SEMMUNA 2024

Rethinking Data Security:

Global Implications of Re-Imagining Data Access

Topic Overview

Topic Explanation:

In an era where data breaches are becoming increasingly common and damaging, the global community must reconsider traditional approaches to data security. As passwords and even multi-factor authentication technologies still fail to prevent private data loss–and as data and privacy breaches wreak havoc on human finance, social reputations, and–increasingly–democratic politics, this committee will discuss alternative approaches to data privacy. The goal is to reduce the value of such data, to limit access to data by corporations and governments, and to prevent its misuse.

This topic is not so much about the technical side of data privacy but the ethical and legal understandings of it. Inevitably, whatever the committee decides will have large scale impacts on international relations, human rights, and global security.

Committees may consider, for instance:

- The concept of self-destructing data
- New technologies to seal/protect data
- A Declaration of Universal Digital Privacy Rights
- The mass release of data from all privacy protections
- A new ethic of “digital ecology” for government and corporations
- Digital abstinence as an individual right
- Re-educating societies to the absence of privacy altogether

Along the way, delegates might ask:

- How might this new understanding operate at an international level?
- How might these approaches affect state sovereignty, corporate interests, and individual privacy rights, legally and ethically?
- What consequences might result for scientific and scholarly research?
- What consequences might result for military and strategic data?

As it is, the variety and accountability of state and non-state hacking is so far-ranging that no single approach to data privacy or its legal protections has been agreed to. As the 21st century opens up to the succeeding generations of AI, one statement stands to dominate every aspect of civilization, and we must decide what it will mean: “Knowledge Is Power.”

1. General Assembly Committee: "Committee on Data Privacy and Human Rights"

Approach: The General Assembly will focus on broad, foundational questions about data privacy, human rights, and the role of international governance. Delegates will debate which of several philosophies of data privacy the international community should invest in:

1. Cognitive Adjustment: A status quo approach to protecting data privacy as each state is able, but accustom the world to the loss of privacy.
2. The creation of a Declaration of Universal Digital Privacy Rights and what it might guarantee.
    a. Whether a right to Digital Abstinence should/can be included.
3. Data Extinction: Adding a self-destruct "tag" to all data which automatically erases it at a certain date
4. The creation of a Digital Ecology Ethic for governments and corporations which demands they limit use of data resources, responsibly dispose of it, and invest in expanding its safe use.
5. Perfect Contextualization approach: Disempower those who hold data against others by intentionally removing all privacy expectations for all information.

Key Objectives:

- **Philosophical Foundation:** Settle which approach (or combination of approaches) the international community will adopt.
- **Regulatory Framework**: Draft resolutions that outline international standards for data, including recommendations for implementation.
- **Ethical Implications**: Debate the costs to individual and societal happiness, justice, and prosperity under the framework.
- **Global Impact**: Assess the differing impacts on developing countries, on nations with different human rights ideologies, on market incentives to develop new inventions.

Expected Outcomes:

- A resolution that proposes a new philosophical foundation to data privacy and initial guidelines for its use
- Expectations for states and corporations in handling data that could be considered sensitive or a potential target for cyberattacks.
- Determining key questions that must be addressed by future debates on the topic.

2. Specialized Committee: “Committee on Technology, Corporations, and State Sovereignty”

Approach: This committee will dive deeper into the implications of self-destructing data enabled by individuals on any of their personal information or by institutions of information “leased” to the outside world. It will examine the potential uses and abuses of this approach for multinational corporations (MNCs) and state actors. Delegates will make recommendations for implementing this approach across a range of social, business, and government applications, amending the framework as necessary.

Key Objectives:

- **Corporate Role**: What individual data might require long-term use? What corporate data should be tagged “no expiration date”? What regulations should be employed to assure compliance?
- **State Control vs. Abuse**: Discuss scenarios where states might require control of access to private information. This could be in areas of media access, historical data, security information, and the personal information of power holders.
- **Balancing Sovereignty and Security**: Examine cases where one nation’s control over data expiration could affect another’s sovereignty, such as in international arms deals or cross-border business operations. In an age of MNCs, IGOs, and other multinational players, how would this play out?

Expected Outcomes:

- A resolution which offers:
    - A policy framework addressing the use of self-destructing data by corporations, including standards for compliance and penalties for misuse.
    - A statement on how the framework fulfills the rights and requirements of individuals, corporations, and governments.
- Guidelines for states on the responsible use of data extinction policies, especially in sensitive contexts like military technology or critical infrastructure.

3. Security Council Crisis Committee: “New Frontiers in Digital Sovereignty and Cyber Arms Control”

Approach: The Security Council will focus on the intersection of data privacy technologies and international security, specifically exploring how self-destructing data could affect military strategy, cyber warfare, and diplomatic relations. This crisis committee will tackle high-stakes scenarios where expired or inaccessible data could lead to (or mitigate or prevent) international conflict. The crisis will likely develop around an existing global conflict, so delegates should be familiar with existing international disputes.

Key Objectives:

- **Cyber Arms Control**: Debate the implications of military equipment or software being subject to expiration. How could this technology be weaponized or lead to strategic vulnerabilities?
- **Digital Sovereignty Conflicts**: Analyze scenarios where one nation’s ability to “kill” software remotely might be seen as an act of war. What are the red lines, and how should international law address such actions? Consider data extinction tags in areas of infrastructure, finance, or social communication.
- **Response Mechanisms**: Develop protocols for responding to breaches or abuses of self-destructing technologies, including potential sanctions or conflict de-escalation measures.

Expected Outcomes:

- A Security Council resolution defining what constitutes an act of aggression or cyber warfare related to data expiration technologies.
- Crisis management protocols that outline international responses to potential abuses of data self-destruction in military and strategic contexts.

Summary

This topic allows for a nuanced exploration of the future of data privacy and security across multiple levels of international governance. The General Assembly will handle broad frameworks with regulatory and ethical considerations, the specialized committee will dive into state and corporate responsibilities, and the Security Council will focus on crisis scenarios that could destabilize global security. Each committee's approach encourages delegates to engage with the complexities of innovative data security measures and their far-reaching implications.