PrivacyNama 2021

October 6 & 7

MEDIANAMA

PrivacyNama is a global conference by MediaNama on key themes related to privacy regulations, and the inaugural edition was held on October 6 & 7, 2021.

The conference featured a stellar lineup of speakers including Data Protection Commissioners, Chief Privacy Officers, and researchers to understand international and global perspectives on privacy legislation: What are the trends that we're seeing in privacy regulations in the BRICS countries? What does it take to operationalise a privacy regulation? How do global businesses adapt products and practices across territorial jurisdictions? What are privacy regulations doing about protecting data pertaining to bodies of individuals? How is privacy legislation impacting the openness of the Internet?

Session #1
Bodies and Data Protection
Session Chair: Nehaa Chaudhari, Ikigai Law

- Amber Sinha, Executive Director, Center for Internet and Society
- Anja Kovacs, Director, Internet Democracy Project
- Beni Chugh, Dvara Research
- Jhalak Kakkar, Executive Director, Centre for Communication Governance, NLU Delhi
- Professor Mark Andrejevic, Monash University

Session #2
CyberBRICS: Impact of privacy legislation on the openness of the Internet
Session Chair: Vrinda Bhandari, Internet Freedom Foundation

- Alexa Lee, Senior Manager - Global Policy, ITI Council
- Dr. Alison Gillwald, Executive Director of Research, Research ICT Africa
- Dr. Andrew Rens, Senior Research Fellow, Research ICT Africa
- Luca Belli, Head, CyberBRICS Project, FGV Law School, Brazil
- Udbhav Tiwari, Public Policy Advisor, Mozilla

Session #3
Operationalisation of Privacy Legislation
Session Chair: Malavika Raghvan, Future of Privacy Forum

- Marit Hansen, Data Protection Commissioner, Land Schleswig-Holstein, Germany
- Raymund Enriquez Liboro, Chairman, National Privacy Commission, Philippines
- Teki Akuetteh Falconer, Former Exec. Director, Data Protection Commission, Ghana

Session #4
Negotiating for adequacy: enabling cross border data flows
Dr. Ralf Sauer, Deputy Head, International Data Flows and Protection Unit, European Commission, in conversation with Nikhil Pahwa, MediaNama

Session #5
Adapting To Global Privacy Legislation
Session Chair: Rahul Matthan, Trilegal

- Idriss Kechida, Chief Privacy Officer, Match Group
- Justin B. Weiss, Global Head of Data Privacy, Naspers & Prosus
- Srinivas Poosarla, Global Chief Privacy Officer and DPO, Infosys

MediaNama hosted this event with support from Facebook, Flipkart, Internet Society, Mozilla, Mobile Premier League, Omidyar Network, Paytm, Star India, and Xiaomi. We are thankful to our community partners, CyberBRICS project, the Centre for Internet and Society, and Centre for Communication Governance at NLU Delhi, and other friends and colleagues, for their help with the programme and outreach.

> PrivacyNama 2021 saw participation from a diverse group of entities like Hero Corp, Microland, Reliance Jio, Times Internet, NODWIN Gaming, Exotel Techcom, Shaadi.com, Thomson Reuters Foundation, ICANN, ZestMoney, Interel Group, Netflix, Salesforce, Info Edge (India), Disney India, Hike, Indian Institute for Human Settlements, Doosra, Google, Mythos Labs, MxM India, Asia Internet Coalition, IBM Corporation, Embassy of France, Human Rights Watch, GIZ GmbH, Data Secure, Ideosync Media Combine, CUTS International, Ashoka University, ICRIER, British High Commission, Indian Competition Watch, Machinist, Vodafone Idea, Snapchat, among others.

This report aims to capture the key points raised during the two-day conference.

1. You can read detailed coverage of PrivacyNama 2021 on MediaNama
2. You can also watch the live-stream recordings on MediaNama's YouTube channel

I. The Data Protection Authority Playbook

Have the right person at the top: After the laws are passed, the first step to setting up a data protection authority is having the right political buy-in. Leadership is very important because the Data Protection Authority will be a new institution. It helps to have a driving chair that is assertive and is willing to provide clarity by breaking down theoretical concepts into something beneficial. For example, Ghana's Data Protection Commission was first headed by a highly respected and retired Supreme Court justice that had a lot of knowledge about human rights issues.

> ***There is no particular playbook in organising data protection authority. However for starters, as an authority, you have to assert your leadership. So that many of your constituents will be looking to you for leadership and clarity — Raymund Liboro, Chairman, National Privacy Commission, Philippines***

Secure resources: Putting in place the right resources is going to help enable the Data Protection Authority. In Ghana, it took more than 3 years for the DPA to be allowed to hire permanent staff. This was due to a lack of financial resources and human resources.

