BACKGROUND PAPER:

General Assembly Ad-Hoc Committee (GA)

Reframing Data Privacy in an Age of Lapsed Security

Introduction:

Some Data Privacy Failures:

- **2018 - Aadhar India Breach** - A database with files of more than *one billion* citizens was breached; it included fingerprints, retina scans, photographs, etc. The identifying information of nearly every citizen of India was sold with black market buyers paying approximately $10USD/file.
- **2024 - Canada's Giant Tiger Breach** - 26 *billion* records from the retailer (including those of companies that do business with GT) were leaked due to a third-party security breach.
- **2012 & 2021 LinkedIn Breaches** - The 2012 breach of professional data included passwords and payment information for 167 million users. After LinkedIn paid damages and updated security, 2021 saw another 500 million users lose data from their site due to web scraping. (Husain)
- **2024 Microsoft Midnight Blizzard Attack -** An unrevealed number of emails of government agencies and businesses were compromised, but more than 60,000 emails from the US Department of State were attacked.
- **2024 United Health Group Attack -** Data was ransomed after an attack on the insurance company responsible for over 50% of all medical claims in the US, disrupting pharmacies, hospitals, and labs.
- **2023 London Metropolitan Police Attack -** The employee records and assignments of 47,000 officers was exposed, including those undercover and in counter-terrorism units.
- **2022 LastPass Data Breach -** Hackers obtained access to password security company's third-party cloud storage services. (Parr)

Significantly, this list is only a sliver of the scale and frequency of major online attacks of governments, businesses, financial institutions, social media, infrastructure, and technology companies tasked with security.

> ***In brief, citizen concerns about loss of control of personal data are significant and widespread, but not yet as widespread as the threat itself or the failures of existing protections.***

In 2024, the major threats to data are caused by a wide array of causes: social engineering, third-party exposure, configuration mistakes, artificial intelligence cyber threats, dns tunneling, insider threats, state sponsored attacks, ransomware, trojan horses, drive by cyber attack, poor cyber hygiene, cloud vulnerabilities, mobile device vulnerabilities, internet of things, poor data management, and inadequate post-attack procedures ("Top 16"). Regardless of approach, data breaches of personal information now occur every 11 seconds (King).

<u>And Another List of Data Privacy Failures:</u>

- A banker gained access to health care records, identified individuals with cancer, and called in their mortgages.
- Consumer Reports found that 40% of insurance companies share health data with employers, marketers, and financial institutions without permission ("Privacy Case").
- In 2023 Instagram paid almost $70 million in fines for use of facial recognition software without consent.
- Six Flags amusement parks retained fingerprints of visitors without consent and was sued in 2019. Other companies, such as White Castle, have violated the law in keeping fingerprint scans of their employees (Ikeda).
- In 2014, the Cambridge-Analytica/Facebook scandal found that former Trump partners and UK Brexit advocates harvested the profiles of millions of people to target them for political influence (Graham-Harrison).
- Religious affiliations and sexual orientation are not globally recognized as "sensitive data" and are consequently not protected equally in all online environments.
- Taliban control of biometric data in Afghanistan gives that government fairly complete records of people and their families; the government has targeted journalists, political opponents, human rights and women's rights advocates, and LGBTQIA+ peoples. The country has no data protection laws ("New Evidence).
- In 2010, the Israeli Intelligence Agency Mossad used the identity of an Australian woman in order to conduct an assassination of a Hamas leader.

She was named a suspect along with similar victims from the UK, France, Ireland, and Germany (King).

The good news is that these UN Committees are *not* tasked with plugging the holes, chasing the hackers, or re-designing the technology. The technological arms race is well under way, and so plummets the population's confidence in their data security and privacy: personal and financial.

There are those who lament that younger generations no longer have the same concerns for data privacy as older people. This could not be further from the truth. While Baby Boomers are least prepared to meet data security challenges and are most concerned about emerging threats, Millennials and Generation Z'ers show high concern about protecting their data–largely for social reasons– and invest significantly more time working to keep it secured (Holmes and "Generation Privacy").

In brief, concerns about loss of control of personal data are significant and widespread, but not yet as widespread as the threat itself or the failures of existing protections.

