The Right to Remain Anonymous: How the GDPR Should Look to India and China to Fix the Incomplete Concept of Data Anonymization

By Moneeka Brar*

I. INTRODUCTION

The rise of the technology industry caused many countries to enact legislation focused on protecting individual citizens' privacy. Data anonymization, a protection layer, is one of the most significant safeguards implemented to protect individuals, but it is relatively unsuccessful in its current form. Two of the most significant problems with data anonymization are that anonymized data can still be easily retraced via reidentification science, and the fact that such retracing misinforms the way individuals think about data anonymization in their daily lives. This public perception should shift to acknowledge that data anonymization is a layer of protection, rather than total protection. By looking at how other countries approach the concept of privacy and exploring how they structure their data protection and privacy laws, a more globally unified system is possible. This uniform global system can emerge once privacy is acknowledged as a fundamental global right, thus fostering shared values around the world, wherein data anonymization is acknowledged and accepted not as total protection, but as a protective layer.

Which information will be privatized and which information needs to remain public are extremely debated topics in data protection and privacy law. There have been various approaches to solving this problem, with the European Union's General Data Protection Regulation (GDPR) at the forefront. Since its implementation, other countries have followed the standards set by the GDPR. This Note will focus on attempts to apply data anonymization to domestic privacy law in the European Union (EU), India, and China. Specifically, this Note analyzes the standard set by the GDPR—even though data anonymization remains unsuccessful in its present form within this framework—and considers

---

* J.D. Candidate, 2021, Syracuse University College of Law. First, I would like to thank my family for all of the support throughout my academic career. I would also like to thank them for constantly pushing me to my fullest and believing in me and the work that I accomplish. I would also like to thank Professor Keli Perrin for her guidance and Michaela Mancini for her invaluable help. Lastly, thank you to my friends who provided unconditional support throughout this process.

how other countries have tackled the issue of keeping individuals' information private. India and China were chosen as case studies because of their differing governments.

The first section of this Note will discuss the history and importance of data protection laws, explaining data anonymization itself. Within that context, the Note will then discuss the current shortcomings of data anonymization, and introduce the idea of reidentification. The second section of the Note will focus on analyzing anonymization. It will look at the GDPR's version of anonymization, and its failure from the outset as predestined by its focus on how anonymization was supposed to work based on its original context. It will then turn to India to analyze its attempt to replicate the GDPR in its domestic laws. Discussion of how India passed and enforces data protection laws will focus on India's switch to the Indian Aadhaar biometric database, and create a version of data protection and privacy laws in 2019.

It will then examine China's approach to implementing data protection and privacy laws from the perspective of a different government. After considering these countries' different approaches there will be discussion of how to fix their attendant problems, first by changing people's mindsets towards anonymization and its use, then by uniquely combining the various forms of safeguards from these different areas. Using these three countries, this Note will discuss and compare the different forms of safeguarding individual's private information to determine whether it is possible to make this specific safeguard more successful. This Note will conclude that, rather than specifically focusing on fixing anonymization in every area, countries should acknowledge that anonymization is unsuccessful in its current form, and encourage governments to be transparent and accountable for individuals' privacy interests.

II. HISTORY OF DATA PROTECTION AND PRIVACY LAWS AND ANONYMIZATION DEFINED

The United States conducted its most recent census in 2020.[1] During this year, every household in the country had to fill out and submit a form

1. *What is the 2020 Census?*, U.S. CENSUS (2020), *available at* https://2020census.gov/en/what-is-2020-census.html?cid=20402:%2Bwhat%20%2Bis%20%2Ba%20%2Bcensus:sem.b:p:dm:en:&utm_source=sem.b&utm_medium=p&utm_campaign=dm:en&utm_content=20402&utm_term=%2Bwhat%20%2Bis%20%2Ba%20%2Bcensus&msclkid=87a5911d1a2217b91b1ecf6868257653 (last visited Apr. 20, 2021).

to the federal government.[2] The form included identifiable questions about individuals' names, sex, race, age, telephone number, and a household's residence type.[3] These are identifiable questions because their answers make it possible to trace the form back to a specific person. While it is normal in the United States to fill out this questionnaire every ten years, the census raises the question of who exactly this form is being sent to and, more importantly, what is that recipient going to do with this data? These questions only give rise to more questions about individual privacy and whether keeping identifiable information private is a fundamental right.

However, to grasp modern-day data protection and privacy arguments, privacy's basic history must be understood. The right to privacy dates back to the late 1800s when Samuel D. Warren and Louis Brandeis wrote *The Right to Privacy*,[4] arguing that the first definition of privacy is the *right to be left alone*.[5] Since its publication, the importance of data protection and individual privacy has grown exponentially alongside the rise of technology.[6] Technological innovation is happening all around the world, with the EU front and center.[7] Data protection and privacy laws prohibit the disclosure or misuse of information about individuals; in recent years, the privacy of that information has emerged as a central issue.[8] Technology plays a prominent role in the emergence of data protection and privacy laws, with countries passing new laws to keep up with technological innovations.[9]

A country has data protection laws if any of its national laws provide a set of basic data privacy principles, and those principles are accompanied by officially-backed methods of enforcement.[10] In 1973,

---

2. *Id.*

3. *Questions Asked on the Form*, U.S. CENSUS (2020), *available at* https://2020census.gov/en/about-questions.html (last visited Apr. 20, 2021).

4. *A Brief History of Data Protection: How Did it All Start?*, EUROCLOUD (Jan. 6, 2018), *available at* https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/ (last visited Apr. 20, 2021).

5. *Id.*

6. *Id.*

7. Emily Stewart, *Why You're Getting So Many Emails About Privacy Policies*, VOX (May 29, 2018), *available at* https://www.vox.com/policy-and-politics/2018/4/5/17199754/what-is-gdpr-europe-data-privacy-facebook (last visited Apr. 20, 2021).

