BACKGROUND PAPER:

Special Committee on Technology, Corporations, and State Sovereignty (SCTCSS)

International Implementation Challenges for Data Extinction

Introduction:

**Delegates will benefit from reading the GA background paper in order to prepare for this topic, focusing most upon the opening pages (1-4), data extinction discussion (12-13), and geo-political challenges (15).*

> It is both plausible and reasonable that a significant number of states would eventually coalesce around a legal instrument which would regulate surveillance and protect privacy in cyberspace. This would be good for citizens, good for governments, good for privacy and good for business.
>
> — Special Rapporteur on the right to Privacy's report to the Human Rights Council, 34th session — A/HRC/34/60

But is this true? And if it is not, how long must individuals wait?

As individuals across the world value their personal data and consequently discover its value to others, the technological steps towards consumer-level data extinction become one of marketplace. If the consumer desires a product, the market often provides.

One of the key differences between Web 2.0 and Web3 is the decentralizing of ownership, of data control. Where 2.0 data was kept primarily in the hands of groups of companies (financial institutions, social media conglomerates, etc.), the advent and advancement of blockchain technologies, token-based economics,

and (perhaps regrettably) NFTs and cryptocurrencies have fundamentally altered the way we understand data control.

Fortunately, we will not pursue the technological dimensions of Web3 too deeply. However, the conceptual framework of this new evolution in data encryption offers an effective equivalent, perhaps, to data extinction, *a control of data property beyond the power of government or business.*

For instance, an NFT (non-fungible token) is essentially a unique identifier (unchangeable) attached to any set of data (think, for instance, artwork) to demonstrate ownership and authenticity. This NFT can be attached to any data or set of data at all, completely determined by the user/creator. While 2018-2021 was filled with buzz about art and game and film sales (even Nike did it to identify their shoes!), the NFT market has since collapsed, with over 95% of NFTs now valued at $0. But this does not change their ability to identify data.

SSI (Self-Sovereign Identity) is similarly a Web3 method for individuals to authenticate who they are without relying upon other institutions. Think, for instance, how often we are offered an opportunity to “safely log on” with Google accounts. Instead of depending on Google’s ownership of our data to do this, SSI offers the same trusted and unique identification methods for individuals to use.

Control of data is the beginning of Web3; and as AI, machine-learning, and Web 4 (which focuses on the “connectedness” of all things like smart homes, self-driving cars, and virtual/personal online experiences) develop, the call for consumers for data extinction is growing stronger. Indeed, it is already within technological reach, perhaps awaiting only sufficient market momentum.

Anticipating these moves, this Special Committee seeks to anticipate (and perhaps mitigate) the changes to international governance that would result if data control (at least partly) shifted to the consumer.

The Current Debate: What’s At Stake

Governments clearly have a stake in a technological change that so alters a shift in political power and the ability of governments (and marketplaces) to function effectively. The first and most effective response they have to such shifts is in the legal framework. In other words, laws can regulate what is and is not permitted in order to ensure a safe and orderly society.

A few premises or guiding points may assist, however, in determining strategies in response:

First and foremost, it should in the first background paper be clear that **the status quo for data privacy and security has too often failed** and there is little promise that this will change on its own. It is unsurprising (and hardly blameworthy) that individuals would seek their own solutions from a (at its

kindest) sluggish response from the national and international communities. Individuals are guided by self-interest, and Web3 and its new incarnations is understandable.

Second, decentralizing data (and the deletion or hiding of data) **absolutely also supports criminal activity** in a number of ways. Money-laundering, drug trade, terrorist planning, etc. can all occur relatively unobserved in such a system. More, any number of fake business schemes and fraud can be perpetrated on too-confidence consumers beyond the ability of legal agencies to protect them.

Further, these technologies **threaten market growth,** especially in emerging economies. As is often the case with new technologies, a few will likely profit heavily at the expense of others, fomenting further wealth imbalances. And, because the market economy may be further divided between different systems of collecting and using short-lived data, volatility in markets will increase, posing dangers of company collapses and larger economic crises.

Web3 (and Web4) have other challenges beyond these, of course (i.e. environmental impacts, interoperability issues, etc.), but this committee is not whether or not to allow/stop these movements. They are with us. Instead, we are looking at a matter *of international regulation on the individual control of personal data.*

Committee Mission

The SCT is charged with making specific international guidelines for the permissible uses of personal data which would act contrary to individual data extinction control. In other words, what personal data privacy rights remain with individuals to terminate their data files and what controls may be placed upon them?

In so doing the Committee should consider:

- Government collected and held data
- Corporate collected and held data
- Transference of that data to third parties
- The “permanent” copying of that data

In addition, to booster consumer/citizen confidence and trust, what additional measures should be placed upon governments and business entities to more effectively secure data or demonstrate transparent use of it?

