What to Know Web3 Privacy & Security

Programme

Award- Winning Author, Co-Founder & Blockchain Historian

Alyze Sam

What to Know Web3 Privacy & Security

History & How to Protect Yourself, Business & Customers in Web 3

Introduction

Meet the Educator

Alyze Sam, Women in Blockchain

Alyze Sam

Blockchain Historian & Course Facilitator

Bio & Contact

Alyze Sam is a refreshing blockchain strategist, a novel educator, a multi-award-winning author, a serial co-founder, and a vehemently driven advocate. Don Tapscott published Sam's eight years of stablecoin research at **The Blockchain Research Institute.** The Bad Crypto Podcast developed a Blockchain Hero NFT inspired by her work: Mz. Stability. Sam has been ranked **Top 50 in Blockchain** & **Top 5 Women in NFTs** (HackerNoon, 2022) and released The ABCs of NFTs with the world's youngest author, her 4-year-old son! Sam's five published books have been awarded best sellers and best releases in over 14 science, business, education, and technical categories. Order Sam's latest #1 new release with Alex Tapscott on Amazon now: **Digital Asset Revolution and** her #1 in Computer Science & Financial Education: **Stablecoin Evolution.**

sam@TechandAuthors.com

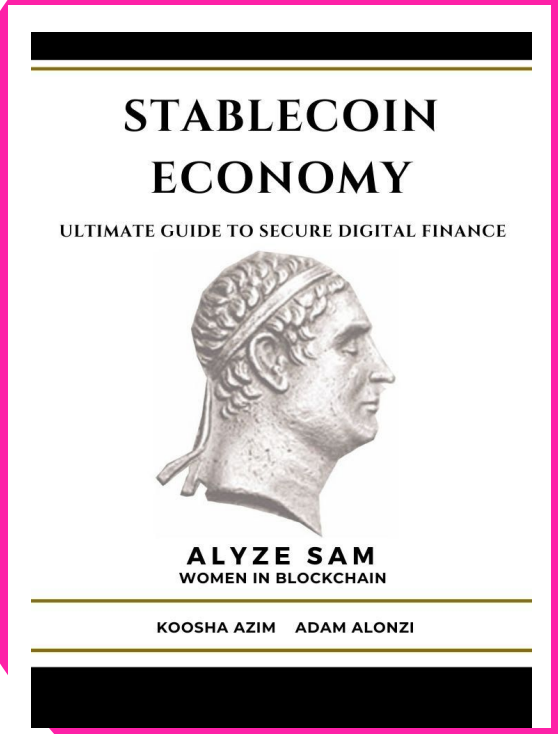
@AlyzeSam

+13165877355

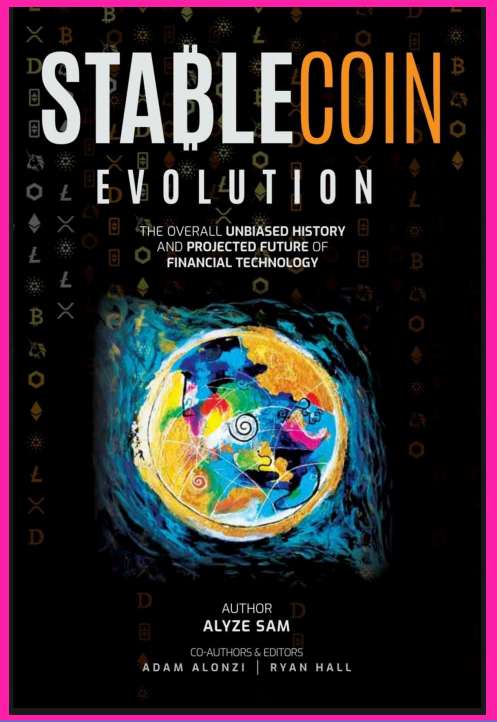
@AlyzeSam

Happy To Share Digital Copies

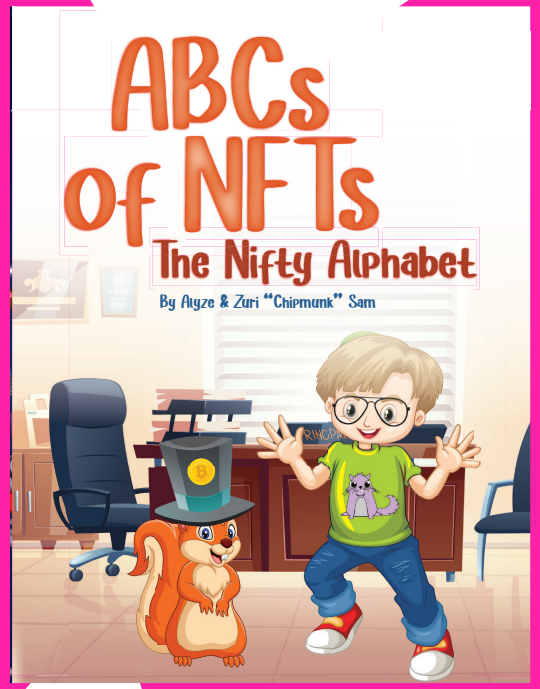
Award-Winning Technical Copy & Education



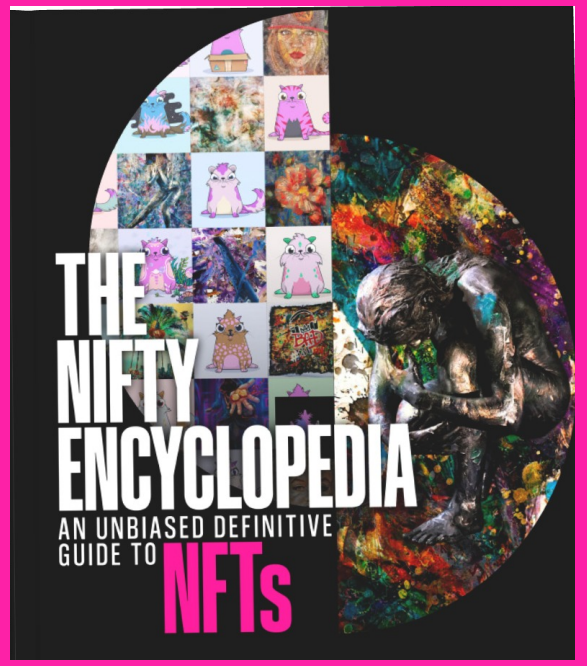
Stablecoin Economy
TechandAuthors.com
Or Amazon



