



# EMERGING DATA PROTECTION CHALLENGES

---

Josue Pierre  
General Conference Associate Treasurer  
& Data Protection Officer

---

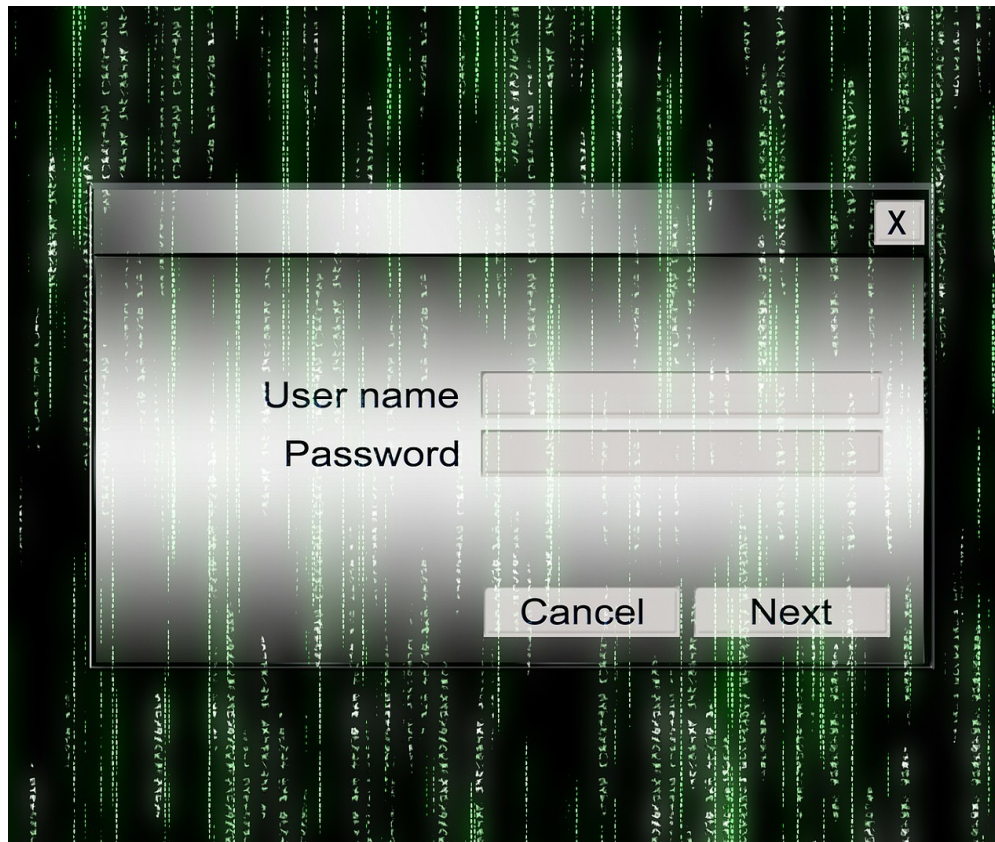
# The Church's Mission

**“And this gospel of the kingdom will be preached in all the world as a witness to all the nations, and then the end will come”**

**Matthew 24:14**



# WHY DO WE NEED TO THINK ABOUT DATA PROTECTION?



# WHY WE MUST BE MINDFUL OF DATA PRIVACY ISSUES

**“If you are not paying for a product, you are the product”**

– Netflix Documentary “Social Dilemmas”

”Protecting people’s privacy ensures their safety, dignity, freedom of thought and expression. **Utilizing personal data through digital technologies provides great social and economic benefits, but at the same time, it can also endanger privacy”**

– OECD.org

## DATA PROTECTION LAWS REQUIRE

- Data protection by design and intent
- Data minimization and anonymity when possible
- Data collection and processing need to be transparent
- Permission from the subject should be requested
- Subjects have the right to be forgotten
- Fines for violating GDPR are substantial