Categories of Consideration

Here are some categories of the types of data which might be deleted by users or secured by governments and businesses:

- Name
- Signature
- Address
- Phone number
- Date of birth
- Credit information
- Employee record information
- Subjective information like opinions, estimates, or judgments
- Information about criminal convictions and offenses
- Genetic data
- Biometric data used for identification
- Health data
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sex life or sexual orientation
- Gender identity
- Social media posts & activity (likes, etc.)
- Passwords, PINS, and Security Questions
- Interests, Hobbies
- Government IDs
- Photographs and other visual or audio records
- Traditions observed
- Languages spoken or accents
- Browsing history and call logs
- Citizenship country and status
- Marital status
- Family connections
- Disability status
- Military status
- Drug use
- Height, weight, tattoos, and other physical descriptors
- IP addresses and other hardware ID
- GPS coordinates or any current locator
- Information acquired by security cameras, turnstile use, door access, etc.
- Financial records including credit, bank account #s, taxes, and investments
- Financial reputation
- Homes and vehicles owned, leased, etc.
- Spending and product history
- Emergency contacts
- Friends and social connections
- Group memberships
- Email and text messages, etc.
- Education records
- Social status: celebrity, athlete, politician, etc.

Next, consider potential uses for such data:

- Criminal investigation (by government authority or journalism or private investigations, or by businesses to detect fraud or misuse)
- Border control
- Military intelligence for risk assessments
- Policymaking (to assess harms, predict outcomes, measure success, etc.)
- Communication (with segments of users for government or business needs)
- Financial transactions (for exchange, marketing, or product creation/recommendations)
- Evaluate credit and loans
- Medical research and predicting healthcare needs
- Social design research (predicting city needs, infrastructure development, etc.)
- Historical records for national identity, education, etc. Who merits preserving?
- Journalistic reporting

Each of these areas is itself an enormous field of data use, too large to discuss here. However, it's important to realize that legitimate use of personal data is a broad range of cases.

And finally, we might consider how we identify categories of personal data control.

- Consider a code for who can access/use (Government - G, Corporate - C, or Private - P). It may be that more specific codes are required.
- A code or rule for duration of use in minimum or maximum terms:
    - i.e. Max 24 months; Min 6 months; "permanent"
    - Or phrases such as "minimally necessary" or "contractually transparent agreement"
- The right to make copies of such data, if possible. For instance, a photo or particular purchase record may have an expiration date, but the equivalent of a "right click" can often make a non-expiring copy. Legal? Or is this beyond the realm of what the international community should consider?
- The right to transfer information to a third party

The SCT is *not creating law*, but offering guidelines for countries to adopt in common to preserve order but ensure user trust. It might be said that the SCT is fostering that "trust-based ecosystem" or "digital ecology ethic" as a response to data extinction.

International Data Security Challenges

Note that almost none of the above conditions for use are exclusively the realm of sovereign governments. That is, while Denmark may make use of personal data, its governments and businesses are very often transacting that data to and from other countries. What good is a French privacy law on criminal records if Singapore chooses to publish a French citizen's arrests? What happens to my personal purchase records if I buy a UAE product from Rakuten (Japan) and have it shipped via a Danish ship to my home in Mexico and have the transaction record stored in third-party files and banks in Austria, the UK, and Ukraine? How effective is Interpol if its needed drug trade data is compromised in a data-sharing country?

Some work here has already been done. The EU's General Data Protection Regulation (GDPR) spells out what data may be kept, under what conditions, and who is responsible. More, it punishes (mostly by fine) violators of EU data whether they are in or out of the EU ("What is GDPR").

The critical point here is that if the global community cannot find agreement on data rights and protection (or the appropriate government/business use of it), the possibilities for data breaches and financial and personal damage continue, and citizen trust is further eroded. When so many companies (from one-person LLCs to larger corporations) do business across international borders, with the proliferations of international non-profits, association memberships, banking institutions, and even organizations like the UN, these guidelines might be better articulated.

Resolutions

Committee resolution(s) will address the principles upon which decisions for data use will be appropriately established in a time when data extinction by users is a real possibility. It will define–where it is able–the types of data governments and business entities will reserve a right to keep and the durations of that retention.

The best resolutions will offer not only a policy framework on self-destructing data for member nations to adopt, but appropriate penalties for parties which might misuse it.

They will in the resolution or a Special Statement, identify how their guidelines fulfill the rights and requirements of individuals, businesses, and governments.

Questions to Consider:

Like the GA, identifying your own nation's position on data use is a good first step. In the face of (nearly) inevitable user-defined data extinction, are there any data uses that your country would consider limiting?

In addition,

1. Are there methods for bolstering citizen trust in data security that your country has not yet employed? How could they be? (Doing so may reduce the amount of data that vanishes from now trusting users.)
2. Which types of data seem most critical to government function? Which would be convenient but perhaps not necessary? Which do not merit discussion and may be left to users to choose?
3. Consider all of the ways such data is collected by your government. Which data can have a shorter lifespan because you know you can easily collect it again? What data collection challenges does your country have that makes this question harder to answer?
4. What about data which is important to the nation's historical record? Is it important to mark the records of athletes, inventors, infamous criminals, or celebrities and leaders differently?
5. Web3 makes private networks and economies possible. Is there a different kind of data (perhaps now undefined) which needs to be considered, collected, or secured?
6. Details in resolutions are often resisted by nations who do not wish to be held so directly or measurably accountable. What phrases can you imagine might be acceptable to most member states in terms of data protection and accountability?
7. If an international crisis were to develop that required cooperation, what information about citizens might be necessary to have available? To receive from a neighboring country?