8. Daniel J. Solove, *A Brief History of Information Privacy Law*, GEO. WASH. L. FAC. PUBL'N & OTHER WORKS 1, 3 (2006).

9. *Id.*

10. Stewart, *supra* note 8.

Sweden became the first country to pass a national data protection law.[11] It was a simple law that only covered personal data processing in traditional, computerized registers, and did not contain any material provisions about when and how the data was processed or any other general data protection principles.[12]

A. Data Anonymization Generally

To anonymize is "to remove identifying information from [something, such as computer data] so that the source cannot be" easily discovered.[13] Anonymization also removes any information that would associate specific data with a particular individual.[14] An extensive amount of data can be anonymized, but anonymized data is simply data that would no longer be immediately attributable to an individual.

Anonymization was partially popularized by social science's attempts to learn about society and the people therein by studying individuals' patterns of behavior.[15] Direct identifiers, such as names, addresses, and telephone numbers, are easily traced to specific individuals.[16] There are also indirect identifiers that, when put together, could reveal the identity of a particular individual.[17] This process occurs by cross-referencing someone's job or social media presence with their surrounding area, thereby identifying an individual using that specific information.[18] This is only one example of how an individual can become traceable again. Anonymization in its proper form would not allow for the reidentification of individuals through indirect identifiers.

The public once believed that anonymizing data sets removed any risks to an individual's privacy and safeguarded the individual's

---

11. Graham Greenleaf, *Global Data Privacy Laws: 89 Countries, and Accelerating*, 115 PRIV. L. & BUS. INT'L REP. (2012).

12. Sören Öman, *Implementing Data Protection in Law*, STOCKHOLM INST. SCANDINAVIAN L. 390, 391 (2010).

13. *Anonymize*, MERRIAM-WEBSTER (n.d.), *available at* https://www.merriam-webster.com/dictionary/anonymize (last visited Apr. 21, 2021).

14. *Anonymize*, CAMBRIDGE DICTIONARY (n.d.), *available at* https://dictionary.cambridge.org/us/dictionary/english/anonymize (last visited Apr. 21, 2021).

15. Kristel Toom & Pamela F. Miller, *Ethics and Integrity*, SCIENCEDIRECT (2018), *available at* https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/anonymization (last visited Apr. 21, 2021).

16. *Id.*

17. *Id.*

18. *Id.*

identity.[19] Yet critics question its credibility, and many wonder if there is even a purpose to data anonymization.[20] Some critics argue that complete anonymization is impossible because other data sets will undoubtedly be released, leading to eventual identification.[21] On the other hand, anonymization defenders believe that the likelihood of reidentification is still relatively low, and that most data sets will remain anonymized using appropriate techniques.[22]

There are multiple techniques to anonymize data,[23] including: data masking; pseudonymization; generalization; data swapping; data perturbation; and synthetic data.[24] Data masking occurs when data is hidden with altered values. Pseudonymization replaces private identifiers with fake identifiers. Generalization deliberately removes data to make it less distinguishable. Data swapping rearranges the dataset values so that they do not correspond with the original data. Data perturbation modifies the original data set by applying techniques that round numbers and add random noise. Synthetic data is manufactured information that has no connection to real events.[25] Each of these techniques offers a different way to anonymize data, yet attackers can still retrace data sets back to the individual.[26] To combat this, conceptualizing anonymization should shift away from individuals putting their entire faith in data anonymization systems and towards the belief that data anonymization is only one layer to maintaining privacy.

A major reason to anonymize data is to protect individuals' privacy when storing or disclosing data.[27] Many industries utilize the process to protect someone's interests and provide anonymity when supplying data, as in healthcare or internet advertising.[28] Many defend the privacy-protecting power of anonymization and believe it is important and successful, despite evidence that indicates otherwise.[29] Data

---

19. Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 704 (2016) (describing the risk to an individual's privacy).

20. *Id.*

21. *Id.*

22. *Id.*

23. *Anonymization*, IMPERVA (n.d.), *available at* https://www.imperva.com/learn/data-security/anonymization/ (last visited Apr. 20, 2021).

24. *Id.*

25. *Id.*

26. *Id.*

27. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1708 (2010).

28. *Id.*

29. Elizabeth A. Brasher, *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*, 18 COLUM. BUS. L. REV. 209 (2018).

anonymization is perceived as essential, but criticism has proved that it alone is insufficient to protect privacy.[30] The process is appealing to the public because it balances the free flow of information with the risks of privacy harms and releases. The main concern with anonymization is that it removes the possibility of retracing information to the original data supplier. While Recital 26 of the GDPR[31] gives a circular definition of data anonymization as "data rendered anonymous in such a way that the data subject is not or no longer identifiable," it emphasized that anonymized data must be stripped of any sort of identifiable information so that a particular individual cannot be reidentified.[32] Compared to pseudonymization—which processes personal data so that it is no longer attributable to a specific data subject without additional information—anonymization completely anonymizes an individual's identity, taking this strategy a step further.[33]

Researchers found that using data while preserving an individual's privacy requires more than simply adding noise, sampling datasets, and other reidentification techniques.[34] A study conducted by communication researchers helped the public understand that retracing data is likely, even if individuals are assured that the dataset they are participating in is anonymized and a limited amount is shared with the general public.[35] This research shows that "once bought, the data can often be reverse-engineered using machine learning to reidentify individuals, despite the anonymization techniques."[36] Reverse engineered data exposes sensitive information about those personally identified, showing how easy it is to pinpoint individuals in practice.[37]

---

30. Ohm, *supra* note 28.

31. *General Data Protection Regulation, Recital 26 Not Applicable to Anonymous Data*, INTERSOFT CONSULTING (2018), *available at* https://gdpr-info.eu/recitals/no-26/ (last visited Apr. 20, 2021) [hereinafter INTERSOFT] ("Data rendered 'anonymous' in such a way that the data subject is not or no longer identifiable.").

32. Matt Wes, *Looking to Comply with GDPR? Here's a Primer on Anonymization and Pseudonymization*, IAPP (Apr. 25, 2017), *available at* https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/ (last visited Apr. 20, 2021).

33. *Id.*

34. *Anonymizing Personal Data 'Not Enough to Protect Privacy,' Shows New Study*, SCI. DAILY (July 23, 2019), *available at* https://www.sciencedaily.com/releases/2019/07/190723110523.html (last visited Apr. 20, 2021).