Background & History - Complex, Long-Term, and Costly:

While nations have responded to the crisis to widely different degrees, it is evident that a global coordinated response has arrived very late. Barely 70% of countries have any national legislation on the topic at all; among developing nations, less than half do. Over a quarter of member states have not reported any protection laws for consumers, suggesting that it is lacking ("Data Protection"). The UN system itself did not document such a policy until 2018.

It has been argued that the Universal Declaration of Human Rights (UDHR) guarantees the Right to Privacy in its Article 12, and that the International Covenant of Civil and Political Rights (as well as similar agreements) echoes that protection in its Article 17. And while the Council of Europe (not the EU) has conventions on personal data protection, its most recent language is from a 2001 protocol to a 1981 convention; an addendum drafted in 2018 is still not yet in force.

Perhaps the most work on data privacy internationally is with the Organisation for Economic Cooperation and Development (OECD), itself practically concerned of course with the confident interchange of global commerce rather than of human rights. Across its primary convention of 1981, its amendments in 2013, and follow-up reports in 2021, the OECD has acknowledged the enormous difficulties in aligning privacy rights and policies across borders, let alone compelling nations to adopt or enforce any. The hardest language in these documents are merely recommendations for nations to cooperate and develop standards.

In the meantime, it has created a few of its own principles and standards, recommendations in principle adopted by (only) 46 UN member states. These include the notion that:

> Protecting people's privacy is essential for fostering a trusted environment around the collection and use of data. Privacy also acts as a driver for data sharing and the generation of economic and social value ("Privacy Principles").

But that isn't possible without a complex and change-responsive system of international cooperation around not just *technology, but legal and human rights agreements* working not just in alignment but without hole or seam and in full transparency of similarly funded and trained data protection authorities. (*Whew!*) And this recommendation came before the widespread advent of AI, which carries additional challenges to building trust and enhancing privacy.

In brief, the OECD Guidelines of 2013 provide language for a **"trust-based data ecosystem."** This last term, an environmental metaphor, may be the first and best way to thinking about the challenge and its complexity, especially if we imagine each human as a minute but essential component of it. The areas the OECD addresses in the ecosystem are:

collection limitation	data quality	purpose specification	use limitation
security safeguards	openness	individual participation	accountability

Delegates can likely puzzle through each of these as they wish, but first imagine the mathematical variation possible in creating policy around these for business, government, and individuals in every data circumstance possible. Put simply, the guidelines may be roughly framed in, but the policy possibilities are infinite.

Not only are the UN system and its member states slow and lop-sided in their approach to data privacy, and not only is the current complexity of the situation seemingly beyond a globally-consistent solution, but the future of the data security challenge looks both to magnify the complexity and its cost. The average cost of any given data breach globally is nearly $5 million USD ("Global Average"). As we look forward to the "promise" of quantum cryptography and AI-assisted security, it's certain that the costs of quantum work (literally encoding data at the subatomic level) are prohibitive: far more than most governments (let alone individuals and health care systems, for instance) can afford (Swayne, & L. Alexander). More, neither quantum work nor AI guarantee that hackers will not also develop tech to balance this security.

> ***The status quo damage is widespread, significant, and always changing, and it will continue into the future as its complexity and costs increase, resisting the efforts of UN member states to create a framework that might manage it.***

The Current Debate:

This Ad-Hoc GA Committee has been charged with addressing entirely different frameworks for approaching data privacy and security as a means of addressing the challenges. In other words, rather than argue privacy and security as it has for the past 45 years, would the world be better served if we re-imagined the entire debate?

Fortunately, thinkers on this topic before SEMMUNA have already advocated for some approaches, though none are easy or address every concern. Still, perhaps one or more will prove better strategies. What follows are brief descriptions of each proposal[1] the Ad-Hoc committee will consider and recommend or not.

Cognitive Adjustment:

Perhaps we should consider that–in most cases–government and technological agencies will be unable to protect privacy as we might wish. Instead, we might better rely upon human coping capacity and adaptability. In other words, as technology and society shifts, so too does human behavior and thinking about it. We surrender our notions of privacy and "absolute secure stability" for an expectation of constant change. As a solution for many data breaches (those involving social currency–personal documents and postings–and much biometric data), this may be viable.

