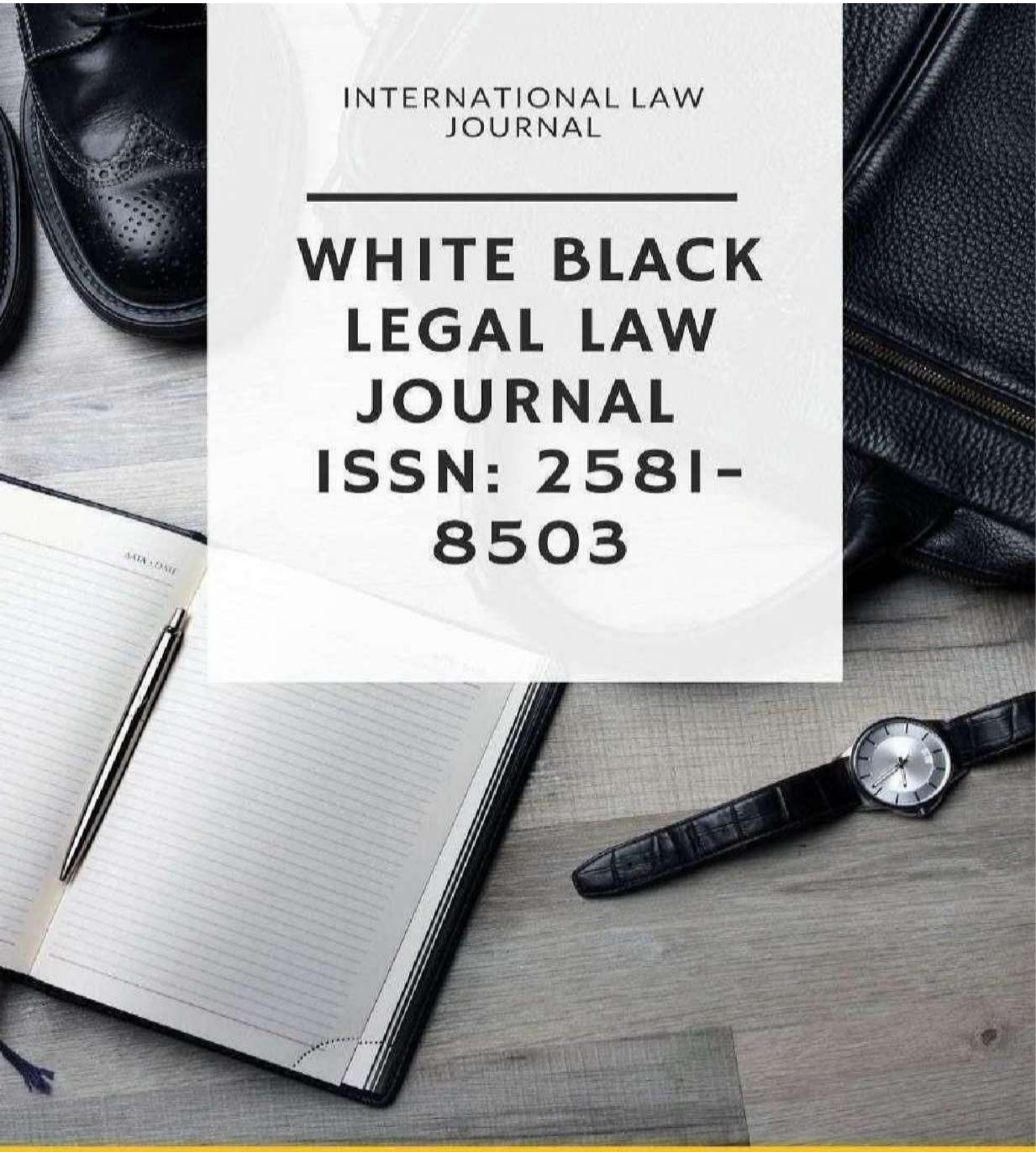

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

IMPLICATIONS OF EMERGING TECHNOLOGY ON PRIVACY LAWS

AUHTORED BY -SHRIKANT SHARMA

Emerging technologies and our understanding of privacy

In the previous sections, we have outlined how current technologies may impact privacy, as well as how they may contribute to mitigating undesirable effects. However, there are future and emerging technologies that may have an even more profound impact. Consider for example brain-computer interfaces. In case computers are connected directly to the brain, not only behavioral characteristics are subject to privacy considerations, but even one's thoughts run the risk of becoming public, with decisions of others being based upon them. In addition, it could become possible to change one's behavior by means of such technology. Such developments therefore require further consideration of the reasons for protecting privacy. In particular, when brain processes could be influenced from the outside, autonomy would be a value to reconsider to ensure adequate protection.