35. *Id.*

36. *Id.*

37. *Id.*

A common misconception about anonymization is that all data sets are untraceable once completed.[38] Critics of anonymization argue that completely detaching an individual's identity from a data set is impossible because other data sets will make it possible to identify that individual.[39] Another criticism of anonymization is that it does not work the way it was intended because of its simplicity. Publications from communications researchers claim the ability to correctly reidentify 99.98% of individuals in anonymized data sets using only fifteen demographic attributes.[40] Researchers also created a statistical model that estimates how easy it would be to identify any individual from a supposedly anonymized data set.[41]

Generally, data anonymization is regarded as a failure, but sustained public belief in this failure results from the current consensus that data anonymization is the only form of data protection. To combat this, data anonymization should instead be considered as one layer of a multi-layer protection initiative. Technological advancements make it difficult to keep data private, but data privacy is not impossible. In light of consumers' growing reliance on technology, information that is online and in datasets is more susceptible to tracking.[42] Reliance on technology is also problematic because it enables large amounts of data collection.[43] While internet sites often give individuals a choice of whether to share their data while using the site, that information may still be tracked another way.[44] Europe's current data protection framework allows for the use and sharing of anonymous data that is truly free; therefore, European nations are careful to recognize reidentification risk, and their laws use the term "pseudonymization" rather than "anonymization."[45] Critics have pointed out that it is a mistake to rely too much on these assessments.[46]

The most prevalent way to track data is through reidentification science. Reidentification science, also known as deanonymization, is a

38. Rubinstein, *supra* note 20, at 704.

39. *Id.* at 705.

40. Natasha Lomas, *Researchers Spotlight the Lie of "Anonymous" Data*, TECHCRUNCH (July 24, 2019), *available at* https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ (last visited Apr. 21, 2021).

41. *Id.*

42. Brasher, *supra* note 30, at 236.

43. *Id.*

44. *Id.*

45. Lomas, *supra* note 41.

46. Rubinstein, *supra* note 20.

technique that reidentifies encrypted or generalized information.[47] This practice leads to two important conclusions: that the power of reidentification will create and amplify privacy harms, and that regulators will protect privacy in the face of easy reidentification at a high cost.[48] Utility and data privacy are connected, so no regulation can increase data privacy without decreasing data utility; thus, no useful database will ever be entirely anonymous.[49] Reidentification science compares anonymized information with other available data to identify a person, group, or transaction. Reidentification can create and amplify privacy harms.[50] It "combines data sets that were meant to be kept apart, and in doing so, gains power through accretion," which facilitates future reidentification.[51]

Data anonymization masks an individual's personally identifiable information (PII), which is available from different fields, such as health services, social media platforms, and e-commerce trades.[52] PII includes information like "date of birth, Social Security Number, zip code, and IP address;"[53] however, "reidentification reserves the process of anonymization by matching shared by limited data sets with data sets that are easily accessible online."[54] Reidentification is simpler to accomplish if the anonymization process is incorrect.[55] Easier reidentification foretells of increasing inability to guarantee anonymity, but with continued technological advances in anonymization reidentification should be harder to achieve, insofar as it outpaces dueling reidentification technology advances.[56]

Opinions differ on whether or not anonymization and reidentification are possible.[57] Critics of anonymization argue for reduced reidentification-based approaches, while those that support reidentification argue that it is an unavoidable means necessary for identity protection.[58] Because reidentification is unavoidable, data

47. Jake Frankenfield, *De-Anonymization*, INVESTOPEDIA (2018), *available at* https://www.investopedia.com/terms/d/deanonymization.asp (last visited Apr. 20, 2021).

48. Ohm, *supra* note 28, at 1705.

49. *Id.* at 1705-06.

50. *Id.* at 1705.

51. *Id.*

52. Frankenfield, *supra* note 48.

53. *Id.*

54. *Id.*

55. *See id.*

56. *Id.*

57. *See* Rubinstein, *supra* note 20.

58. *See id.*

anonymization is an inherent failure which processes cannot be successfully implemented on the scale that data protection and privacy laws require.[59] Replacing names and values with random numbers or pseudonyms often passes as anonymized data, but actually increases the risk of reidentification instead.[60]

B. History of Data Protection in Europe and the GDPR

In Europe, the adoption of data protection and privacy laws eventually led to the implementation of the GDPR in May 2018. This law replaced the EU's Data Protection Directive 95/46/ec as the primary law regulating how companies protect EU citizens' personal data.[61] The goal of the more expansive GDPR was to evolve data and privacy protections alongside current technology. Because of the strict rules of the GDPR, companies had to comply with the new regulations before it became effective on May 25, 2018.[62] The law's reach extends beyond the EU to other countries, forcing non-member states to comply with these regulations in order to continue doing business within EU borders.[63]

One basic GDPR principle is that compliance with the law need be widespread, spanning the entire world.[64] Any company that does business in the EU will be subject to GDPR standards.[65] This includes businesses located within EU borders and individual employees working in EU member states or selling products and other goods to EU citizens. Businesses must get explicit consent from individuals regarding the processing of their data.[66] A pop-up window typically requests consent when an individual visits the company's website; these pop-ups inform the user that the website will track and collect their data as they navigate through the site.

---

59. *Id.*

60. *Id.*

61. Juliana De Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DATAINSIDER (Dec. 2, 2019), *available at* https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection (last visited Apr. 20, 2021).

62. *See id.*

63. *Id.*

64. Jessica Barker, *What Does GDPR Mean for You?*, DATAINSIDER (July 11, 2018), *available at* https://digitalguardian.com/blog/what-does-gdpr-mean-for-you (last visited Apr. 21, 2021).

65. *Id.*

66. *Id.*

The purpose of the GDPR is to create a set of standards for companies that handle EU citizens' data in order to better safeguard its processing and movement.[67] This measure prevents member states from writing their own data protection laws, thereby ensuring that these laws are consistent throughout the EU.[68] The GDPR helps promote uniformity, allowing for clearer interpretation of data regulations. Another issue the GDPR seeks to remedy is the effect of privacy laws as impediments to the free flow of information, which travel is instrumental to certain political and economic functions.[69] Part of the growth of data protection and privacy laws is attributable to the Internet's growth and the increasing normalcy of performing tasks online.[70] Consumers leave a digital trail of activity—from e-mail and social media communications to search engine queries and payment transactions—with private companies that have an interest in collecting, storing, and selling that data. Data anonymization is appealing because it lowers the risk of harm and enables the release of valuable, sensitive information while reducing that data's linkability to its owner.[71] As people put more information on the globally accessible internet, individuals continue to seek ways to keep themselves off of search engines and maintain their privacy; many do not want any possibility of being traced.