It is clearly limited when it comes to economic and financial considerations or those which involve criminality. These would require different solutions. However, if we could be conditioned to "accept" that what seemed true of a political candidate or friend from a "post" or even of ourselves a year ago is not true today, we might shift our ideas of what privacy should be limited to. Put another way, we might be taught to ignore or become skeptical of electronic data and move back to a reliance upon personal memory and face-to-face transaction. In business and criminal prosecution,

[1] Except where noted, these frameworks are derived from similar arguments made by Viktor Mayer-Schonberger in his book, *Delete*, which I have updated to today's uses.

the conditions of confidence might also make this shift. Similarly, to accomplish this, we might begin to limit the data that we commit to digital storage (Boyd).

Can we condition the world to rely less upon digital storage of data? Is this essentially a surrender back to the 1970s? It's impossible to reverse the digital universe we've created, but it may be possible–with the proper social conditioning and re-education–to limit the data security frontier to the worlds of government and high finance who can afford it, and then allow the global population to relax over what any of the rest of the "data" means.

But which data must remain secure? And how would we alter global attitudes?

Digital Abstinence

This perhaps requires the least work on behalf of nations beyond guaranteeing its use. It relies upon the idea that once individuals understand the risks and costs to privacy loss, they will elect to cease sharing their information with others. If there is no significant digital memory of any individual, they can move more freely and with less risk. Indeed, this has been by absence of resources the default position of many developing nations.

This is not specifically anti-technology behavior, but it relies upon individuals educated in the risks of data loss and thereby limiting their participation in the flow of their own information. Such an education is not remotely easy, however, not with social media triggers and financial incentives to spend instantly. And it isn't as if people are not aware of the dangers now; it's just that they–for whatever reason–value the online environment more (imagine giving up social media, Amazon, and Google). It can also be argued that the digital world has an unprecedented power to serve as a global community, a product of inestimable value.

It also might work best when the business and financial sectors do not *insist* upon a digital record only. Perhaps a "digital abstinence light/lite" is more appropriate: that we rely on educated individuals simply to be more cautious, to themselves investigate the uses companies put to their data, and for companies to adjust their practices.

Other problems here, too: the first is a *power imbalance* in information between a company and the individual: the individual must "trust" the company needs *x* information without fully understanding why. More, if most of that person's neighbors choose to "sign on," the pressure to join is increased (and the pressure on companies to change reduced). Finally, what becomes of the data given is not addressed, and most data breaches and abuses involve third-party use, databases storing information, and information sold to others.

Digital Privacy Rights

Acts of digital abstinence or cognitive adjustment might–if properly framed–benefit from a more global declaration of the rights of individuals to digital privacy in the first place. As indicated earlier, however the number of member states who have such laws (or are even considering them) is low; more these national rights are a far cry currently from a more universal acceptance and commitment to them. At present, the most open comments are that these are "assumed" under the UDHR and ICCPR.

But at the heart of any concept of rights is a principle: that individuals have a legal claim to maintaining informational control. This does not stop hackers, data abusers, or failed data storage incidents, but it does demand a legal accountability for those failures.

There are a number of ways this might be framed.

- Data privacy as a "property right" - If we think of a piece of information (say, a home address or phone number) as your personal property, and then you give that to the post office, there is no reason they cannot also transfer/sell that piece of property to someone else. Another way of thinking is necessary.
- Purpose Limitation - Most data privacy policies limit not the information itself but the purposes to which it can be put. That way, if a doctor shares your health information with a hospital, or a bank keeps your contact information, they cannot use it to, for instance, bombard you with spam. So no matter who has your phone number or how they acquired it, there are only certain purposes it can be used for. Think of it as not *whether* someone can use data, but *how* they can.
    - In the US, such laws are generally based around government use of information. For the private sector, each individual contracts with the company for the purposes of their data (think when we click on the "Terms of Service" and "User Agreements" which explain these). In Europe, however, the laws extend to all public and private groups who may use your data

Unfortunately, even though individuals have legal protections under the condition of their own consent, creating such laws at all is quite difficult, even in places like the US; more, individuals in Europe seldom use the laws; and who can say how long an under-used law will survive into the future? Perhaps an international standard would be of greater use.