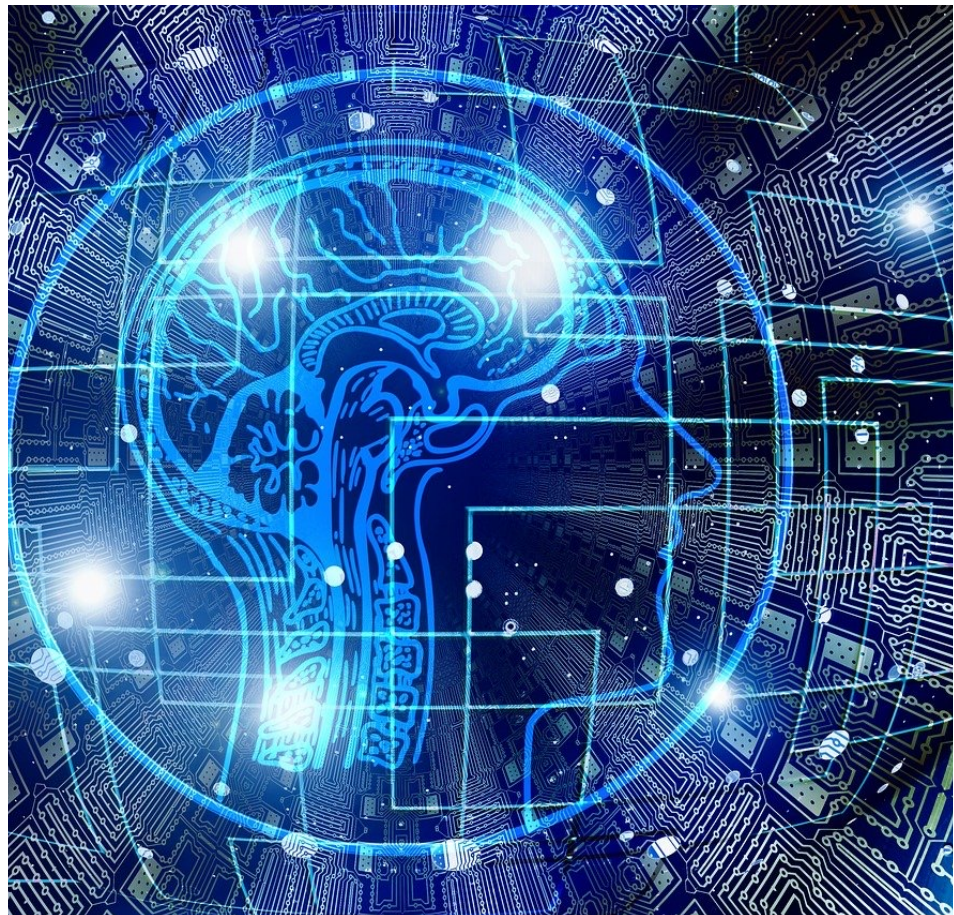
# Technological Tsunami

“The world is experiencing an unprecedented wave of technological change, transforming how we live, work, and interact with each other. This phenomenon, dubbed the “Technology Tsunami,” is characterized by the rapid pace of innovation, the emergence of new industries, and the disruptive impact on traditional businesses and institutions.”

- **Rui Venancio**



# EMERGING TECHNOLOGIES



- Artificial Intelligence
- Robotics
- The Internet of Things
- 3D Printing
- Blockchain

**IN THE DIGITAL MISSION  
FIELD, WHO IS YOUR  
AUDIENCE?**

# POPULATION DISTRIBUTION IN THE U.S. BY GENERATION IN 2023 – by Zippia

Gen. Z (1997-2012) – 20.67%

Millennials (1981-1996) – 21.75%

Gen X (1965-1980) – 19.83%

Baby Boomers (1946-1964) – 21.16%

Silent Generation (1928-1945) – 5.76%

# Where is Your Audience? Social Media Platforms are they on?

## US GEN Z - 2020

- YouTube: 85%
- Instagram: 72%
- Snapchat: 69%
- Facebook: 51%
- Twitter: 32%

## US GEN Z - 2023

- Youtube:88%
- Instagram:76%
- TikTok: 68%
- Snapchat: 67%
- Facebook: 49%

# Where is Your Audience? Social Media Platforms are they on?

## US Millennials - 2020

- YouTube: 85%
- Instagram: 72%
- Snapchat: 69%

## US Millennials - 2023

- Facebook: 87%
- Instagram: 72%
- YouTube: 66%

# WHAT CORPORATE INTERESTS ARE SAYING ABOUT MILLENNIALS & GEN Z



- “Companies are being forced to change their approach when it comes to marketing to Millennials and Generation Z consumers.” (42% of the population)
- “If you want to reach the younger generations, it's not about shock value anymore. It's about standing for something meaningful, and then proving that you and your company walk that walk.” – Deep Patel, *INC.*