Stablecoin Evolution
TechandAuthors.com
Or Amazon



ABCs of NFTs
TechandAuthors.com
Or Amazon



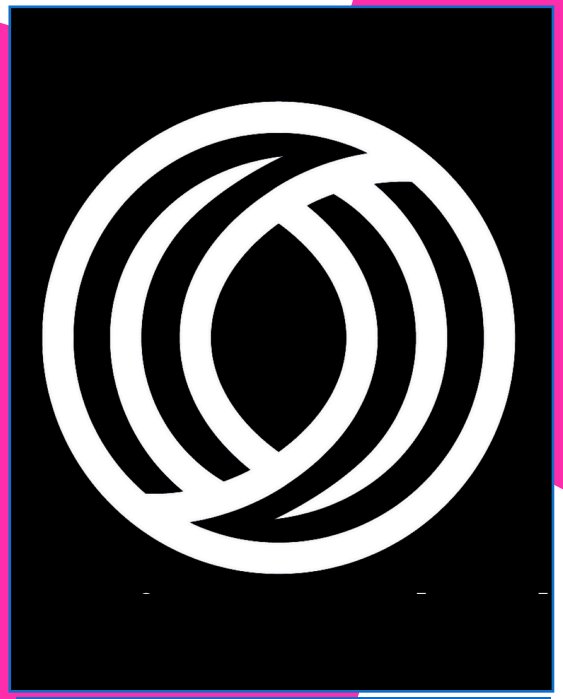
The Nifty Encyclopedia
TechandAuthors.com
Or Metaverse Publishing

Projects

Sam is a serial Co-Founder and currently launching

Tech & Authors

TechAndAuthors.com



OnionClub

OnionClub.io

Bakeree

https://bakeree.io/

One Game Initiative

https://1lab.network/

Section 1

History & Defining **Security**

What is Security?

Online Security *is aimed at safeguarding data, whereas* ***Digital Privacy*** *is the sole authority to private data & information.*

Security is protection from, or resilience against, potential harm caused by others, by restraining the freedom of others to act.

The main security & privacy differences include;

Security aims to safeguard sensitive data & information from unauthorized access.

Any security approach addresses either or all of these objectives.

Section 2

Security Timeline

Security Timeline

A New Kind of Network 1960

"Distributing the connections in a system becomes more resilient in the face of outages."

Engineer Paul Baran argues that a decentralized communications system with many redundant links could help the United States recover from a Soviet nuclear attack. The key was that information could flow across many different paths – much like today's Internet – allowing connections even if much of the overall system suffered damage.

Packet switching theory 1968

"Several users can share a single packet-switched line, allowing for better use of scarce computing resources."

Donald Davies, a top official with Britain's National Physical Laboratory, describes a system for chopping data into smaller pieces to make transmissions more efficient. He calls the pieces "packets" and the technology for transmitting them "packet-switching." The idea remains an essential technology of the Internet.

History of Online Security

The internet expanded from the yield of multiple individuals over several decades.

Few predicted the integralness of being connected to the world wide web, nor how it would evolve to make nearly everyone connected vulnerable to scam artists, stalkers, data collectors, preditors, and spies.

Examine some of the climacterics of conceiving today's insecure online world.

Alyze Sam @ TechandAuthors.com

The precursor to the Internet 1969

ARPANET

The Pentagon's Advanced Research Projects Agency designs and funds a packet-switched network called the **ARPANET** – considered the most important precursor to the Internet. The first **ARPANET** message was sent at 10:30 p.m. on October 29, 1969, from the UCLA computer lab of Leonard Kleinrock, a networking pioneer.

A road not taken 1978

Encryption

Computer scientists Vinton G. Cerf and Robert E. Kahn attempted to build encryption technology directly into **TCP/IP,** a set of protocols that would give rise to the internet several years later. But the scientists encounter several obstacles, **including resistance from the National Security Agency.**

The Birth of the Internet 1983

Standardizing how networked machines communicate with each other enabled the internet's massive growth.

ARPANET requires its network users to communicate via TCP/IP, quickly making it the global standard. Networks worldwide could then communicate easily with each other, creating the internet.

Computer Fraud and Abuse Act 1986

Congress enacted a comprehensive bill establishing legal sanctions against data theft, unauthorized network access, and other computer-related crimes.

The Morris Worm 1988

Morris becomes the first person convicted by a jury under the Computer Fraud and Abuse Act.

A Cornell University graduate student named Robert Tappan Morris released several dozen lines of code, which replicated wildly and spread to thousands of computers worldwide.

The worm crashes about 10 percent of the 60,000 computers then linked to the internet.

(Internet) power to the people 1993

The first browser, **Mosaic**, is released, allowing users with little or no technical skills to browse the World Wide Web, fueling a new period of massive Internet growth and the commercialization of cyberspace. As the community of online users grows, so make security threats.

The web became animated in 1996

Flash & other browser add-ons have been a significant source of security flaws, w/ some experts recommending that users disable them entirely.

New drawing & animation tools, such as Macromedia's Flash, dramatically expand the abilities of browsers. This revolutionizes the look and feel of Web sites. Hackers soon discover that these Web tools also can allow them to take remote control of computers on the internet, no matter where they are in the physical world.

Insecurity spreads 2000

A rash of new computer worms, such as **ILOVEYOU**, spread wildly across the internet, taking advantage of security flaws in widely used software made by Microsoft and other major tech companies. Tens of millions of computers are affected.

No longer a fad 2003

The more devices using the internet, the more entry points there are for attacks, & the more difficult it becomes to overhaul how the system works.

The amount of data created in 2003 surpassed all information created in the rest of human history combined. The internet has become so central to commerce and culture worldwide that the opportunities for hackers grow.

The internet in your pocket 2007

The introduction of Apple's iPhone fuels the rise of mobile devices. Smartphones running Google's Android operating system hit the market the following year. This heralded a new era of snooping, as police, spies, and even jealous spouses found ways to monitor people through powerful personal computers doubling as phones.

Internet deemed complex, unpredictable 2010

"Distributing the connections in a system becomes more resilient in the face of outages."