Apart from evaluating information technology against current moral norms, one also needs to consider the possibility that technological changes influence the norms themselves (Boenink, Swierstra & Stemerding 2010). Technology thus does not only influence privacy by changing the accessibility of information, but also by changing the privacy norms themselves. For example, social networking sites invite users to share more information than they otherwise might. This "oversharing" becomes accepted practice within certain groups. With future and emerging technologies, such influences can also be expected and therefore they ought to be taken into account when trying to mitigate effects.

Another fundamental question is whether, given the future (and even current) level of informational connectivity, it is feasible to protect privacy by trying to hide information from parties who may use it in undesirable ways. Gutwirth & De Hert (2008) argue that it may be more feasible to protect privacy by transparency – by requiring actors to justify decisions made about individuals, thus insisting that decisions are not based on illegitimate information. This approach comes with its own problems, as it might be hard to prove that the wrong information was used for a decision. Still, it may well happen that citizens, in turn, start data collection on those who collect data about them, e.g.

governments. Such "counter(sur)veillance" may be used to gather information about the use of information, thereby improving accountability (Gürses et al. 2016). The open source movement may also contribute to transparency of data processing. In this context, transparency can be seen as a pro-ethical condition contributing to privacy (Turilli & Floridi 2009).

It has been argued that the precautionary principle, well known in environmental ethics, might have a role in dealing with emerging information technologies as well (Pieters & van Cleeff 2009; Som, Hilty & Köhler 2009). The principle would see to it that the burden of proof for absence of irreversible effects of information technology on society, e.g. in terms of power relations and equality, would lie with those advocating the new technology. Precaution, in this sense, could then be used to impose restrictions at a regulatory level, in combination with or as an alternative to empowering users, thereby potentially contributing to the prevention of informational overload on the user side. Apart from general debates about the desirable and undesirable features of the precautionary principle, challenges to it lie in its translation to social effects and social sustainability, as well as to its application to consequences induced by intentional actions of agents. Whereas the occurrence of natural threats or accidents is probabilistic in nature, those who are interested in improper use of information behave strategically, requiring a different approach to risk (i.e. security as opposed to safety). In addition, proponents of precaution will need to balance it with other important principles, viz., of informed consent and autonomy.

Finally, it is appropriate to note that not all social effects of information technology concern privacy (Pieters 2017). Examples include the effects of social network sites on friendship, and the verifiability of results of electronic elections. Therefore, value-sensitive design approaches and impact assessments of information technology should not focus on privacy only, since information technology affects many other values as well.

Tadayoshi Kohno[1], the Short-Dooley Professor of Computer Science and Engineering at the University of Washington, began the session by noting that the next panel would also focus on emerging technologies, with an emphasis on analytics and the cloud. He encouraged the participants to prepare questions to pose to panelists during the open discussion session. Kohno, as moderator,

[1] National Academies of Sciences, Engineering, and Medicine. 2016. Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community. Washington, DC: The National Academies Press. https://doi.org/10.17226/21879.

then introduced the following panelists and gave each of them 5 minutes for opening comments:

- Carl Gunter, professor of computer science, University of Illinois;
- Roxana Geambasu, assistant professor of computer science, Columbia University;
- Steven M. Bellovin, Percy K. and Vidal L. W. Hudson Professor of Computer Science, Columbia University; and,
- James L. Wayman, research administrator, San Jose State University.

Carl Gunter discussed privacy implications of the growing use and collection of digital health data. He distinguished between "health care" technologies (tools for diagnosis and treatment of disease) and "health" technologies (the quickly growing market of tools for disease prevention and encouragement of healthy habits, such as the Fitbit), and suggested that these two areas may be moving toward a disruptive convergence.

Gunter described emerging capabilities in analysis of both structured and semi-structured data, including doctor's notes or even information from a Fitbit or an Apple watch, and noted that data mining of electronic health records (EHRs) has led to the identification of prescription drug risks. Such capabilities could have enormous societal benefits, but they require access to large quantities of data about individuals, who may not want their records to be accessible even for such purposes.

He suggested that the rapidly changing field of health IT has a number of characteristics that could make it a useful laboratory for monitoring privacy trends and developments, including the following:

- There are many stakeholders with competing interests;
- Regulations and rules are evolving;
- Privacy provisions in existing laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act were developed following much public debate and negotiation;

- The field is seeing increased use of distributed networks where institutions hold data to support research, but share answers to research queries on their data;
- Analysis of health data can yield great public benefit (in the form of medical breakthroughs and advances in public health); and

- Collection and analysis of data can pose privacy risks.