Compliance with the GDPR is a very serious matter. Companies that fail to follow the new GDPR rules face severe fines, potentially up to 20 million EUR or 4% of annual global revenue.[72] These fines depend on the severity of the violation and its surrounding circumstances.[73] The EU declared that GDPR compliance is not optional, and strictly enforces its rules in order to maintain compliance.[74]

The GDPR has an expansive view about what constitutes personal identification information, and companies have to find ways to safeguard smaller forms of identification, such as IP addresses and cookie data, the same way they protect larger ones, like names, addresses, and

---

67. De Groot, *supra* note 62.

68. *Id.*

69. Sophie Stalla-Bourdillon & Alison Knight, *Anonymous Data v. Personal Data – A False Debate: An E.U. Perspective on Anonymization, Pseudonymization and Personal Data*, 34 WIS. INT'L L.J. 284 (2016).

70. *Id.*

71. *Id.*

72. Richie Koch, *Everything You Need to Know About GDPR Compliance*, GDPR.EU (2020), *available at* https://gdpr.eu/compliance/ (last visited Apr. 19, 2021).

73. *Id.*

74. *Id.*

identification numbers.[75] It says that companies must provide a "reasonable" level of protection for personal data, but does not define what constitutes "reasonable."[76] This lack of direction regarding the requirements of these strict rules and regulations could make uniform compliance difficult to maintain.[77] Recital 26 of the GDPR says the following about data anonymization:

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, an account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, name information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes.[78]

The EU is generally stricter with its privacy regulations than the United States.[79] They enforce a comprehensive data privacy regulation upon all member states, with the GDPR imposing heightened privacy protections, including anonymization.[80] The GDPR defines an individual as an identifiable person if they can "be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,

75. Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant*, CSO (June 12, 2020), *available at* https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (last visited Apr. 20, 2021).

76. *Id.*

77. *Id.*

78. *See* INTERSOFT, *supra* note 32.

79. *See* Brasher, *supra* note 30, at 244.

80. *Id.*

cultural or social identity of that natural person."[81] This definition heightens the threshold for determining whether a natural person is "identifiable" by saying that an "account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."[82] Through this, the regulation indicates that forms of reidentification need to be acknowledged and that those attempting to regulate data privacy should be aware of potential attempts to take data.

While the idea behind GDPR – having a uniform system across multiple countries – sounds good in theory, certain aspects of this regulation have not worked quite to plan in practice. In particular, data anonymization has not worked because the process of deleting an individual's traceable facts is still unsuccessful. The GDPR brings data anonymization to the center of the discussion on data protection and privacy laws because many of its rules and regulations focus on how data collected by companies and individuals should not have any individual identifying information. In doing so, it emphasizes the importance of allowing people to maintain their anonymity when browsing the Internet or conducting business.[83] Although this approach is lacking, looking at other countries to learn from their anonymization attempts could improve the process.[84] India and China are two such countries that have developed anonymization regulations and continue to implement them through their respective data protection and privacy laws.[85]

C. Data Protection and Privacy in India

India is a federal democratic republic with a parliamentary system of government.[86] India has a modern parliamentary institution that originated with the British colonial administration and developed organically over time due to struggles for better representation in the government.[87] After India won its independence from the British, the

81. *Id.*

82. *Id.* at 245.

83. *Id.*

84. *Id.*

85. *See* Brasher, *supra* note 30.

86. *India Government Type*, INDEX MUNDI (2019), *available at* https://www.indexmundi.com/india/government_type.html (last visited Apr. 20, 2021).

87. *National Parliaments: India*, LIBR. OF CONG. (2014), *available at* https://www.loc.gov/law/help/national-parliaments/india.php (last visited Apr. 20, 2021) ("Colonization of India by the British helped developed the basis of a functioning government in India.").

Constituent Assembly[88] convened to draft the Constitution of India. In this Constitution, the Assembly stipulated the need for a "Parliament for the Union which shall consist of the President and two Houses to be known respectively as the Council of State and the House of the People."[89] Under this system of governance, the process of a bill becoming a law in India is as follows:

The *first stage* consists of the introduction of the Bill which is done on a motion moved by either a Minister or a Member. During the *second stage*, any of the following motions can be moved: that the Bill be taken into consideration; that it be referred to a Select Committee of the House; that it be referred to a Joint Committee of the two Houses; or that it be circulated for the purpose of eliciting opinion thereon. Thereafter, the Bill is taken up for clause-by-clause consideration as introduced or as reported by the Select/Joint Committee. The *third stage* is confined to the discussion on the motion that the Bill be passed and the Bill is passed/rejected either by voting or voice vote (or returned to the Lok Sabha by the Rajya Sabha in the case of a Money Bill).[90]

This system allows politicians to voice differing opinions, and safeguards bills as they go through the many legislative stages before becoming law. This is India's approach to maintaining the democratic system and allowing elected government officials to scrutinize each bill before it is passed.

In 2017, the Indian Supreme Court ruled that the Indian Constitution guarantees a fundamental right to privacy, but at that time, India had neither a data protection act nor a data protection agency.[91] However, the country later created a large biometric database called Aadhaar,[92] which is now the largest in the world.[93] An Aadhaar number is a twelve-digit number issued by the Unique Identification Authority of India (UIDAI) to residents of India who complete a specific verification process.[94] It is

88. *First Day in the Constituent Assembly*, LOK SABHA (n.d.), *available at* http://164.100.47.194/loksabha/constituent/facts.html (last visited Mar. 22, 2021) ("The Constituent Assembly took three years to draft the Constitution for an Independent India.").

89. Brasher, *supra* note 30.

90. *Id.*

91. *State of Privacy India*, PRIV. INT'L (Jan. 26, 2019), *available at* https://privacyinternational.org/state-privacy/1002/state-privacy-india (last visited Apr. 21, 2021).