How to solve a constraint of resources?

1. Strategically prioritise the most important resources
2. Try and learn how others do it
3. Develop relationships with players in the global community
4. Cooperate and collaborate with them for solutions

Make the Data Protection Authority visible: In terms of perception, the DPA has to be visible while ensuring that privacy disasters are avoided. In Germany's Land Schleswig-Holstein, the DPA's powers and perception saw a major shift in the right direction after citizens became aware of their right to privacy and thus, wanted data protection authorities to help them.

> ***It's my job to prevent disasters, still, if there are no disasters it seems that people don't learn. Similarly, also show the solutions — Marit Hansen, Data Protection Commissioner, Land Schleswig-Holstein, German***

Build awareness: Taking out an awareness campaign is a key step to kickstarting a DPA. Creating awareness can be useful in demystifying the subjects from the technical standpoint. These campaigns help develop a humane outlook that allows people to identify more closely with data protection issues. In fact, the DPA for Philippines came up with a strong awareness campaign in the first year itself. While these awareness drives are being carried out, one can use that time to build capacity and train personnel. The media can be

of great help in spreading awareness. When Ghana's DPA was starting out, they had to leverage traditional media to an extent that the press became their partners in helping identify public issues around data protection.

Give time for companies to be compliant: Afterall, Ghana took 5 to 10 years to operationalise the law. In that time period, the Ghana DPA spent the first 3 or 4 years creating awareness. It's registration exercise took another 3 or 4 years after that. However, Germany's DPA was a lot quicker as it gave just two years for compliance. This was because the country already had a privacy directive in place even before the GDPR. So, most of the German companies had already put in place most safeguards.

> ***One of the things we realized at that time with a staff of five, was that there was no way we could register all data controllers across the country manually. So, we had to leverage technology — Teki Akuetteh Falconer, Former Executive Director, Data Protection Commission, Ghana***

Avoid turf wars: When one or two government institutions have similar rules, or their functioning clashes with each other, it often turns into a powerplay issue. This is not uncommon in governments. Ghana's DPA would have fallen for such a trap were it not for the right people being appointed at the beginning as they put in place a governance structure and ensured that the DPA had a key institutional role.

Bring regulators and institutional reps on board: Encouraging buy-ins at the board level from critical sectors like communications, information technology, and banks also helps the DPA push forward. In this way, it is easier to disseminate the importance of decisions taken during meetings.

Distinguish between subjects of the law: There are generally two types of non-compliant bodies — the first type could be totally non-compliant because they don't understand the law. The second type may be compliant with the law on paper i.e. they may have a registered Data Protection Officer, but they are waiting for the DPA to guide them.

How should a DPA handle the non-compliant?

1. A DPA's strongest powers, like the power to prosecute, must be reserved for those who are wilfully violating the law.
2. Administrative powers of a DPA are more useful than prosecuting powers as it allows the authority to change something. An order that a company's approach to data processing has to change in order to be compliant or that the data subjects have to be notified about a breach, is much more important than fines.
3. The DPA should pave the way for companies willing to be compliant with the rules by providing requisite information on a website.

4. Keep the message simple. By doing this, companies will naturally know their way around compliance.
5. Don't make them think of data protection as a sort of legal obligation. Instead, it should be positioned as something that will help them build their credibility.
6. Talk about the role of data protection in eliminating corruption and promoting transparency in order to grab the attention of government players.
7. Issuing fines may not be such a good idea as companies have started accounting for these fines in their annual budget.

Naming and shaming should be the last resort when dealing with non-compliant entities. This measure particularly helps when dealing with the public sector as the public sector cares more about perception.

II. Who can be a Chief Privacy Officer?

Someone with more than just a law degree: Typically, companies begin by assuming that the privacy leader should be a lawyer. But very quickly, what they discover is that a legal background is probably not sufficient. A full suite of skills is necessary. Although, the salary range for a Chief Privacy Officer (CPO) is similar to that of a mid-level attorney.

Someone who reports to the board: The CPO needs to report directly to the company's board to avoid interference from other functions within the organisation. It is very important for the CPO to have the ability and autonomy to report issues directly to the top. CPOs also need to seek sponsorship from the highest level of the organisation for their privacy agenda.

> ***You need to find that sponsorship at the highest level, and employees need to be aware of that decision or policy the company has so that when those decisions are taken, they know where it comes from and they know why it makes sense for the company — Idriss Kechida, Match Group***

Someone who lets the boss make assignments: People are rewarded and recognised for doing work that their bosses expect of them. If a CPO comes in and expects them to do the work, it seems like a favour. But if the boss says you've got to do this thing, and you're going to be rewarded and recognised on that basis, that's significantly different.