A group of the nation's top scientists concluded in a report to the Pentagon that **"the cyber-universe is complex well beyond anyone's understanding and exhibits behavior that no one predicted, and sometimes can't even be explained well."** The scientists, part of a Pentagon advisory group called JASON, said, **"In order to achieve security breakthroughs, we need a more fundamental understanding of the science of cyber-security."**

The future of Internet security, resides in human intervention & innovation.

Car Hacking 2014

"A deadly new hack"

Security researchers published a guide to hacking automobiles, revealing deep flaws in how automobile electronics communicate. Shortly after that, Massachusetts Sen. Ed Markey's office found that nearly all ***"cars on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions."***

Implementing hardware & software solutions and using human intervention to monitor the network continually are two of the best ways to keep up-to-date on outside attacks.

Section 3

History & Defining: Privacy

“Privacy rights are inherently intertwined with **information technology.”**

Few attempts have been made to clearly and precisely define the *"right to privacy."*

There is **no clear definition** of the term "**privacy**". Some **experts believe that privacy is a human right** that every human being has simply by being alive.

What is Privacy?

Privacy can be defined as the ***right to be left alone.***

The right to privacy is an element of various legal traditions that intends to restrain governmental and private actions that threaten the privacy of individuals.

Privacy is a comprehensive & fundamental human right that any entity should treasure & retain for safety & security.

Why does a *right to privacy* matter?

"Privacy matters because ***good privacy rules can promote the essential human values of human identity, political freedom, and consumer protection.*** *If we want to preserve our commitments to these precious yet fragile values, we will need privacy rules."*
-Neil M. Richards

*A society with a total lack of privacy would be **intolerable**; further, a civilization possessing complete privacy would not allow for any community, business, or cultural growth.*

Privacy is a BIRTHRIGHT, NOT an OPTION!

Privacy is the right of people;

* **to make personal decisions regarding their intimate matters**
* **to lead their lives in a manner that is reasonably secluded from public scrutiny**
* **to be free from such things as unwarranted drug testing or electronic surveillance.**

Section 4

Privacy Timeline

Privacy Timeline

12th Century, Bologna, Italy

"A right – an entitlement a person possesses to control or claim something,"

The concept of a human ***"right to privacy"*** begins when the Latin word *ius* expanded from meaning "*what is fair"* to include "*a right – an entitlement a person possesses to control or claim something,*" by the **Decretum Gratiani** in Bologna, Italy in the 12th century.

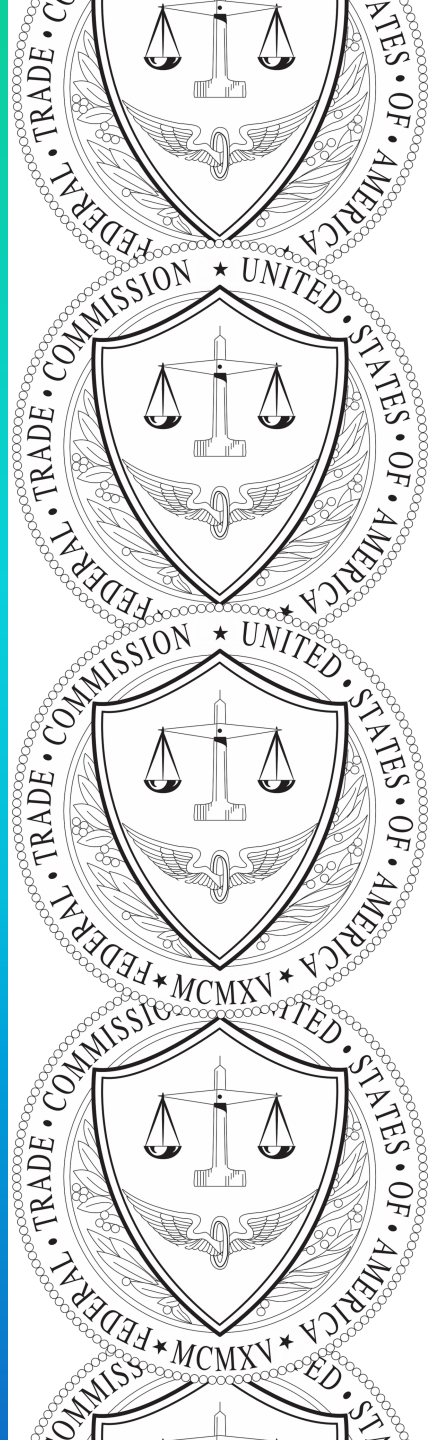
1789

U.S. Constitution

While not explicitly guaranteeing the right to privacy, the Supreme Court has found that the U.S. Constitution provides a ***right to privacy*** in its **First**, **Third**, **Fourth**, and **Fifth** amendments.

How the Constitution deals with privacy in a technological change:
https://youtu.be/co4cHIJJux4

Photo Source:
Decretum Gratiani



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

1890, United States

"Right to be let alone"

In the 15 December 1890 issue of the *Harvard Law Review* entitled "The Right to Privacy," by attorney Samuel D. Warren II and future U.S. Supreme Court Justice Louis Brandeis, is cited as the first explicit finding of a right to privacy. This work states that privacy is the "*right to be let alone*" and focused on protecting individuals. This approach responded to recent technological developments, such as photography and sensationalist journalism, also known as "*yellow journalism.*"

1914

Establishment of the FTC

The Federal Trade Commission Act (FTCA) of 1914 established the Federal Trade Commission and outlawed unfair or deceptive commercial practices. Since the 1970s, the FTC has been the leading federal agency that is most often involved with privacy issues, regulations, and enforcement.