92. *Welcome to AADHAAR*, AADHAAR (2020), *available at* http://www.aadhaar.nl (last visited Apr. 21, 2021) ("foundation" in Hindi).

93. Brasher, *supra* note 30.

94. *What is Aadhaar*, UNIQUE IDENTIFICATION AUTH. INDIA (2019), *available at* https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html (last visited Apr. 21, 2021).

a non-commercial and non-governmental organization that began development in 1997 to support grassroots-level development in India.[95] Its purpose is to bridge the gap between classes of people, improve the standard of living, and lead people out of poverty.[96] Citizens may voluntarily enroll with UIDAI to obtain an Aadhaar number; during enrollment they must provide minimal demographic and biometric information, which is free.[97] The official purpose of Aadhaar is as follows:

> Aadhaar is a strategic policy tool for social and financial inclusion, public sector delivery reforms, managing fiscal budgets, increas[ing] convenience and promot[ing] hassle-free people-centric governance ... [it]facilitates financial inclusion of the underprivileged and weaker sections of the society and is, therefore, a tool of distributive justice and equality. The Aadhaar identity platform is one of the key pillars of the "Digital India," wherein every resident of the country is provided with a unique identity. The Aadhaar programme has already achieved several milestones and is by far the largest biometrics-based identification system in the world.[98]

Since the creation of Aadhaar, Indian's legislative body worked on passing an all-encompassing data protection and privacy law based on the GDPR.[99] The law included individual rights protections, heightened consent requirements, and stiff penalties for non-compliance.[100] It also created barriers, making it more difficult to transfer personal data out of India. Further, the committee defined personal data slightly differently than the GDPR,[101] as "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic ... of the identity of such person."[102] However, there is nothing in the law about data anonymization regarding collected data because the draft bill argues that anonymization must be "irrevocable," despite the fact that irrevocability is most likely impossible under current standards.[103]

---

95. AADHAAR, *supra* note 93.

96. *Id.*

97. *Id.*

98. *India's Aadhaar System*, DFT EMPOWER (2017), *available at* http://www.dftempower.com/index.php/aadhaar (last visited Apr. 19, 2021).

99. *Key Provisions in India's Draft Personal Data Bill*, INSIDE PRIV. (Sept. 12, 2018), *available at* https://www.insideprivacy.com/international/key-provisions-in-indias-draft-personal-data-bill/ (last visited Apr. 20, 2021).

100. *Id.*

101. *Id.*

102. *Id.*

103. *Id.*

While the goal of Aadhaar was to make the lives of Indian citizens more equal and protect their privacy, the legislature is still working through inconsistencies and bumps in the law to make the it successful.[104] Problems include issues with accessing Aadhaar numbers, particularly as experienced by citizens who are sick, immobile, or bedridden;[105] generally lacking awareness of Aadhaar's individual benefits; and the denial of replacements to persons who lost their Aadhaar cards, which led to fake Aadhaar numbers.[106] The Supreme Court of India also ruled that illegal immigrants will not get an Aadhaar number.[107] With the biometric system in place and the fact that the country is still working on passing an all-encompassing law, India has leeway when incorporating data anonymization into its domestic regulations. Since Aadhaar already exists, individuals should be able to elect to keep their information private if the data is used for any purpose.

D. Data Protection and Privacy in China

China's government consists of four different divisions—the legislative, executive, judiciary, and military—which comprise the Communist Government of the People's Republic of China.[108] China's legislation is often passed in very vague terms because legislators want to see the effect of a law before adding clarifying details.[109] China has a National People's Congress (NPC), which is the highest ranking body[110] and largest in their government.[111] Its 3000 members rarely meet, requiring the NPC to rely on its committees to conduct the central government's regular business of drafting legislation.[112] For national

104. Reetika Khera, *Aadhaar Failures: A Tragedy of Errors*, ECON. & POL. WKLY. (Apr. 6, 2019), *available at* https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare (last visited Apr. 20, 2021).

105. *Id.*

106. *Id.*

107. *Cabinet Gives Go-Ahead to Aadhaar Bill*, ECON. TIMES (Oct. 9, 2013), *available at* https://economictimes.indiatimes.com/news/economy/policy/Cabinet-gives-go-ahead-to-Aadhaar-Bill/articleshow/23762608.cms (last visited Apr. 21, 2021).

108. Amber Pariona, *What Type of Government Does China Have*, WORLDATLAS (Apr. 25, 2017), *available at* https://www.worldatlas.com/articles/what-type-of-government-does-china-have.html (last visited Apr. 21, 2021).

109. *Id.*

110. *Id.*

111. *Id.*

112. *The PRC Legislative Process: Rule Making in China*, US-CHINA BUS. COUNCIL (2009), *available at* https://www.uschina.org/sites/default/files/prc_legislative_process.pdf (last visited Apr. 20, 2021).

laws, the NPC's Law Committee reviews the drafted laws and other legislative items, then writes a report to the NPC Standing Committee Council of Chairs.[113] They intently read this report three times before passing it, at which point it is published in the NPC gazette.[114] Under the Chinese Constitution, the Communist party has complete political authority and governs according to democratic centralism.[115] This system of governance allows open discussion and policy decisions, but all the members must uphold a collective decision.[116]

China's legislature tends to pass deliberately incomplete legislation at promulgation because it gives lawmakers more flexibility to adapt laws after their effects become apparent.[117] In other words, they wait to see how the laws and regulations play out before they decide how to enforce and interpret them. An issue often mentioned is that there are inconsistencies between the national laws and their local implementation guidelines because of the vagueness of their legislation.[118] This is because local guidelines are published months or years after creation.[119] China is often considered a surveillance state—a government that uses facial recognition and big data to control and monitor its citizens.[120] These practices coincide with their growing need for privacy protections, and the country is working faster to achieve these protections.[121]

Citizens of China often view privacy differently because they have a distinctive understanding of its principles and how it works. Currently, there is no data anonymization in China because data is collected from citizens whenever necessary, especially via facial recognition. When the Chinese government drafted its data protection and privacy laws, it looked to the GDPR as a model, particularly when it came to

113. *Id.* at 3.