At the basis of most personal data use is trust, either in the business/institution data is given to, or in the government to enforce laws against its misuse. And what if the government does not itself believe in privacy regulation? (Consider the Nazi invasion of the Netherlands in the 1930s when the religions and ancestry of millions of Dutch

citizens was seized for the purpose of persecution. Today's nations, too, are not in agreement about the individual's right to privacy. If not, what good a Declaration of Rights?)

The first steps towards any Declaration of Privacy Rights must be 1) in understanding how we want to describe those rights: who has the rights, what these are; how those rights are restricted by purpose; for whom; and for how long; 2) What manners of accountability are recommended: within nations, amongst regional groups, or the global community; the party(ies) held responsible for violations–nations, corporations individuals, etc.; the punitive measures recommended for violations; 3) following up with education and the means for individuals to use the Declaration. Privacy International is one organization that has placed most of its weight in these projects ("Learn").

It's important to note, too, however, that international Declarations–especially in the human rights realm–act as broad principles and recommendations, never themselves vehicles for enforcement or accountability. As profound a document as the UNHDR is, for instance, it isn't possible for anyone to be sued using it. And, except for the most extreme abuses of human rights (genocide or war crimes), the UN cannot take action against violators. It can, however "call upon" member states to do so, urging and recommending. So while a Declaration of Data Privacy is helpful in aligning UN member state ambitions and ideals, it will likely do little immediately practical to eliminate any of the instances described at the beginning of this paper.

> ***Will our re-framing of digital rights depend upon individuals, on laws, or upon technology?***
>
> ***Will we strategize about information power or about how we think and make decisions about data use?***

Digital Rights Management Technologies (DRM)

This is a fairly familiar concept in the world of Intellectual Property (IP): securing files against sharing (think ebooks, video games, and professionally-recorded films). The age of streaming and digital creation has obviously undermined its effective use, but this does not prevent us from using the technology to literally encode and contract personal data at almost every level.

Any time personal data is released to a government or business, for instance, a closer description might be that the data is being "sold" as a contracted use. (Old-school DVDs are intended for home use, not viewed for profit, etc. They are intellectual property with copyrights.) The same would be true here: data (such as

phone numbers, health records, criminal files, financial records) would be “encoded” with meta-data tags that described its purpose and uses. Receiving institutions would have to use the correct software to even open it and understand its uses. Violators (hackers, data pirates) would be prosecuted in the same manner and with the same set of laws as copyright violators.

More, it is possible that individuals who sell their data for use could, on their own or as a group, use market economies to re-value that price. Consider the model, for instance, of Amazon Kindle ebooks, which are technically “sold” to individuals as a right-to-read loan; at the time of their choosing, that right can be rescinded unless a re-purchase is made

Relying on a technological solution to data privacy, however, still has some of the same problems as password protections and other encryptions: it is only as good as those who keep the information, and the technological arms race (very costly) continues. Even so, individuals might have more power to choose how their data is used and what ways they might use to hold third parties accountable.

There are other problems with the DRM system. One is that all data is at some moment “unencrypted” for use (the DVD is viewed, the video game played) and it is at that moment that the data can be copied without the DRM protections or tags. More, the hacking of DRM systems is big business online (consider methods to strip iTunes songs from their protections, to break PDF file protections, or any number of game hacks offered for free or fee). In addition, how are individuals themselves to know if their data has been misused? Presently social media companies like TikTok and YouTube have automated programs to spot protected IP (with only some degree of accuracy), but how would individuals do this across the entire globe for all of their personal information? (The rise of a new business model, perhaps: this author has his own credit card companies scouring the dark web routinely for his personal info, not that he can do much about it if something is found there. And keep in mind, I had to give those companies my personal information to store and use in order to search for me!) Finally, and this seems most challenging, how would individuals themselves find the means and time to encode all of their data properly and update that coding as new hacking methods develop?

The Digital Ecology Ethic

Think of this in terms of how we might best treat the environment. Can we create a set of regulations that limit businesses, governments, and institutions to:

- what information may be collected
- what information may be stored
- who may store it
- how long it might be stored?

Over 90% of the data breaches and damages are the result of poor data storage management and of vast databases of information being retained for far longer than might be essentially needed.