1917

Ruling on Protection of Sealed Mail

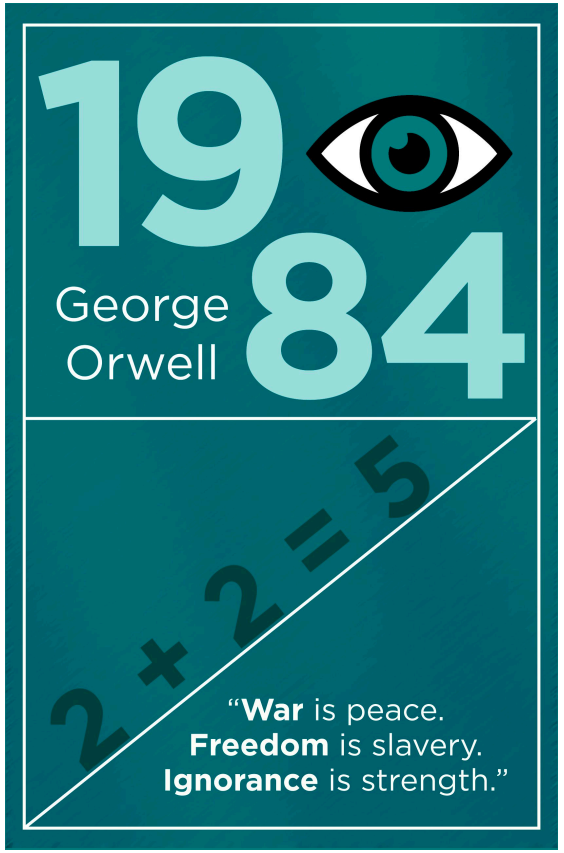
The newly established **Bureau of Investigations** actively investigated acts of foreign sabotage and rooted out subversion. Surveillance extended to monitoring and illegally opening correspondence of suspected subversives. *When the bureau filed an official request to open mail, Solicitor* ***General Judge William Lamar*** *ruled against the privacy infringement and upheld long-established protections of sealed mail.*

TechandAuthors.com Privacy Timeline

1948

George Orwell Writes *1984*

1984 is a dystopian novel by George Orwell containing themes of nationalism, futurology, censorship, and surveillance. Inhabitants of Oceania, the "*super-state*" where the book takes place, have no privacy. Public and private spaces are filled with cameras and microphones. Even thought is controlled by undercover agents of the "*Thought Police.*".



1948

U.N. Declaration of Human Rights

Proclaimed by the United Nations General Assembly on December 10, 1948, the U.N. Declaration of Human Rights (UDHU) was drafted by representatives from all over the world with various legal and cultural backgrounds. Article 12 states, "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*"

Privacy Timeline

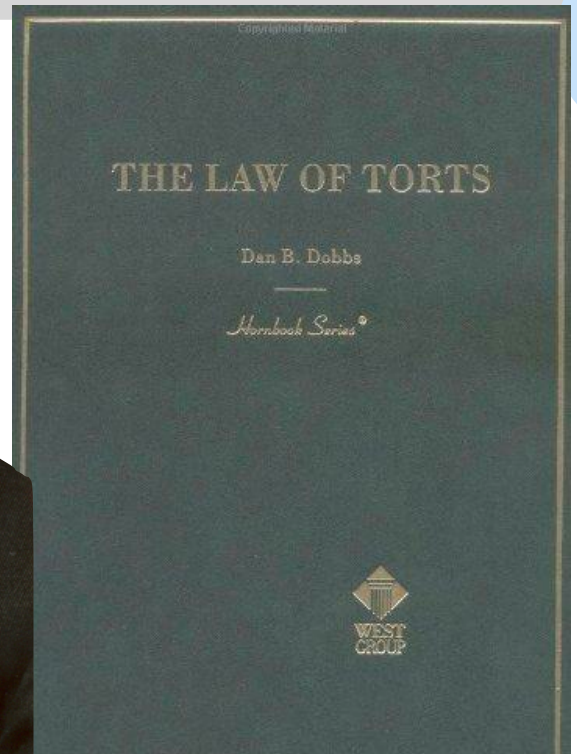
1960

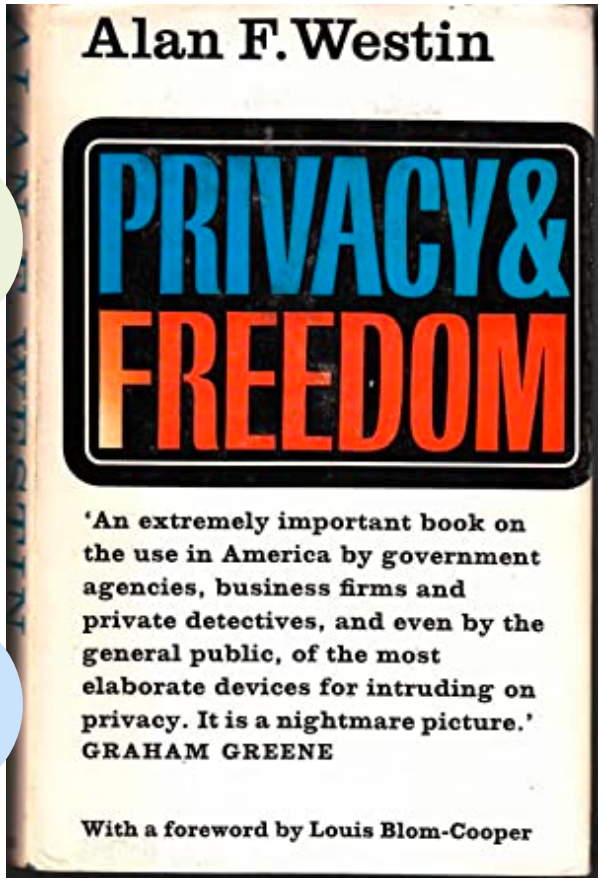
Privacy Torts

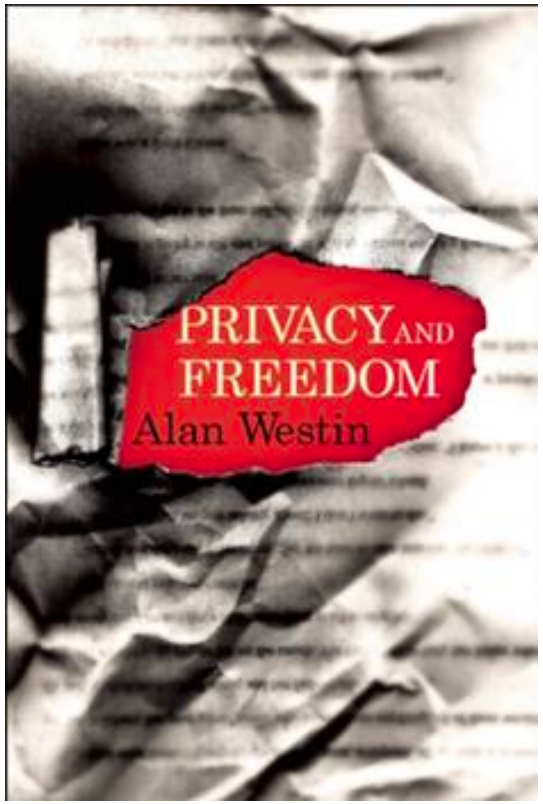
In 1960, **William L. Prosser**, a well-known legal scholar, published the article Privacy. In the article, still considered influential in the field of privacy law today, he outlined four torts allowing someone whose privacy was violated in one of those four ways to sue the perpetrator for damages.

