PUBL363 Policy Brief

International Policy Management

Mehul Sen

May 2021

1 Introduction

Technology is evolving exponentially, the internet connects people around the world, irrespective of their geographic locations. According to statistics published by Leftronic for 2021, roughly 40% of the world's population has access to the internet and 90% of the world's data was generated in the past two years (Lynkova, 2021). IT companies are no longer limited to single countries, most of them have international headquarters and data is constantly flowing through geographic borders. This means that the data gathered by these organizations are no longer subject to a single set of policies and data privacy regulations, but instead, the data has to be managed based on the policies of the various server locations in different countries, with different laws applicable to them. This brings up a whole new set of challenges, that we have no previous experience in solving. An intergovernmental organization like United Nations could be the solution to this issue. They could oversee creating standardized policies and make sure that data privacy and management laws are streamlined as well as making it easier for businesses to propagate internationally.

2 Audience

This implementation needs the involvement of many different nations, and this can be brought forth by the United Nations in order to unite the different cyberspaces and ensuring regulated and smooth data flow as well as a conflict resolution. United Nations has been a valuable asset when it comes to providing aid and assistance to various nations as well as bringing forth the economic development of different nations (Bright, 2013). It has proven itself capable of effectively handing international policies and agreements. An effort to unite cyberspace can also be conducted by the UN, which would be benefiting for all the member nations.

3 The Problem

Data privacy and management laws are very different for most countries. Each country has its own set of issues and to deal with them, it has its unique set of rules and regulations. It enforces laws and regulations with the assumption of what is best for that country. This is also applicable in the field of cybersecurity, where the data regulation and data privacy laws for a lot of countries are different depending on the country they apply to. Certain countries emphasize maintaining the privacy of their citizens, to accomplish this, they have drawn out data privacy laws to regulate how IT companies should collect, store, and manage their customer data, as well as what regulations apply to sharing that data with third parties. A good example of this would be the European Union and its policy on the protection of individuals with regards to user privacy and processing of personal data (*Data protection in the EU*, 2021). On the other hand, we have countries that allow the collection of personal data and mass surveillance of their citizens. This allows them to rapidly act on any possible threats to the country before they have a chance to rise in severity. Some governments like North Korea, China, and Russia follow this principle (*Internet Censorship 2021: A Global Map of Internet Restrictions*, 2021). Some countries are not completely developed and do not have concise data privacy laws and regulations in place yet. With such a diverse set of policies across the world, it is very difficult to implement strong data and privacy laws that can be accepted and implemented by everyone.

One thing that all these countries do have in common is their dependency on businesses. Each country wants to expand its business infrastructure, they want to ensure that their economy increases. As of lately, one of the leading industries in the world is the tech industry. It is one of the fastest-growing in the world's economy and shows no signs of slowing down (Wolinsky, 2020). With most of the businesses moving online, every nation needs to comply with these businesses or risk losing a big part of their economy. The biggest players in the tech industry as of now are IT Companies like Facebook and Google. These companies are expanding internationally to increase their audience and customer base. This expansion requires collaboration between both the governments and the companies itself. By allowing them to operate within their countries, the government ensures that they are not at the risk of getting left out, on the other hand, this allows the private companies to grow. Businesses are no longer restricted to certain countries and tend to expand internationally to larger markets which is much more profitable and for them.

The issue arises when these companies share user data through the internet to servers located in different countries around the world. To comply with the policies imposed by these different countries, their privacy policies are made even more complicated. There is no clear consensus on how this data should be handled and due to the differences in policies and regulations, legal loopholes are created. This brings up situations where data privacy laws can be neglected risking the safety and privacy of individuals. In terms of policies, this is unexplored territory, never in human history has this much personal data been collected before, much less transported across geographical boundaries and stored at different parts around the world.

4 Rapid Cyberspace vs Established Cyberspace

As governments are realizing this, they have started taking action. Policies are being made based on where they stand concerning data policies and sharing data with other nations. At this stage, governments all around the world have a choice, working individually or collaborating with other nations. Working individually gives them complete authority over policies and laws that get enforced, this would make it easier to impose restrictions and monitor data flow. This also gives them the benefit of setting up a secure cyberspace fast. This would ensure that they become one of the leading countries in terms of policies, laws and managing their cybersecurity issues. However, this would make conducting international business much more difficult. Since they will not be able to enforce their policies and laws throughout that business, eventually leading to the nation closing itself to international businesses that do not comply with their policies and seriously impacting their own economy.