Governments that collect information on their populations would future-proof that data from hacking or abuse if it never collected it in the first place or retained it for, perhaps, less than a single year of study (Balkin). Consider this in the cases of religious or ethnic identification, credit ratings, etc. Businesses would retain only the essential payment and delivery methods of purchases for the lengths of their business return policies. Health care providers might digitize only internally-networked data that signaled when private conditions (diagnoses or test results) needed to be temporarily encrypted and exchanged but not retained. Criminal records that are designated as “expunged” (for instance, at the end of a sentence served), would actually be deleted (along with DNA records). The European Court of Human Rights in 2008 ruled that DNA records of the innocent could not be kept forever, for instance. Microsoft and other larger companies are more and more adopting “information ecology” rules, which essentially say that user data can only be kept for the minimum amount of time required of business purposes or to meet legal requirements.

Such an ecological principle, properly implemented, might easily reduce the largest dimensions of data breaches and circumvent many security challenges. However, it may miss a key dimension of privacy expectations: it leaves the decisions for what data is protected or not to governments and laws rather than to the individuals who have a stake in its protection.

But another problem emerges, and that is government and financial security. Since Sept 11, 2001–and despite some new corporate data policies–data *retention* is on the rise, not its extinction. Think, for instance, of various wars on terror, investigations into organized crime and international drug trafficking, etc. Even telecommunication companies retain data “in case” they are needed for law enforcement. Because of Sept 11, international law enforcement has moved from solving crime to working to prevent it, and this requires the combing of vast amounts of data. As a consequence, governments create more laws demanding that corporations retain information longer.

Finally, the seeming epidemic of corporate and financial sector corruption which has defrauded millions and caused its own economic collapses across the world has produced new calls for “transparency” in many areas: from workplace safety to nutrition labels on food, and from cumbersome finance record reporting (US Sarbanes-Oxley of 2002) to environmental law adherence, information of all kinds is kept for inspection to combat corruption. Without these laws, what trust do we have in business?

Nevertheless, threading the needle between information *needs* and mere information *desires* may be possible.

Perfect Contextualization

This may seem too radical for most. However, it raises enough questions about our data privacy assumptions that it is worth including.

First, understand that anxiety around the loss of data is because we assign that data *value*. Hackers and abusers of information exist because data can be used to a *profitable advantage*. That profit is often financial, but not purely: profit is also found when another receives a degree of power with that data: that might be social power (the embarrassing Snapchat photo saved and shared) or political power (the closed meeting recording or image taken out of context and used for propaganda), for instance. And, in most cases, that advantage is created when one party has more data than another, when one party can distribute the data (often selectively) to their own best advantage.

We keep framing the data rights argument in terms of how we can restrict the flow of information, prevent others from gaining access to the data. *What if we reversed it?*

> ***This isn't Big Brother because everyone is watching everything. It isn't surveillance, but "sousveillance" (we watching us).***

Imagine, then, a global environment not of privacy but of transparency, in which (pretty much) all data was always available to anyone who wished it? In other words, for any bit of data (a health record, a criminal file, a bankruptcy proceeding, "that" photo taken at the party), we could always know the complete picture, the whole story. No one would have a true advantage over anyone else. Indeed, the video/meta age of technology is moving us rapidly in this direction, where many humans are become more "lifeloggers," offering every detail of themselves to the world. We create a true digital memory of everything.

First reactions are any number of dystopia movies, of the "panopticon" evil (an all-seeing eye watching over us), but this is not the same thing. Complete surveillance plots only work when power is out of balance: this isn't Big Brother, because everyone is watching everything. It isn't surveillance, but "sousveillance" (we watching us) (Gandy).

Intriguing, but not without flaws, of course. The first is that it is unreachable, and if so, then the power imbalance would continue. Our behavior *would* change under such conditions of being ever-recorded. And the global village or global family would

become closer to reality, perhaps socially scoring individuals who do not conform. (The very reason that we value privacy is for some things not to be seen by our mothers.) More, it isn't access to data so much as the uses to which it can be put: financial organizations and governments will likely always have more resources to correlate, analyze, and act upon data than individuals. Even so, one of the chief struggles of emergent AI technology is a lack of complete information for it to deliver satisfactory/reliable answers. And, since the human attention span itself is brief (*I'm* not going to sift through and analyze the treachery hiding in that credit card loan offer), AI may be the best tool to do so.