Someone who can budget resources: There are three crucial elements to consider when budgeting for an in-house privacy initiative: The number of people required which will depend on the nature of the business, automated services that offer to make it easier for your company to implement privacy measures, and training including automated training modules and creating original video content.

Someone who adheres to high privacy standards : It can be a challenge for companies operating in multiple jurisdictions to comply with local privacy legislations. A good fix for that is companies can adapt to a single privacy standard that makes them compliant in most jurisdictions.

Someone who can address customer concerns: The role of any data protection authority, at least in part, is to address privacy issues brought up by citizens. But CPOs may need to shoulder the burden too.

> ***Effectiveness lies in listening to requests properly and take them as an opportunity for improvement. If you don't, these same people will go to the data protection authority — Srinivas Poosarla, Infosys***

Someone who can balance user privacy with company growth: The way to think about risk management for privacy roles is slightly different because you're not just thinking about the risk to the company. The CPO's primary duty is to think about risk to individuals. Of course, that leads to conflicting priorities between the privacy of individuals and the company's growth. But the right approach is to steer clear of a yes or no approach.

> ***The question is not, should you take away all algorithms, yes or no. The question is, what are the features of an algorithm that balance in a proportionate way the need to do what the algorithm is supposed to do — Justin Weiss, Naspers & Prosus***

III. Key Insights on Cross-Border Data Transfers

Data adequacy is a status granted by the European Commission (EC) to countries outside the European Economic Area (EEA) who provide a level of personal data protection comparable to that provided in European law.

How would the EU determine if India has an adequate level of data protection?

Make an informal request: Countries approach the European Commission first with an informal request about whether they would be willing to engage in a dialogue because adequacy is based on a very thorough assessment and therefore, it requires certain meetings where you go through the rules of the country. Many countries are interested because the free flow (of data) is important to offer services in the EU or to European customers, which in today's world often requires obtaining personal data from the European Union.

> ***Adequacy is not a requirement of identity. It requires a high level of convergence but we are not expecting that countries' data protection laws are a photocopy of EU's rules — Dr. Ralf Sauer, Deputy Head, International Data Flows and Protection Unit, European Commission***

Conversations are confidential: Since the EC's adequacy finding is not a given, the conversations are confidential. These talks are kept confidential until a draft decision is adopted by the EC. After that, it is left to the third country to make it public as countries do not want a negative finding that data adequacy is not possible.

Observations shared on countries' data protection law: There are certain instances where the EC will approach a country while the latter is in the process of drafting a law. This allows for a discussion on certain elements of the draft law which could become problematic later on for an adequacy assessment. The country can take these observations into account but the decision is fully sovereign.

Countries can conduct their own self-assessment: Although it is not a formal requirement, some countries conduct a self-assessment of their data protection law and the rules which are relevant for a data adequacy decision to go in its favour. This helps to speed up the process. There is also some guidance from data protection authorities on how to apply the adequacy test. The self assessment is done typically against that guidance paper.

Meetings with the country: The EC will typically ask the third country about whether they are implementing rules, whether they have guidance papers, anything that illustrates and explains how these rules apply in the country. When it is close to finalising the data adequacy assessment, there is another discussion on gaps. Not every difference is of importance but if there are crucial differences then we discuss whether there is a way to bridge these gaps.

> ***We go through a process where we have meetings with the country and go through their data protection law. For instance, we need to carry out an assessment on the limitations in safeguards for access to data by criminal law enforcement authorities or by National Security Authorities — Dr. Sauer***

Submission to National Data Protection Authorities: The EC drafts a decision based on its data adequacy assessment, and the decision is shared with the country to make sure that the EC has correctly understood what was revealed over the course of the meetings. This draft decision is endorsed by the EC at a high political level and then sent as a draft to the EU's National Data Protection Authorities which come together in the European Data Protection Court. They prepare an opinion on the draft decision and when this decision is public, there is another check to see if there is something which needs to be addressed or clarified about the decision.

Approval from EU Member States: The last two steps are — there is a special committee with representatives from the EU member states, with whom the data adequacy decision is discussed. The EU representatives then vote, and a majority vote means that the data adequacy decision has been green lighted.

> ***We have to not just look at how the data will be protected in the third country but also if it could be then transferred to yet another country without protections because then the protection is incomplete in a world where data flows easily — Dr. Sauer***

What needs to be kept in mind while applying for adequacy?