Since the internet itself has no boundaries, data travels all across the world, bouncing from server to server, located all around the world. Imposing restrictions on the data that can enter and leave countries would be extremely difficult to implement and would severely restrict the capabilities of the internet as we know it. As Bruce Schnier put it "The internet works differently ... Communications between Rio de Janeiro and Lisbon might be routed through Florida. Google doesn't store your data at its corporate headquarters in Mountain View;

it's in multiple data centers around the world" (Schneier, 2016). The other option is for governments to collaborate and work on a standardized set of data laws. Given a couple of years, this could lead to a less cluttered set of regulations and data privacy laws that seamlessly aligns itself with the different data laws in place in different countries. Working together with multiple nations would allow for a more robust cyberspace. This option would be much more effective in the long term when most of the nation's catch up with each other. The incentive for more advanced countries to share common international data policies with their less-developed counterparts would be to establish their own businesses over them. The less-developed nations would agree to this because they will get the opportunity to adopt robust cybersecurity policies and regulations as well as establish common data laws with the more developed nations speeding up their own development.

5 Recommendation

As we have done so in the past with different territories like land, ocean, and space. Cyberspace is not much different, with good policies and regulations, data flowing through nations can also be managed properly. UN is one of the few bodies that have successfully handled past international conflicts and issues. This makes them more than capable to handle cyberspace conflicts and create standardize policies. UN could take the first step in unifying different nations and setting forward a set of policies that are agreed upon by different nations. They can preside over international agreements made by countries to agree on how data should be shared among each other as well as oversee the data shared between different governments ensuring that data privacy laws are maintained. Having a central standardized set of policies would benefit every member nation that is a part of this agreement since this would allow faster implementation and changes as newer technologies get adopted. Since every member nation would comply with these policies, the businesses between these countries would no longer need to navigate through complicated obstacles. Member nations would be able to work together and collectively vote on changes and modification of these policies and any disagreements and issues that arise would also be remediated effectively with the UN acting as an intermediary.

We are already seeing similar collaboration initiatives like European Union's general data protection regulation that standardized the privacy policies for many countries in Europe. UN could simplify and standardize the policies applied to data regulation, making it easier for international companies to implement privacy policies that are inviolable. This could also prove useful in instances where governments have to work together and share their data and resources. As described by Josephine Wolff in chapter 4 regarding Operation Tovar, international governments came together and collaborated to combat the GameOverZeus botnet (Wolff, 2018).

Governments would also be incentivized to associate themselves with these standardized policies as it would allow them to expand their business and boost their economies, at the same time building a much safer and securer cyberspace. This implementation would not be cheap and would require large investments and various governments to work alongside each other, however, this could unify us as a society, it could also take us one step closer to creating a simpler and safer version of the internet while also providing us with a long term solution to international relations concerning data and privacy.

References

Bright, J. (2013, Dec). *Benefits of being a member of the united nations organization.* Retrieved from `https://hosbeg.com/benefits-of-being-a`

-member-of-the-united-nations-organization/

Data protection in the eu. (2021, Jan). Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Internet censorship 2021: A global map of internet restrictions. (2021, Feb). Retrieved from https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/

Lynkova, D. (2021, Feb). *How fast is technology growing statistics [updated 2021].* Retrieved from https://leftronic.com/how-fast-is-technology-growing-statistics/

Schneier, B. (2016). *Data and goliath: the hidden battles to collect your data and control your world.* Norton.

Wolff, J. (2018). *Youll see this message when it is too late: the legal and economic aftermath of cybersecurity breaches.* MIT Press.

Wolinsky, J. (2020, Oct). *The top 10 most successful sectors in tech.* Retrieved from https://www.valuewalk.com/2019/03/top-10-successful-sectors-in-tech/#:~:text=Thetechnologyindustryisbyfarthefastest,economyandshowsnosignsofslowingdown.