These torts are still used today:

- Intrusion upon seclusion or solitude, or into private affairs;
- Public disclosure of embarrassing private facts;
- Publicity which places a person in a false light in the public eye; &
- Appropriation of one's name or likeness.







1967

Alan Westin Writes **Privacy and Freedom**

Alan Westin, who defined privacy as an individual's right to control, edit, manage, and delete information about them [selves] and decide when, how, and to what extent information is communicated to others. His book, *Privacy and Freedom*, is still one of the seminal works on privacy to this day and helped set the stage for modern debates about technology, privacy, and personal freedom.

1973

Records, Computers & the Rights of Citizens

Report of the **HEW** Advisory Committee on

Automated Personal Data Systems

The Department of Health, Education, and Welfare (*HEW*) Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS) developed the landmark Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems.

This report was the origin of Fair Information Practices, a set of principles that formed the basis for modern privacy legislation.

1995

EU Data Protection Directive

Adopted by the European Union in 1995, **the Data Protection Directive regulates the processing of personal data within the EU**. *In comparison to the United States, the right to privacy is a more highly developed field of law in the EU.* The Data Protection Directive was superseded by the General Data Protection Regulation (GDPR) in 2018.

2012

European Union's Right to be Forgotten

The European Commission released a draft **European Data Protection Regulation** **that would supersede the EU Data Protection Directive.** *The law allows EU citizens to submit requests to search engines to have personal information delinked from the results of searching their name.*

2018

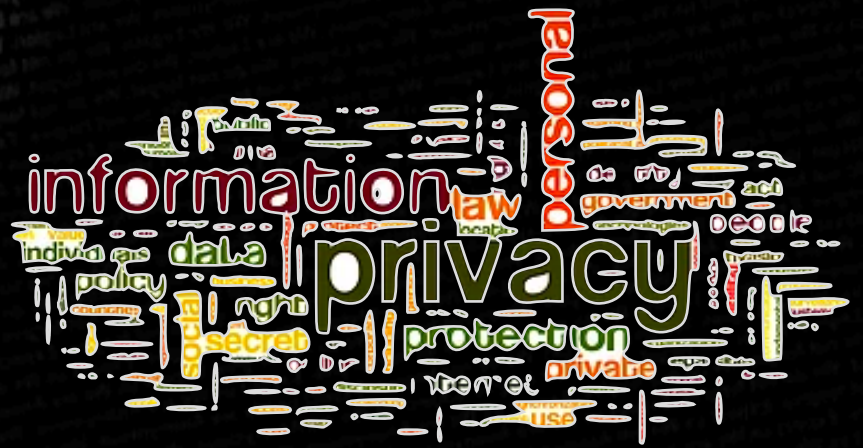
GDPR May 25, 2018

The **General Data Protection Regulation** (**GDPR**) is a European Union (EU) and the European Economic Area (EEA) law. *The GDPR consists of data protection and privacy for individuals, an essential component of EU privacy and human rights law.* GDPR further addresses the transfer of personal data outside the EU and EEA areas. *The GDPR's primary aim is to enhance individuals' control and rights over personal data while simplifying the international business regulatory environment.*

The First Chief Privacy Officer did not fully emerge until 1999

A **Chief Privacy Officer (CPO)** *is a senior level executive responsible for managing risk related to and ensuring compliance with information privacy laws*. The role exists in an increasing number of corporations, public agencies, and other organizations.

While the first example of a CPO can be found with the 1991 implementation of the role at the consumer database marketing company Acxiom, *it became more well known with the 1999 hiring of privacy lawyer **Ray Everett** by the internet advertising technology firm **AllAdvantage**.*



Privacy Timeline

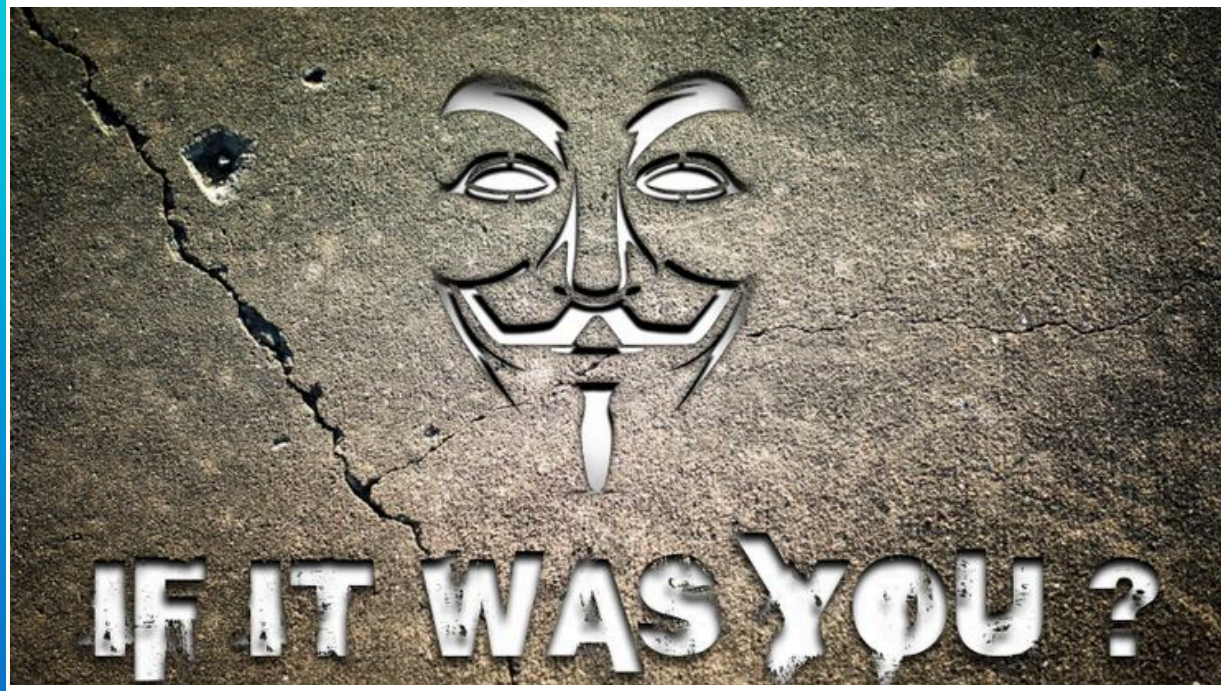
2023 & Beyond

Now: The Reality of Perpetual Connection

We live in ubiquitous technology, seemingly indiscriminate data collection, and pervasive surveillance. *These developments represent fundamental challenges to how we perceive and approach privacy, even if they often make our lives easier.*