In some senses, this framing of data is emerging now, in any event. The world's citizens and governments are reeling from the possibilities. Perhaps they will be dull and benign; but here is, perhaps, an opportunity to define who–if anyone–or what–if anything–might be exempted from the sousveillance universe. How do we limit the power imbalances which might result? Suggesting to governments–any governments–that they must relinquish data power is no small order.

Data Extinction

How can individuals retain control of most all of their data, even after it has been given to a government or business? Part of the answer may be in a single simple addition to that data: an expiration date, selected by the individual. For every document, photo, upload of information, etc. in addition to the "Save/Submit" button would be a field for expiration which would automatically be enacted at that point.

The key to this framing of data privacy is to change the behavior of individuals online, to slow them down (even if briefly) to consider the possible uses and needs of the data they are releasing to the world. Indeed, this technology is already in use across much of the internet: outdated Wikipedia entries are revised; scheduled posts are often deleted automatically when an event passes. In the mid-2000s, Google, Microsoft and others even engaged in a bidding war about how many days they would "save" users' private search histories, each deleting that history after a shorter and shorter period. Now we can often "purge" our search histories and caches with a single click. This would be similar but more extensive: the expiration would be a user-defined meta-tag that would be a "ticking" portion of the file wherever it traveled.

The European Union has already weighed in on some applications of this approach as far back as 2008, looking at RFID (digital identification) chips. They recommended automatically "deactivating RFID chips" to empower "user control" (Council of the European Union).

As intriguing as this possibility is, it also has limits and complications. First, this cannot be strictly a technological solution; it still must be supported by legal protections (such as anti-tampering by receivers of information or DRMs on that information). More, in many instances, users may be unfamiliar with how important

some data is, so some data may have prescribed minimums or maximum lengths of existence (for instance, employment W2s to be kept for five years or a doctor's health records for a single year past the life of the patient).

For ecommerce and similar transactions where more than one user is involved in the production of data, a negotiation of date might be required. Amazon, for instance, might say that they "must" keep data for six months and so a consumer would have to agree to that minimum, though Ali Baba or Walmart might offer the same product transaction with a shorter minimum. What of photos where there are many people who might need to negotiate? What of government records? And don't larger agencies like banks still have enough power to cause the negotiation for extinction dates to be unfair? What about libraries and archives of history? Some individuals may have a desire to "forget" or return to privacy even when social interest wants to remember history and learn from it. More, what if–after a piece of data vanishes into the digital shredder–the individual later discovers they want it back?

At the heart of the data extinction framework is the question not only of privacy but of human memory, individual and social. Trying to decide what types of data should be preserved *against individual wishes* would be a fascinating human rights debate!

In Summary:

None of these seven frameworks for data privacy is perfect, though they may also be used in various combinations. The point is ***not to solve*** the entirety of the data privacy debate, just as we have been unable to solve international conflict, poverty, organized crime operations, or global illiteracy rates. Instead, through a re-envisioning of the topic, we might reduce the impact of a failing data security system. If we ignore all of these approaches and return to the status quo, there is every reason to expect the problem will grow both more expensive in its technological "patches" and the costs of their failure.

	Addresses Digital Power	**Addresses Thinking and Decision-making**
Individual Behavior Change	Digital Abstinence	Cognitive Adjustment, Data Extinction
Legal Changes	Privacy Rights Defined	Digital Ecology, Data Extinction
Technology Changes	Privacy DRM	Perfect Context, Data Extinction

The Ad-Hoc GA Committee is not tasked with **solving**. Therefore, delegates should not allow the debate to be bogged down in small details raised as an attempt to

derail the debate: “My grandmother lost her prize chicken recipe to Pilsbury, and your method won’t fix that, therefore we should not use your method!” Instead, in larger, macro-level strategic thinking, is some combination of these both more effective and more agreeable to nations than the status quo’s under-discussed and rarely-agreed upon approach?

—

Committee Mission

The Ad-Hoc GA Committee on Data Privacy and Security is charged with making recommendations for the appropriate framework(s) to adopt globally in addressing the data privacy crisis, to create a “trust-based ecosystem” for data privacy and security.