Privacy Policy for Emerging Technologies

Emerging technologies such as artificial intelligence, machine learning, and the internet of things have become integral to our daily lives. However, these technologies also bring with them privacy concerns, which is why it's essential to update your privacy policy to reflect the use of these new technologies. This article will discuss how to update your privacy policy for emerging technologies.

How to Update Your Privacy Policy for Emerging Technologies?

Identify the Data You Collect and Process

The first step in updating your privacy policy is identifying the data you collect and process. This includes both personal and non-personal data. Personal data is any information that can be used to identify an individual, such as their name, address, or email address. Non-personal data includes information that does not identify an individual, such as their browsing history or device information.

Determine How You Use the Data Privacy Policy for Emerging Technologies

Once you've identified the data you collect and process, the next step is to determine how you use the data. This includes the purpose for which you collect the data, how long you retain the data, and who you share the data with.

For example, if you use artificial intelligence to analyze user data, you need to specify how you use the data and what insights you gain from it. You also need to specify who you share the data with, such as third-party vendors or advertisers.

Update Your Privacy Policy

Now that you've identified the data you collect and how you use it, it's time to update your privacy policy. Your privacy policy should be clear, concise, and easy to understand. It should also be written in a language that is accessible to the general public.

Your privacy policy should also include the following:

- The types of data you collect and process
- The purpose for which you collect the data

- The legal basis for collecting and processing the data
- How long you retain the data
- Who you share the data with
- How you protect the data
- Your users' rights about their data
- Privacy Policy for Emerging Technologies- Obtain Consent
- In order to update your privacy policy for new technologies, consent is essential. Before gathering and using your users' data, you must get their consent. Both non-personal and personal data are included in this.
- By giving their approval, you can be sure that your users are aware of and accept your privacy policy. It also indicates that they are aware of how and with whom you share their data. One way to get consent is by putting a checkbox on your website or by using a consent form.
- Educate Your Staff
- It's not enough to just update your privacy policy; you also need to provide your staff with training. Your staff members need to be aware of the privacy policy and how it applies to their roles. They also need to comprehend how crucial it is to safeguard user information Data breaches and other problems can be avoided by educating staff members on privacy regulations and cutting-edge technologies. Workshops, in-person meetings, or online courses are available for this training.
- Perform Audits on a Regular Basis
- And last, it's critical to regularly audit your privacy policy. It is important to periodically evaluate and update your privacy policy to take into account modifications to company operations, legal obligations, and evolving technology.
- You can find weaknesses in your privacy policy and make necessary corrections with the aid of routine audits. Additionally, it can assist you in avoiding new privacy issues and safeguarding user data.
- Talk about data breaches and security.
- Emerging technologies raise fresh security issues and hazards. It's critical to address these issues in your privacy policy and advise consumers of the safeguards in place to protect their

personal information. Access controls, firewalls, encryption, and other security measures might be a part of this.

- A section on data breaches should be included in your privacy policy as well. This section should define a data breach, describe how to report and discover one, and outline the actions you take to lessen any damage that may have been done.
- Give Control and Transparency
- Users demand control over their data and transparency. This should be reflected in your privacy policy, which should detail users' options for data access, update, and deletion. One way to do this is to provide consumers the option to refuse data collection or processing for certain uses.
- Users can also choose what kinds of notifications they get from your app or website. Provide them with the choice, for instance, to unsubscribe from push notifications or advertising emails.
- Think about regional and global privacy laws.
- There are regional and national privacy rules that you have to abide by. It's critical to comprehend these regulations and modify your privacy statement as necessary. This covers the CCPA, GDPR, and additional privacy laws.
- You might need to draft several versions of your privacy policy that adhere to local legislation if your business operates in several different nations or areas. For instance, you might require different privacy policies for users residing in the United States and the European Union.
- Be Open and Honest About Outside Services
- A lot of apps and websites leverage third-party services to enhance their capabilities or add new functionality. It's critical to include information about third-party services in your privacy policy if you use them.
- It is important to clarify what information is shared with third-party services and how it is used by them. In order to allow consumers to study the privacy policies of these services, you should also include links to them.
- Problems and Restrictions:
- There are a number of obstacles and restrictions to consider while revising your privacy policy for developing technologies:

- Training and ongoing instruction are necessary to make sure staff members are aware of the nuances of privacy policy modifications pertaining to cutting-edge technologies. Implementation problems could result from misunderstandings.