114. *Id.*

115. *See id.*

116. *See id.*

117. Daniel Rechtschaffen, *Why China's Data Regulations Are a Compliance Nightmare for Companies*, THE DIPLOMAT (June 27, 2019), *available at* https://thediplomat.com/2019/06/why-chinas-data-regulations-are-a-compliance-nightmare-for-companies/ (last visited Apr. 20, 2021).

118. *Id.*

119. *Id.*

120. Samm Sacks & Lorand Laskai, *China's Privacy Conundrum*, SLATE (Feb. 7, 2019), *available at* https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html (last visited Apr. 20, 2021).

121. *Id.*

strengthening individuals' control over their personal information.[122] The Republic of China is known for its notoriously strict internet laws, which censor the Internet platforms citizens can access within its borders.[123] Because of this, they minimized individuals' privacy rights when it comes to using the Internet.[124] This minimization included setting up a specific regulatory system to monitor social media sites, like Facebook.[125]

China does not have a single comprehensive data protection law.[126] China's cybersecurity law, the Cyber Security Law, came into effect on June 1, 2017, and was its first national law addressing cybersecurity and data privacy protection.[127] The Cyber Security Law introduced a framework for comprehensive regulation for the privacy of electronically stored data.[128] This law has only further complicated the system by creating a multi-layered pyramid that implements regulations and measures, guidance notices, and national and technical standards, which narrows into highly granular rules at the top.[129]

As with many Chinese laws, the application of the Cyber Security Law and the steps needed to ensure uniform compliance are uncertain.[130] Some of the biggest concerns is protecting online information security; safeguarding the lawful rights and interests of citizens, legal entities, and other organizations; and ensuring national security and public interests.[131] The law requires consent to collect personal information and grants the government power to demand that companies turn over more information on users through random inspections of internet service providers,

---

122. Samm Sacks, *China's Emerging Data Privacy System and GDPR*, CSIS (Mar. 9, 2018), *available at* https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr (last visited Apr. 20, 2021).

123. Cheang Ming & Saheli Roy Choudhury, *China Has Launched Another Crackdown on the Internet - but it's Different This Time*, CNBC (Oct. 26, 2017), *available at* https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html (last visited Apr. 21, 2021).

124. *Id.*

125. Rechtschaffen, *supra* note 118.

126. DLA Piper, *China: Law*, DATA PROT. L. OF THE WORLD (2020), *available at* https://www.dlapiperdataprotection.com/index.html?t=law&c=CN (last visited Apr. 20, 2021).

127. *Id.*

128. Richard Bird & Pern Yi Quah, *Where Are We Now With Data Protection Law in China?*, LEXOLOGY (Sept. 10, 2019), *available at* https://www.lexology.com/library/detail.aspx?g=6f52a281-b5b7-4f9f-940d-1951a905c4e1 (last visited Apr. 21, 2021).

129. *Id.*

130. Ming & Choudhury, *supra* note 124.

131. DLA Piper, *supra* note 127.

making it increasingly difficult for users to be anonymous online.[132] Government action has shown this difficulty. In recent years China has cracked down on its internet platforms, including social media, for content violations.

Most importantly, from this case study, Chinese citizens' mindset towards collecting data can be useful for the Western world, particularly as reflected in how they do not depend on one system to completely privatize their information. Their thinking is more relaxed because their information is protected, so they do not worry about tracing their data and information. With this idea spreading to the west, the mindset regarding data anonymization will lead to an evolution of more realistic data protection techniques.

China defines personal data as all kinds of information recorded by electronic means, or otherwise, that can be used to independently identify or be combined with other information to identify a natural person's information.[133] Sensitive personal data is personal information that, if disclosed or abused, will adversely affect the data subject.[134] Some examples include a personal identification number, correspondence records and contents, property information, credit information, location tracking, lodging information, health, physiological information, and transaction information.[135]

The enforcement of the Cyber Security Law depends on specific data protection laws and regulations.[136] Because of this, there is no bright-line punishment for violators. Affected individuals may claim indemnification under Chinese Tort Liability Law,[137] and in severe cases breaches may lead to higher fines or license revocation.[138] China is looking to find the balance that allows the construction of a data protection regime which is both uniquely suited to China's needs and does not undermine the government's ability to maintain control.[139] Their mindset towards what should be private and how it should stay private would help advance data anonymization in other nations as well, insofar as anonymization is therein regarded as one piece of a layered approach to privatizing information rather than the entire solution.

---

132. Rechtschaffen, *supra* note 118.
133. DLA Piper, *supra* note 127.
134. *Id.*
135. *Id.*
136. *Id.*
137. *Id.*
138. DLA Piper, *supra* note 127.
139. Rechtschaffen, *supra* note 118.

III. FINDING A SOLUTION TO THE DATA ANONYMIZATION PROBLEM

To be successful, the international structure around data anonymization must change to reflect individual countries' needs. The EU, India, and China all provide an interesting look at how different governments handle this issue, and how that allows them to introduce their data protection and privacy regulations. Independently, each effort is not a total success; there are problems within each that require individualized solutions. However, if portions of the three strategies were taken together, then small provisions like data anonymization would become stronger. Broadly, this is achieved by acknowledging that privacy is a fundamental international right, which would create a common, shared value throughout the entire world. The international community should also accept that data anonymization is a protective layer, not full protection.

A. Mindset on Privacy

First, the international community needs to acknowledge privacy as a fundamental right. The EU set forth this right in the Charter of Fundamental Rights of the European Union (Charter) shortly after its establishment.[140] Chapter II of this Charter lists many freedoms,[141] including the right to private life.[142] The Charter also includes the right to privacy and the right to data protection, which form the foundation of the Charter.[143] When collecting data, the data subject must know why the data is being collected and what purpose the data collection serves.[144] It "must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes."[145] The data should also be adequate, relevant, and not exceed its purpose.[146]

---

140. *Charter of Fundamental Rights*, EUR. DATA PROT. SUPERVISOR (2009), *available at* https://edps.europa.eu/data-protection/our-work/subjects/charter-fundamental-rights_en (last visited Apr. 21, 2021).

141. Charter of Fundamental Rights of the European Union ch. 2, Dec. 7, 2000, 2000 O.J. (C 364/01).

142. *Id.* at art. 7.