# WHAT ARE MARKETING EXPERTS SAYING ABOUT MILLENNIALS & GEN Z

- **“Millennials like authenticity, but Gen Z takes it to a new level. Brands should strive to be authentic at every turn. Those that do will reap the benefits.” - Salesforce**
- **“Passive consumption of content is a thing of the past.” - SocialPost**
- **Traditional marketing efforts don’t have the same effect on millennials as they do on other generations. Before millennials purchase something, they do the work. They conduct research, ask their peers, test the products in stores, or through free trials. They want assurance that what they’re spending their hard-earned money on is *worth it*. –Social Post**



# POPULATION DISTRIBUTION IN THE WORLD BY AGE GROUPS 2020

UNDER 20  
Years Old – 2.6  
Billion (33.1%)

20-39 Years  
Old - 2.3  
Billion (29.9%)

40-59 Years  
Old – 1.8  
Billion (23.1%)

60-79 Years  
Old – 918  
Million (11.9%)

80-99 Years  
Old – 147.5  
Million (1.9%)

100+ Years Old  
- .6 Million  
(0.01%)

# Balancing the Obligations of Data Protection and Emerging Technologies?

Examine the data protection challenges that arises when integrating AI into our digital strategy

How does AI impact user permissions and the protection of sensitive data.

# AI CAPABILITIES ARE GROWING EXPONENTIALLY

- ChatGPT ver. 3.5 took a simulated Bar Exam in the America and passed in the bottom 10%
- ChatGPT ver 4 took a simulated Bar Exam in the America and passed in the top 10%

# CHALLENGES TO DATA PROTECTION WHEN INTEGRATING GENERATIVE AI

COPYRIGHT INFRINGEMENT

INHERENT BIAS

DEEPFAKES

AI HALLUCINATIONS

ALGORITHMIC AUDITING CAPABILITIES

DATA SECURITY

ETHICAL & MORAL GUARDRAILS

# GENERATIVE AI & COPYRIGHT LAW

Generative AI are raising new issues regarding Copyright law principles such as:

- **Authorship** – Can Generative AI create original works that should be afforded the legal protections like other Intellectual property rights?  
In March 2023, the US Copyright Office released guidance that when AI determines the expressive elements of its output the generated material is not the product of human authorship (and therefore not copyrightable)
- **Infringement** – Currently the US Copyright Office will recognize original works created by a human being. Since AI programs are trained to generate outputs by exposing them to large quantities of existing work is the work really an original? Who is the creator, the AI user, the AI programmer, or the AI program?  
OpenAI, acknowledges that its **programs are trained on “large, publicly available datasets** that include copyrighted works” and that this process “necessarily involves first making copies of the data to be analyzed.” Creating such copies, without express or implied permission from the various copyright owners, may infringe the copyright holders’ exclusive right to make reproductions of their work.

# GENERATIVE AI & INHERENT BIAS

Generative AI, because of the types of inputs that are collected by algorithms and because they are **designed, operated, and the oversight is done by humans, biases will occur** in generative AI and should be addressed:

- **Confirmation Bias** – choosing **information that will corroborate with an already established lines of thinking**. This can result in cherry-picking, where problematically large portions of information are being discarded.
- **Survivorship Bias** – Reflects a tendency **to choose only examples of successes, the “survivors”** and to neglect all the negative examples of a certain case and what they would add to the dataset.
- **Availability Bias** - A tendency to **use information most easily available and convenient to our reasoning**, making it easier to miss the big picture and more often than not, you don't have the full picture available to make a well-reasoned decision.

