, agriculture and farming, and industry automation.
  - There were around 22 billion internet-connected devices in use around the world in 2018, and the number is projected to grow to over 50 billion by 2030.

  - On the **less obvious end of the spectrum**, things like:
    - **Smart TVs:** use cameras and microphones to spy on users,
    - **Smart Lightbulbs**: track your sleep and heart rate, and
    - **Smart Vacuum Cleaners:** recognize objects in your home and map every inch of it.

  - **As a User**, it is important to make an informed decision by understanding the trade-offs between privacy and comfort when buying, installing and using an internet-connected device.
  - Studies have shown that, for example, owners of smart home personal assistants have an incomplete understanding of what data the devices collect, where the data is stored and who can access it.

- **Why do websites track browsing activity?**
  - In some cases, it's simply to make your **browsing experience faster and more convenient**.
  - Also used to **determine your browsing habits and preferences**—information that is frequently used by advertisers in determining what ads to show you online.

- Here are a **Few Common Examples** of when a website might track your online activity.
    1. **Video sites** like **YouTube** and **Netflix** collect information on the videos you watch, which helps them suggest more videos you might like.

    2. **Online stores** like **Amazon** and **eBay** keep a record of the different items you view and purchase, which helps them suggest other products you may want to buy.

    3. **Search engines** like **Google** keep a record of the things you search for. This can help them suggest more relevant searches, but it can also be used for advertising purposes.
        - **For example**, if you search for a coffeemaker on Google, you might see ads for coffeemakers on other websites in the future.

- **How do cookies work?**
    - **What are Cookies?**
        → It is a piece of data from a website that is stored within a web browser that the website can retrieve later.
        → Cookies are used to tell the server that users have returned to a particular website.
        → The term "cookie" was coined by web-browser programmer **Lou Montulli.**

    - **Cookies also store information** such as
        ☑ Shopping Cart Contents,
        ☑ Registration or Login Credentials, and
        ☑ User Preferences.

    - **Cookies don't pose a serious risk to your online security**—you're unlikely to acquire malware or expose sensitive financial information by using cookies.
    - Advertisers use cookies to **track user activity across sites** so they can better target ads. Advertisers often **use third-party cookies**.
        - Third-party cookies enable entities to track user behavior in a way the user might not be aware of -- and they may **infringe upon the user's privacy**.
        - This is a privacy concern for many who don't want to be tracked or have their browsing habits shared.

2. **Intrusion to Privacy**
   - Invasion of Privacy is the **intrusion of an unwanted individual** or business into the private affairs of a person without consent.
   - Invasion of Privacy is the **violation of a person's freedom** to control their image and be left undisturbed in private spaces and conversations.

   - **Four Types of Situations that are considered invasion of privacy such that you can file a civil lawsuit:**
     1. **Misappropriation of a person's name or likeness for the defendant's benefit.**
        - This occurs when a business uses a person's name or image in marketing materials without consent.

     2. **Intruding on someone's seclusion.**
        - Intentionally violating someone's privacy when they're in solitude or seclusion could be grounds for a lawsuit.

     3. **Portraying someone in a false light in the public eye.**
        - This occurs if something you say or publish puts a person in a negative light.

     4. **Publicly disclosing private facts.**
        - Whenever you disclose sensitive, embarrassing, or private information about a person, you could be at risk of invasion of privacy.
        - You can get sued whenever you:
          - ☑ Disclose information about a person's private life
          - ☑ Say or write something that is offensive to a reasonable person
          - ☑ Make revelations that do not legitimately concern the public

   - **Definition of Terms**
     - **Tort** – is a wrongful act that causes injury or loss to someone resulting in legal responsibility for the wrongful act.
     - **Deception** – first type of invasion of privacy, occurs when an employer collects information, he claims is for one reason but uses it for another reason, which could result in the employee's termination.
     - **Violation of Confidentiality** – second type of invasion of privacy, this occurs when information given in confidence is then given to a third party.
     - **Intrusion** – third type of invasion of privacy, this occurs when an employer intrudes in an employee's private life.

Laws in the Philippines that is Related to Such Act

- In 2012, the Philippines passed **Republic Act No. 10173** or known as the **"Data Privacy Act of 2012"**

> *SEC. 2. Declaration of Policy. – 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.*

- The Data Privacy Act is broadly applicable to individuals and legal entities that process personal information, with some exceptions.

- The Data Privacy Act of 2012 (DPA) is a **legal measure implemented in response to the growing need for data security and protection** in today's digital climate. It upholds the rights of Filipino citizens to be in control of how organizations store, use, transmit, and handle their personal data, and ensures that they are protected by law in the event that their information is compromised.

Cybercrime is an ongoing threat. You might think that the only form of cybercrime you have to worry about is hackers stealing your financial information. Anyone using the internet should exercise some basic precautions.

- Be Smart with Devices.
- When visiting unauthorized websites, keep your information secure.
- Never give out personal information to a stranger.
- Enforce concrete security and keep it up to date.

References:

A Summary of RA No. 10173 or the Data Privacy Act of 2012. (2022). ECC International. https://eccinternational.com/ra-10173-data-privacy-summary/

BlueVoyant. (2022). What is Cybercrime? Types and Prevention. https://www.bluevoyant.com/blog/cybercrime-types-and-prevention

GCF Global Authors. (n.d.). Internet Safety: Understanding Browser Tracking. GCFGlobal.org. https://edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/

Gold Star Law Authors. (2018). Invasion of Privacy. Gold Star Law. https://www.goldstarlaw.com/our-focus/invasion-of-privacy/

Insureon Authors. (2022). Invasion of privacy. Insureon. https://www.insureon.com/insurance-glossary/invasion-of-privacy

Intellipaat Authors. (2022). What is Cybercrime? Types and Prevention. Intellipaat Blog. https://intellipaat.com/blog/what-is-cybercrime/

Kerner, S. M. (2021). cookie. SearchSoftwareQuality. https://www.techtarget.com/searchsoftwarequality/definition/cookie

Microsoft. (n.d.). The Data Privacy Act. https://www.microsoft.com/en-ph/dpa-trustcenter/privacy/dpaoverview

Monitoring technology Definition. (2022). Law Insider. https://www.lawinsider.com/dictionary/monitoring-technology

National Privacy Commission. (n.d.). Republic Act 10173 – Data Privacy Act of 2012. https://www.privacy.gov.ph/data-privacy-act/

Winston, K. (2016). Take Online Courses. Earn College Credit. Research Schools, Degrees & Careers. Study.com. https://study.com/academy/lesson/what-is-invasion-of-privacy-definition-examples.htm l

Yus, R., & Pappachan, P. (2022). Smart devices spy on you – 2 computer scientists explain how the Internet of Things can violate your privacy. The Conversation. https://theconversation.com/smart-devices-spy-on-you-2-computer-scientists-explain-how-the-internet-of-things-can-violate-your-privacy-174579