Users demand freedom from intrusion:

"Rather than waging a losing battle against technological intrusions, we should put more effort into recognizing the inherent value of our data. Doing so would allow us to shift our focus towards understanding and exercising our rights and options and making informed decisions regarding how our data is used."

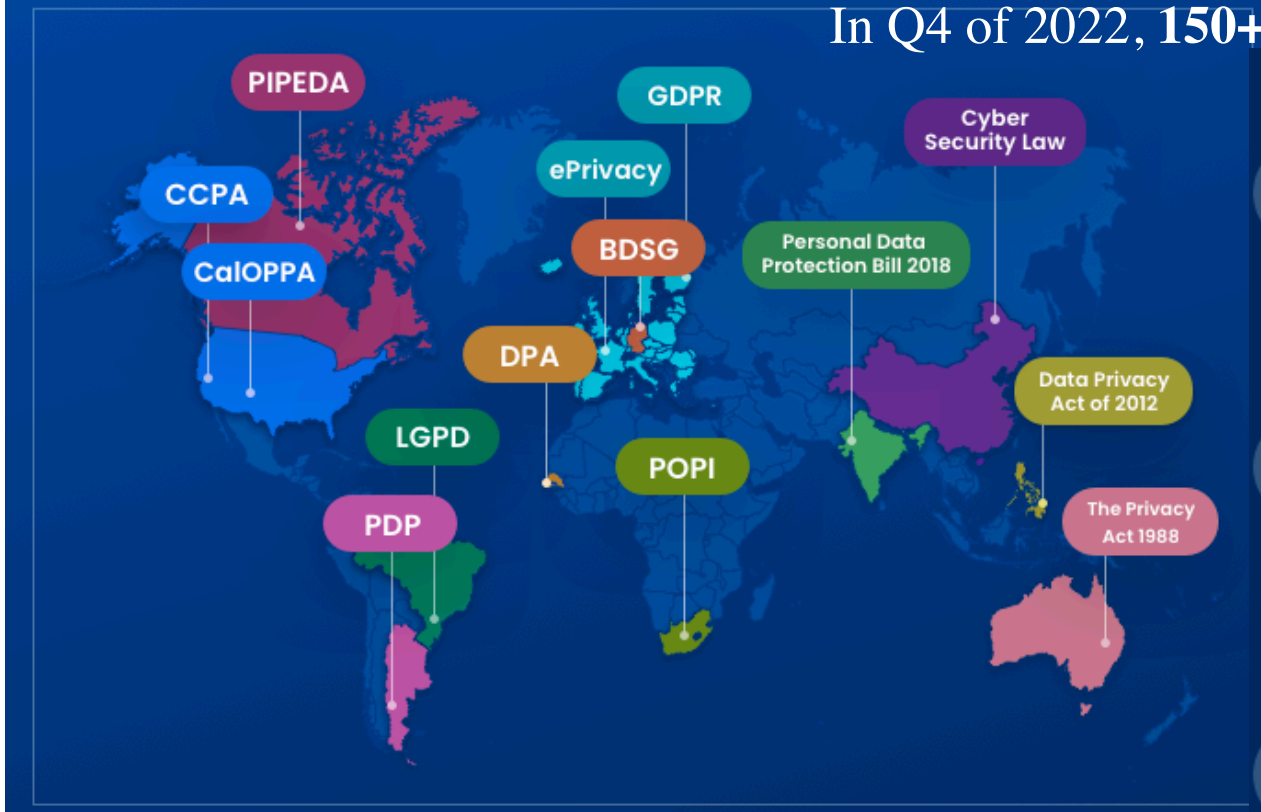


Acting **ethically** and will due diligence, can help ensure your, your business and clients protection, in Web 2, Web 3 and the future.

Everyone should have a space where they can be ourselves — and be let alone.

Privacy Laws Around the World

In Q4 of 2022, **150+ national constitutions** mention *the right to privacy*.



4.2 Billion Individuals share their data online

6 out of **10** people worldwide are subject to data collection

Cost of non-compliance?

$ 500K | € 20M | ₹ 50M

*potential fines for violations

100 # of countries that have data protection laws

98% **Respondents to a U.S. survey** feel they should have control over the sharing of their personal data

79% **Respondents in India** didn't feel comfortable having their data sold to third parties

74% **Global respondents** feel some degree of concern over the treatment of their data

Personal Data Protection Bill 2018

Personal Data Protection Bill 2018 | India

After India's Supreme Court determined privacy to be a fundamental human right in 2017, India's first data privacy law was quickly created. The legislation sets privacy and data protection standards, and notably introduces mandatory annual data audits.

Cyber Security Law

Cyber Security Law | China

Enacted in 2017, China's Cyber Security Law has garnered some controversy. While it has the makings of a standard data protection law, it is feared to be just another tool in the Communist Party's belt. Claims have been made by US officials that the law allows the Chinese government to spy on users via Chinese businesses.

Data Privacy Act of 2012

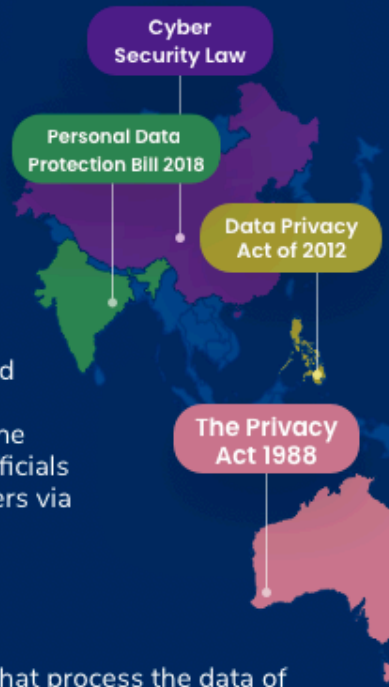
Data Privacy Act of 2012 | Philippines

Based in the Philippines, but applicable to all businesses that process the data of Philippine citizens and residents, the Data Privacy Act of 2012 is centered on the principle that data processing should be transparent, proportional, and based on legitimate purposes.