1. Certain essential elements like rules on purpose imitation and data security must be there. The country must guarantee rights to individuals, and provide oversight by an independent authority.
2. There must be an element of necessity in proportionality that data cannot be processed for whatever reasons.
3. There can be differences in how exceptions to certain rights are formulated but they need to be framed. They cannot be unlimited, you cannot undermine individual rights by having broad exemptions.
4. Data adequacy can be rejected if there are big carve-outs for certain economic sectors that exempts them from the data protection law.

5. Always have a horizontal data protection law that covers all sectors, including the public sector.
6. The Data Protection Authority has to be independent. The authority has to be effective in what it can investigate, the tools it has for the investigation, and the measures it can impose at the end.

Question marks on India's draft data protection law: Some of the grounds for processing by public authorities, whether they were sufficiently framed, raised eyebrows. The law on data transfers is quite strict in terms of data localisation. Concerns were raised about their impact on India's trade and fragmentation of the internet. Although India's Data Protection Authority is meant to be independent, there were some provisions which cast doubts in terms of the government being able to give directions through the authority.

> ***It is better not to have them and trust that such an authority can function and will do very good for India without a need for the government to keep control over it — Dr. Sauer***

IV. Key Trends in Privacy Legislation

Different countries have different concepts of privacy: For instance, there are many important aspects in which China's Personal Information Protection Law (PIPL) differs from GDPR and other privacy regulations from around the world. A key difference is that the PIPL is not a law by itself, it's a set of broad principles that enables specific rules to follow. The PIPL's focus is national security as opposed to individuals and when it comes to cross-border data transfers, data processing entities have to pass a security assessment by China's regulator. The provision which allows the government to blacklist overseas data controllers and processors from processing Chinese personal data, and the lack of a provision for an independent data protection authority stand out in the PIPL.

Expect delays in on-ground implementation: South Africa has had the Protection of Personal Information Act (POPIA) for several years now. But several aspects of the law really only became operational after close to a decade. Despite the country's history of developing policy in time, it was different with the POPIA because the adoption was not there. Institutions that existed in law had not been established. Even when they were established, the necessary institutional capacity and the autonomy required to perform functions in a way that protects individuals, was not there either. Finally, lobbying from an influential private sector that argued that it was too onerous for them to comply was also a reason for the delay.

What is the law, versus what is actually practiced: Brazil's General Law for the Protection of Personal Data has a "nice authority" but that's only on paper. In practice, Brazil has been dragging its feet on its data protection law for two years. A key concern is that the data protection authority in Brazil is severely under-resourced, not just financial

but intellectual resources as well. Not to mention that it depends directly on the office of the cabinet of the President of the Republic.

> ***If you want the regulation to work, you have to invest in it, and then it works well, if you're not ready to invest in it, it's really useless [...] You need to have very well-trained lawyers and data scientists and this costs money because if you don't pay well, these people will go to work for Google and Facebook. — Luca Belli, CyberBRICS Project***

The push for data sovereignty: There are essentially two drivers of digital sovereignty - One, the free flow of data is highly asymmetric. For instance, there's only a couple of powerful US-based corporations that are harvesting the data collected around the world. Second, data localisation is gaining traction because the alternative is to let Big Tech companies continue to exploit the data.

> ***The reason I think that localisation is getting so much power right now is there's not a great alternative. The alternative is Facebook can exploit us — Dr. Andrew Rens, Research ICT Africa***

Impact of digital sovereignty on the internet: There is a concern that data localisation will have us all in silos and we'll be able to barely speak to each other on the internet. But that will largely depend on the global political economy. For example, it will depend on whether the US will create a data protection regime that doesn't tolerate its own exploitative corporations. When the US draws boundaries around surveillance capitalism, other economies will tolerate integration with the US because there's a level of protection. But the barrier for compliance shouldn't be too high as with the European Union. It creates problems as developing countries may not have the resources to comply with all the standards.

> ***Very often I think we're seeing this notion of digital sovereignty being used as a fig leaf to include provisions or push for ideas that may not necessarily be in the best interest of the subjects of [India's PDP] bill — Udbhav Tiwari, Mozilla***

Will data localisation help drive economic value?

1. No, it will not. In fact, data becomes valuable only when it can come into your country, when it can flow out and be exchanged with the rest of the world.
2. Data localisation is not practical. Thinking that you can keep all the data in your own country and that you will make the best use of it is more or less a pipe dream.
3. The value of data comes from how it's being used, not how it's stored. But exploiting data can cause people to lose trust in the data ecosystem. This will lead to people either refusing to give their data or giving inaccurate data.

4. Data nationalism raises concerns. In China, data localisation measures are used to support surveillance and thus, assert greater social and political control.