If the resolution offers one or more frameworks for recommendation, it should indicate through operatives or pre-operatives its rationale for these recommendations and any conditions or details it can make in the brief session for adoption. The more answers it can provide, the better.

Similarly, the resolution may explicitly *not* recommend some frameworks; if so, the rationale for rejection must be offered.

Finally, where details are not settled, the resolution should provide an agenda for later committees of specific questions that have yet to be addressed. The Ad-Hoc Committee may recommend these be discussed in a variety of global or regional conferences, one or a series; may place these questions for discussion only in home governments; may place these questions for agendas in existing or new UN bodies; or may call for a unique method of addressing the concerns. Remember, too, that this UN committee is an assembly of governments only, perhaps not the only stakeholders in this debate.

Whatever approaches are used, the recommendations should provide for the means to address future challenges as the nature of data and technologies change.

Good luck!

Geo-Political Challenges to Consider:

Of course, selecting the "most effective method" is one thing, but the real challenge may emerge in bringing together different nations around the idea, especially those which vary widely in each of the three sub-topics here: technology, law, and the nature of human rights.

Human Rights

To say that nations vary in their own definitions around human and civil rights is understatement. Still, every nation *has* signed on to the UNDHR and ICCPR, and the right to privacy (related to human autonomy and individual dignity) is echoed in dozens of regional agreements around the world. Some nations sign on understanding that such documents are 1) aspirational or ideals towards which to strive, not to always achieve (even an historically global leader like the US regularly is called out for violations); and 2) such Declarations in international law are not directly enforceable as a result. Mostly, governments who resist this dimension of the discussion argue that data retention and surveillance are necessities to combat crime and thus protect their people. Typically, the UN encourages and supports nations in achieving HR goals rather than seeks punishment for failures.

Technology

As with all imbalances related to resources and the demands for development, any frameworks related to technology use will rely upon several areas of resources that are not shared. Technology infrastructure (access to the internet itself, for instance) is still not globally available, and while mobile/cell networks are proliferating, the costs and hardware to carry the most advanced protections is not universal, nor are standards for telecommunications and data exchange. More, when asked, countries most in need of development are tasked with other resource needs to combat poverty, disease, illiteracy, and the like.

Law

A nation's laws most often reflect the cultural ideologies of its people. Aligning the laws of nations to satisfy the needs of a framework is not a small undertaking (in fact, this is the very business of the UN, in one key sense). So rapid adoption and response to changing technology may fail here, even if we could agree on human rights and provide resources for technology. And even if nations were to agree, the effectiveness of legal systems (corruption, policing resources, court failures, process protections, etc.) vary widely, as well.

Questions to Consider:

1. Would it be easiest to approach the problem from a legal, technology, or human behavior angle? Is data privacy and failures a problem of misaligned power or of bad individual choices? The table on page 13 may help you in narrowing down a framework that fits your thinking best.
2. Consider your own nation's approach to this issue:
    a. How effective are its technological, legal, and educational institutions? Why?
    b. What policies does it currently have on data privacy and security?
        i. How effective have these policies been?
        ii. What challenges remain?
    c. What are the relationships between the government, private business, and technological advancement? Who controls what, and which areas are autonomous? How does this complicate the issue?
    d. How does your nation balance the seeming conflict between human rights and national security?
    e. Does your thinking on Question 1 align with what you are answering here? Where might changes need to occur?
3. Focus on improvements to the current crisis, not full "solutions." Which harms does your approach work to reduce?
    a. Explain *how* your ideas reduce any of the problems listed in this paper.
    b. Note what problems are *not* solved (and leave yourself open to the ideas from others to add here, then).
4. Consider implementation, how to achieve the plan, a roadmap from now to the working system.
    a. What steps need to be taken (list them), and how long might each take?
    b. How will your plan be quickly updated as change happens?
    c. How will you know if your plan is effective? (How will you measure success?)
    d. What methods for holding parties accountable (not necessarily guilty through a system of enforcement) will you use?
5. Where might other nations resist your ideas and *why*? How can your plan accommodate their needs?
6. What frameworks from this paper would your nation reject and why?
7. What additional problems might be solved by your approach to this topic (beyond mere data privacy help)?