The Privacy Act 1988

The Privacy Act 1988 | Australia

Although this privacy law was established in 1988, it has undergone frequent amendments since then. It establishes Information Privacy Principles (IPPs) for Australian citizens when it comes to the collection of their data by government organizations, companies contracted to work with government organizations, and health service providers.



Alyze Sam @ TechandAuthors.com

CCPA

California Consumer Privacy Act | USA

Officially in effect on January 1st, 2020, the CCPA boasts three guiding principles: transparency, accountability, and control. It demands that companies inform users of data processing, take extra measures to protect user information, and allow users a say in what data is collected and how it is shared.

CalOPPA

The California Online Privacy Protection Act | USA

In 2004, CalOPPA broke ground on data privacy in the United States, as the first to require websites to post privacy policies detailing data collection and use. As the act is applicable to any business or online operation with users in California, millions are subject to comply with the law.

PIPEDA

The Personal Information Protection and Electronic Documents Act | Canada

PIPEDA mandates that businesses using data for, or in the course of, commercial activities, must disclose the purpose of that data collection to the owners of that data, and obtain consent to proceed.

LGPD

Lei Geral de Proteção de Dados Pessoais | Brazil

Set to take effect at the beginning of 2020, the LGPD is a landmark legislation for Brazil, outlining data processing standards, including the 10 legal bases on which data can be processed. While the law was modeled after the EU GDPR, it is notably less strict. For instance, the LGPD threatens maximum fines of 2% of a company's annual revenue – only half of what the EU threatens for similar violations.

PDP

National Directorate of Personal Data Protection | Argentina

Finalized in 2017, this law replaced Argentina's Personal Data Protection Law from 2000, and upped the ante considerably for data privacy. Among many notable provisions, it gives users – for the first time in Argentina – the right to request the deletion and transfer of their data.

GDPR

General Data Protection Regulation | European Union

The big name in data privacy, the GDPR sets the strictest and most far-reaching standards for the handling of user data. It is based on principles of consent, transparency, protection, and user control, and threatens fines as high as 4% of a company's annual revenue.

ePrivacy

ePrivacy Directive & Regulation | European Union

The ePrivacy Directive is often referred to as the Cookie Law, due to its requirement that websites obtain user consent to non-essential cookies before launching those cookies. The directive is currently under revision, and will be re-released as the ePrivacy Regulation.

BDSG

Bundesdatenschutzgesetz | Germany

Widely accepted as the earliest data protection law, the BDSG sets rigid standards under which businesses are required to adopt and maintain protective measures for data stored in IT systems.

DPA

Senegal's Data Protection Act | Senegal

The DPA only applies to businesses whose means of data processing are located in Senegal. It is notably less rigid than recent laws like the GDPR, and only applies to data collection with the intention of being shared with third parties.

POPI

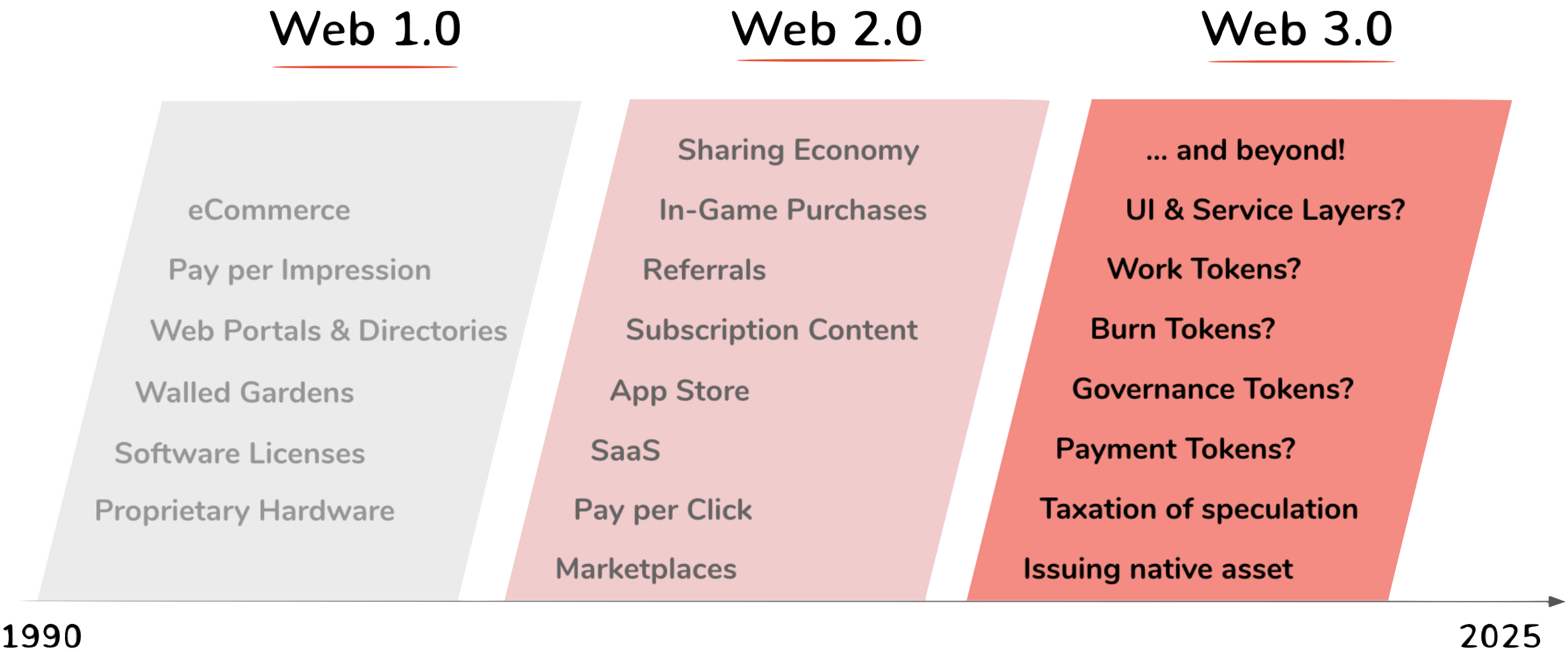
Protection of Personal Information Act | South Africa

POPI (also referred to as POPIA) went into effect in 2014 and applies to all South African organizations. It sets a standard of accountability for responsible data processing, and establishes the requirement of customer consent to direct marketing outreach.