143. *See Charter of Fundamental Rights*, *supra* note 143.

144. Robert Jan Uhl, *Data Protection*, EUR. UNION AGENCY FOR FUNDAMENTAL RTS. (Aug. 2012), *available at* https://fra.europa.eu/en/data-protection (last visited Apr. 21, 2021).

145. *Id.*

146. *Id.*

The general public only has access to information related to "public interest," otherwise, the access is limited to the European Agency's staff.[147] With the focus on maintaining this information's privacy, the EU can collect personal data to perform tasks conducted in the public interest, or to exercise the official authority vested in the EU and a particular institution. This applies to compliance with legal obligations to which the Agency is subjected, and processing is based on individual consent.[148]

Other countries have also begun to take action. In India, its nine-person Supreme Court bench held in a 2017 landmark decision that the "right to privacy" was a fundamental right.[149] The three focal points of this bill are: (1) the growth of the digital economy expanded the use of data as a critical means of communication between people, so it is necessary to create a collective system that fosters a free and fair digital economy; (2) respecting the informational privacy of the individuals, ensuring empowerment and progress; and (3) innovation through digital governance and inclusion.[150] The bill, similar to the GDPR, looks to "personal data" as information that will be obtained via consent from entities that classify as data fiduciaries.[151] The proposed bill suggests that some form of data anonymization will occur, but does not specifically mention anything except the government's ability to direct data collectors to hand over anonymized personal information or other "non-personal data" for "evidence-based policy-making."[152] This bill is intentionally vague, and it is not readily clear what the above might entail.[153]

The bill's intentional vagueness leaves open endless possibilities for what can be done with the data. The bill may include a discussion or reference to the fact that individuals have a right to privacy, and therefore mandate taking specific precautions. India could look to the GDPR's definition of data anonymization to clarify that this is only a step towards complete anonymization. It is important to again emphasize the layering effect, within which data anonymization would be only one part.

---

147. *Id.*

148. *Id.*

149. K.S. Puttaswamy v. Union of India, (2012) 1 S.C.C. 809, Judgement No. 494 (India).

150. Arindrajit Basu & Justin Sherman, *Key Global Takeaways From India's Revised Personal Data Protection Bill*, LAWFARE (Jan. 23, 2020), *available at* https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill (last visited Apr. 20, 2021).

151. *Id.*

152. *Id.*

153. *Id.*

China defines personal data as all kinds of information recorded by electronic means or which can otherwise be used to identify a natural person's information either independently or in combination with other information.[154] The translation of "privacy" in Chinese is "yinsi," which means "shameful secret."[155] It is an "instrumental good" rather than an intrinsic good.[156] China's approach to privacy differs; its government favors technologies like facial recognition, which are generally frowned upon by Western countries.[157]

The different types of accepted regulations create problems when deciding the purpose of anonymization rules. As facial recognition gains traction in China, leading the Chinese government to keep tabs on their citizens, the same type of software is swiftly denounced in the EU and other Western countries.[158] The EU and India have democracies as their main national government, while China has a more centralized government. The difference in structure and values explains the difficulty of creating a uniform system of laws. The EU and India focus on the betterment of their institutions, where each individual is a small, important piece that fits into the puzzle. However, China's difference lies in the fact that the government represents the group, and although they do not legally own the labor force, the central planners direct where citizens should work.[159] The cultural belief in China is that its citizenry should all happily contribute to a commonly shared skill, eventually resulting in their economy surpassing capitalism.[160] This belief stands in stark contrast to the Western concept of individualism, heavily contributing to different law enforcement systems in each of these countries.

To make effective changes, individuals' conceptualization of anonymization must shift. Right now, people believe that the anonymization of private information should be secure and unidentifiable. However, suppose those people were to accept that pure

---

154. Ming & Choudhury, *supra* note 124.

155. Tiffany Li, *China's Influence on Digital Privacy Could Be Global*, WASH. POST (Aug. 7, 2018), *available at* https://www.washingtonpost.com/news/theworldpost/wp/2018/08/07/china-privacy/ (last visited Apr. 21, 2021).

156. *See id.*

157. *Id.*

158. *Id.*

159. Kimberly Amadeo, *Communism, Its Characteristics, Pros, Cons, and Examples*, THE BALANCE (Oct. 30, 2019), *available at* https://www.thebalance.com/communism-characteristics-pros-cons-examples-3305589 (last visited Apr. 20, 2021).

160. *Id.*

anonymization is not feasible; in that case, they could look for other ways to maintain anonymity, even if not at the level that they expected. This change in process would not come easily, but with modern cyber surveillance it would be simpler to implement safeguards moving forward instead of focusing on the fact that the information is not actually private. The development of global privacy norms will strengthen if the international community is willing to work together and include different government types.[161]

For anonymization to be successful, a few things must initially be accepted. First, that privacy is a basic human right that needs to be protected by national governments.[162] Acceptance of this principle motivates taking steps towards protecting an individual's identity and keeping their information private. If privacy is viewed as a societal value by individuals, it opens to an economic investigation that is important for developing societies, which will ultimately lead to a sociological investigation of the concept.[163] Many privacy-specific goals focus on confidentiality and un-linkability, hoping that researchers, and those collecting data, will be able to strip away any identifiable information without taking away the purpose of collecting that data in the first place.[164]

B. Promoting Compliance

Another reason that anonymization has become an issue is that definitions of "personal data" vary. The GDPR defines "personal data" as:

> [A]ny information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[165]

---

161. *See* Basu & Sherman, *supra* note 151.

162. *See* Jan Zibuschka et al., *Anonymization is Dead – Long Live Privacy*, OPEN IDENTITY SUMMIT (2019), *available at* https://dl.gi.de/bitstream/handle/20.500.12116/20995/proceedings-06.pdf?sequence=1&isAllowed=y (last visited Apr. 20, 2021).