> ***It's not surprising, countries like Russia and China are the most significant users of data localisation, because it'll align with their political goals — Alexa Lee, ITI Council***

V. Key Challenges to Effective Regulation Of Biometric Tech In India

1. There is absolutely no incentive right now for companies to actually invest in a privacy policy or models for clear, informed, and granular consent-seeking documents.

> ***Our data and our body are so intimately interwoven that what we call our virtual bodies and our physical bodies, the line that is supposedly dividing these two becomes irrelevant, even if you can argue that maybe it exists — Anja Kovacs, Internet Democracy Project***

2. There is ambiguity around the legal standing of any biometric-based technology deployed by the government as it is usually based on SOPs that are often not in the public domain.

> ***AI systems are being developed in the western world and very often just being translated fairly blindly into other contexts — Jhalak Kakkar, National Law University Delhi***

3. The Indian government needs to disclose information on the procurement of biometric systems, data storage processes in these systems, the duration the data is retained, how it is being shared, etc.

> ***Risk-based regulation is like an educated compromise because we know that we're not going to have enough State capacity and enough institutional bandwidth to go and regulate every person out there who has data — Beni Chugh, Dvara Research***

4. Stakeholders are not being given enough chances to give their perspectives on the Personal Data Protection Bill which was first introduced in 2019 and is currently under consideration by a Joint Parliamentary Committee.

> ***Essentially what the draft [PDP Bill] does is it takes power away from the private sector and gives it to the government. That needs to change — Amber Sinha, Center for Internet and Society***

5. The landmark Puttaswamy judgement is being violated by the Indian government with no consequences due to minimal judicial review and legislative oversight

> ***I think it's going to be very important to think about these inferential uses [of biometric tech] and how they can be used for new forms of social sorting and discrimination — Mark Andrejevic, Monash University***

6. There needs to be frameworks that guide the industry on complying with the Puttaswamy judgement's three-prong test.

Essential Reading

1. **Biometric Recognition**
    a. Lucknow Safe City Project: Uttar Pradesh To Deploy Facial Recognition, 'Label' Faces Of Suspects [Read]
    b. Why A UN Body Is Raising The Alarm On Biometric Recognition Tech In Public Spaces [Read]
    c. The Use Of Facial Recognition Technology For Policing In Delhi: An Empirical Study Of Potential Religion-Based Discrimination [Read]
2. **Privacy Legislation in BRICS Countries**
    a. A Complete Guide To India's Personal Data Protection Bill, 2019 [Read]
    b. Summary: China Passes GDPR-Like Data Privacy Law, Except That Many Restrictions Do Not Apply To The Government [Read]
    c. Several flaws in South Africa's draft data and cloud policy, say experts – ITWeb [Read]
    d. An overview of Brazil's General Data Protection Law – IAPP [Read]
3. **Data Sovereignty & Cross-Border Data Flows**
    a. Consumer Impact Assessment of Data Localisation [PDF]
    b. Data Localisation: India's Double Edged Sword? [PDF]
    c. India's Data Localisation Policies Have Hidden Objective And This Is Affecting Its Growth: Study [Read]
    d. India's Digital Policy Agendas Are Gradually Resembling That Of Other BRICS Nations [Read]
    e. EU backs personal data flows with Britain as deadline looms – Reuters [Read]
    f. European Commission adopts adequacy decision on Japan – EU [Read]
    g. EU's adequacy decision for South Korea – IAPP [Read]

***MediaNama* is the premier source of information & analysis on Digital Policy in India.** *We focus on key issues like privacy, data governance, fake news, misinformation, cybersecurity, cyber diplomacy, digital payments policy, Net Neutrality, intermediary liability, website blocking, internet shutdowns, data localisation, e-commerce policy, IoT, content regulation and censorship, among others.*

Our mission is to help build a digital ecosystem which is open, fair, competitive, and global.

***On MediaNama.com**, our reportage attracts a readership of policy professionals, government officials, Members of Parliament, startup founders and business leaders, as well as investors with an eye on policy developments shaping the future of the Internet in India.*

***MediaNama's events** enable meaningful conversations for a high quality and curated audience to discuss opportunities, challenges and issues that they care about, in a manner that helps in building capacity. The fact that they are among peers with similar depth of understanding, and come at the same issues from a different point of view, ensures that our audience keeps coming back for more.*

Nikhil Pahwa | Founder & Editor | nikhil@medianama.com
Harneet Singh | Operations & Partnerships | harneet@medianama.com

MediaNama.com | Twitter | Facebook | YouTube | LinkedIn
Subscribe to Telegram | Newsletter