Section 5

Knowing Web1, Web2, & Web3

Knowing The Difference Between Web1, Web2 & Web3



Section 6

How & Why's of Privacy in Web3

Web 3.0 & Privacy

*"The most notable privacy upgrade with Web 3.0 is removing centralized third parties from the equation. Users will interact directly instead of relying on companies like **Facebook** to facilitate the exchange. That way, people don't have to worry about an intermediary listening in on their private conversations."*

The primary goal of developing a Web 3.0 or *Web3* ecosystem is to provide sovereignty back to internet users.

Web3 will allow users to create and execute tools independently rather than providing enterprises with their data to use digital services.

Web3 uses advanced technologies, including blockchain, to decentralize the web, extracting dependency on third parties.

On Web 2.0, merely a few corporations, including Meta, Microsoft, Google, and Amazon, control the internet, whereas Web 3.0 is a dispersed digital environment among everyone.

Section 7

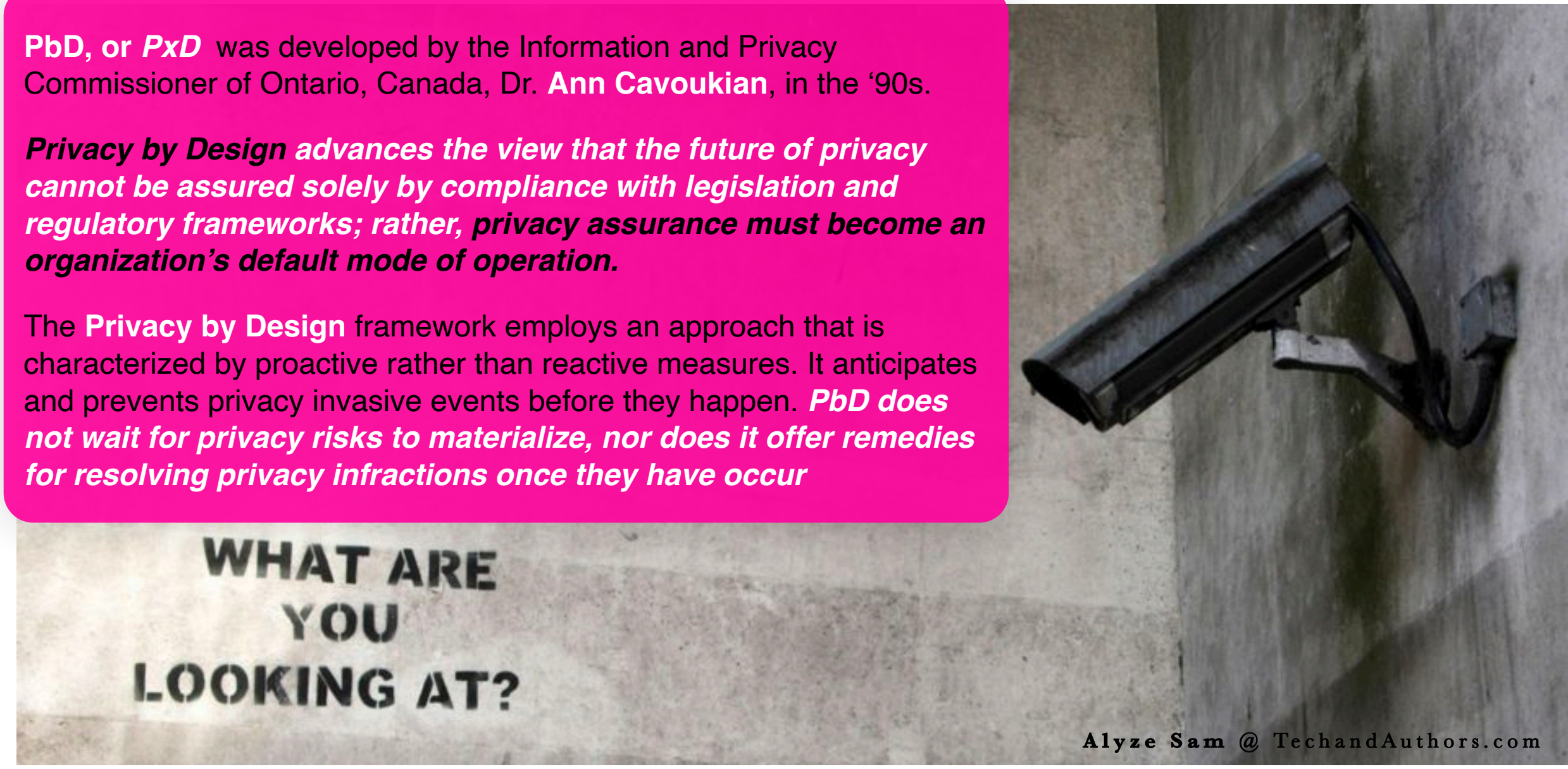
Privacy by Design: '***PbD***'

History of Privacy By Design

PbD, or *PxD* was developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. **Ann Cavoukian**, in the '90s.

Privacy by Design** advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, **privacy assurance must become an organization's default mode of operation.

The **Privacy by Design** framework employs an approach that is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. ***PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occur***



Section -End-

Alyze Sam

OnionClub.io Co-Founder

Reach Out To Me!

@AlyzeSam

Looking for an Ethical Blockchain Incubator?

My team of experts and I will build you blockchain solutions at MassCrypto.io

@MassCryptoio

Looking for poetic technical copy?

My highly experienced technical writers and I can provide legal, technical and evergreen copy, as well as apply for business grants at TechandAuthors.com

@TechAndAuthors

THANK YOU

QUESTIONS?

TechandAuthors.com
MassCrypto.io

OnionClub.io
MassMediaDivision.com

sam@TechAndAuthors.com

fb.com/AlyzeSamWIB

@AlyzeSam

@AlyzeSam