# GENERATIVE AI & DEEPPFAKES

Deepfakes also referred to as **synthetic content** refers to **multimedia that has been digitally altered or synthetically created** using deep learning models. It allows nonexperts and nontechnical people to create sophisticated results. **Which threatens the dependability, reliability, and integrity of information on the internet.**

- Deepfakes can result from face swapping, enactment/animation of facial expression technologies
- Digitally generated audio or non-existing human faces
- Face manipulation technologies involve modifying facial attributes

# Generative AI & AI Hallucinations

- Making **subtle changes to images, text, or audio** that can fool these AI platforms and systems into perceiving things that are not there.
- It is said that **it is still too easy to fool AI systems or sabotage their learning** or perceptions. There is no clear way to protect the deep neural networks that AI depends on.
- AI systems are still vulnerable to adversarial attacks or are just **too gullible by accepting bad or maliciously planted data.**
- “A deep neural network is very different from a human being.”

# Generative AI & Algorithmic Auditing Capabilities

- Regulations are emerging where owners of **AI platforms and processes are required to verify and prove that there is responsible use of AI**
  - With government authorities increasing their enforcement, rulemaking and legislating in this complex arena, it is critical that organizations **understand the privacy requirements** that currently apply to AI
  - AI platforms owners and users are increasingly **required to affirmatively prove that the algorithms will respect data privacy restrictions** and boundaries
  - EU has a draft of a proposed AI Act which would attempt to regulate the usage of AI
  - A recent US FTC decision ordered the destruction of algorithms trained on unlawfully collected personal information

# Generative AI & Data Security

Globally accepted privacy principles such as **data quality, data collection limitation, purpose specification, use limitation, security, transparency, accountability and individual participation** apply to all systems processing personal data, including training algorithms and generative AI.



Latest reports on leaks of sensitive information and chat histories underline the urgent need for robust privacy and security measures in the development and deployment of generative AI technologies.

OpenAI reported in March that a glitch resulting in disclosure of sensitive user data and chat histories

Potential liability arises when AI engages in **scraping** that violates data privacy terms and conditions. (FB was fined \$276 million for data scraping leak in the EU)

Italian authorities issued a blanket ban on OpenAI's GPT products in March 2023 after a data breach wherein ChatGPT and GPT API could see sensitive data generated by other users

# Generative AI & Ethical and Moral Guardrails

- "Disruptive technologies such as artificial intelligence **require new skills and fresh insight as they gain wider commercial adoption**. While its potential for good is enormous, so is AI's potential for misuse. Due in large part to regulatory and academic guidance, **we are already seeing the need for ethicists and privacy professionals in the design and coding of AI systems.**"

Todd Ruback – Managing Director, FTI Tech - IG, Privacy & Security

- Just because you can do it, doesn't mean you should do it.
- Developers planning on integrate AI into processes and platforms **should by design and intent institute data protection policies and controls** to ensure that data being collected does not violate data privacy rights and protections.

# Balancing the Need for AI Algorithms to Collect and Process Large Sets of Data



**Scraping** – refers to the automated extraction of data from websites or other sources using tools to gather information from the web pages often large quantities.



It can potentially violate data protection regulations if personal data is collected without obtaining consent or complies with privacy principles



It can also impact data privacy by harvesting publicly available data and aggregating it, which may lead to re-identification of individuals or the creation of an extensive profile of and individual without their consent.



Data that is scraped and processed by AI can also result in utilizing personal data for purposes beyond the initial permissions that was granted when the personal data was shared.

# Balancing the Need for AI Algorithms to Collect and Process Large Sets of Data

- **Data Protections Obligations** apply even more so when looking to integrate AI capabilities to your platforms, processes, and programs:
  - Personal data protections and privacy must be by intent and by design
  - Must ensure that the Church is acting morally and ethically and that you are transparent and honest about what PII is being collected and purposes for processing PII
  - Must ensure that you have received true consent for any personal data being collected and processed from individuals
  - Must be ensure that the data being collected is not inaccurate, outdated, or misleading to eliminate as much as possible the possibility for bias or unreliable models or outcomes

# Balancing the Need for AI Algorithms to Collect and Process Large Sets of Data

- Considerations and safeguards should be integrated into the parameters of AI usage to minimize copyright infringements or violations of terms of use of websites and databases. On the front end, you need to determine legally and ethically, who owns the data or the intellectual property
- Anticipate unintended consequences where AI techniques may cause harm or unfair treatment of individuals

# We Must Ensure the Advancement of Mission?

**“Then you will know the truth, and the truth will set you free.”**

**John 8:32**