163. *Id.*

164. *Id.*

165. General Data Protection Regulation, art. 4, 2016 O.J. (L 119) 33.

Compliance is made difficult through these varying differentiations across countries, making uniformity difficult to maintain. In China, through the elimination of the free market, the government can set prices for the rest of the economy.[166] China also enacted regulations that align with the GDPR.[167] These regulations were promulgated to ensure that Chinese companies and corporations would not get fined while conducting business in the EU.[168]

Privacy compliance has become a basic component of privacy law because without it nobody would be liable for failing to adhere to the laws. Since the passage of the GDPR, countries have been working on passing laws and creating a framework that delivers a quick, cost-efficient solution.[169] These countries must understand the GDPR's compliance risks, so they should create programs that are easily maintained and work on training employees to keep the programs running as to avoid any issues.[170]

The initial cost of compliance is high, but will eventually even out over time.[171] These compliance systems will support and uphold democratic values and respect basic human rights.[172] Informing individuals that network operators are not gathering irrelevant information through their use of services, and assuring those individuals that their personal information will not be shared without their consent, supports basic human rights through privacy laws in the long run.[173] The GDPR recommends that the information collected "be stored in GDPR-compliant locations," no matter where those may be.[174] When working to comply with the GDPR, the Chinese Cyber Security Law took the

166. Nicolas Sartor, *9 Data Anonymization Use Cases You Need To Know Of*, AIRCLOAK (July 29, 2019), *available at* https://aircloak.com/data-anonymization-use-cases/ (last visited Apr. 21, 2021).

167. Wei Sheng, *One Year After GDPR, China Strengthens Personal Data Regulations, Welcoming Dedicated Law*, TECHNODE (June 19, 2019), *available at* https://technode.com/2019/06/19/china-data-protections-law/ (last visited Apr. 21, 2021).

168. *Id.*

169. Andrew Henderson, *The 10 Steps to Achieving a Data Privacy Compliance Framework*, LEXOLOGY (Apr. 23, 2018), *available at* https://www.lexology.com/library/detail.aspx?g=4ff0c436-2438-4b0d-b6f2-f617665049e8 (last visited Apr. 20, 2021).

170. *Id.*

171. Sartor, *supra* note 167.

172. *Id.*

173. *Id.*

174. Focal Point Insights, *Beyond the GDPR: A Look at China's National Data Protection Standard*, FOCAL POINT (June 13, 2019), *available at* https://blog.focal-point.com/beyond-the-gdpr-a-look-at-chinas-national-data-protection-standard (last visited Apr. 21, 2021).

opposite approach and stated that "personal information or important data collected in China must be stored solely in China."[175]

As mentioned above, similarly defining terms would narrow the varying privacy laws and disallow the current, existing variations. The numerous definitions of what comprises "privacy" create confusion in and between different world regions. Providing definitions using basic words like "privacy" allows for more coherent laws to be easily applied. Privacy should encompass an individual's basic information, such as name, address, and telephone number. It should also include identification numbers, which vary in usage from country to country.

Looking to data anonymization, its wide-ranging acceptance would succeed if it also acknowledged that stripping away a person's entire identity is not possible. Data anonymization should protect an individual's identity, not erase it. Current laws attempt to remove any personal information that could trace a person's identity back to them. However, because this strategy fails, it gives the entire concept of anonymization in data protection and privacy laws a bad name. Data anonymization turns "sensitive data into usable data sets by stripping identifiable information and making it anonymous."[176] These data sets are important, but are often compromised through reidentification science.

Critics argue that data anonymization is "dead" and that its current failures have had an irreversible, worldwide effect.[177] It is argued that the quality of anonymized data is lost once the identifiable information is taken away.[178] This is the opposite of pseudonymized data, where the link to the identifier is still present, and identifiable processes could be enabled at any time.[179] If the information no longer has this link, then the original data set is also impossible to identify, making the data hard to place into a specific context.[180] The biggest concern is that the data already collected is not anonymized and, therefore, will have consequences for privacy engineering.[181]

---

175. *Id.*

176. *8 Fundamental Data Anonymization Mistakes That Could Put Your Business at Risk*, CLOVERDX (Nov. 27, 2019), *available at* https://www.cloverdx.com/blog/data-anonymization-mistakes (last visited Mar. 22, 2021).

177. Zibuschka et al., *supra* note 163.

178. *Id.*

179. *Id.*

180. *Id.*

181. *Id.*

The focus should move away from attempting to erase an individual's identity and towards transparency and accountability.[182] In the EU, India, and China, withholding information is not possible because each country, in its own way, maintains that privacy is a fundamental right; therefore, each citizen has the right to assert its protections. Accountability would make adherence to compliance and uniform laws more possible because each country would be responsible for its own system.[183] This will be important, especially when companies and corporations conduct business internationally. Accountability will also decrease the belief that anonymization is a failure because it will not focus on the fact that people's information is not private; rather, on how those collecting the information are working to safeguard it.

IV. CONCLUSION

Data protection and privacy laws still have a long way to go before they even approach finalization and perfection. With technology continually changing, the laws that protect privacy must evolve in conjunction with these advancements. This task is accompanied by the challenges with varying governmental systems in different countries and the pace at which laws are passed.

The rise of the technology industry created a new set of problems for protecting individuals' privacy. As discussed, countries are doing their best to develop data protection and privacy laws which allow their citizens to live public lives on the Internet while maintaining a level of anonymity. These laws are extremely debated and anonymization is one of the issues at the forefront. The EU's GDPR is the leading standard in this field. If a country wants to work within EU borders, it must comply with the GDPR's baseline of rules or risk fines for non-compliance. This has become cost-heavy for businesses and foreign countries, but it is strictly enforced.

The GDPR is considered the gold standard of privacy laws. Compliance is not optional, and rules must be enforced to protect citizens' identities. The GDPR uses anonymization to protect individuals' identities by attempting to strip away their names, addresses, and identification numbers. Companies must safeguard an individual's data by "reasonable" levels, but "reasonable" is not defined, which leaves a large gray area open for interpretation. The concept of anonymization

182. Amadeo, *supra* note 160.

183. *Id.*

is appealing to the general public because it makes individuals feel as though they have power over what kind of personal information they can give; this is a false pretense, however, that leaves the public feeling as if the government is tricking them.

A country has data protection laws if their domestic laws provide a set of basic data privacy principles and a method of enforcement. Finding a uniform system across the countries is not impossible but could be difficult to manage. With India's biggest focus being on the biometric system Aadhaar, it has tried to pay attention to all citizens of India, especially those living in poverty. The intention behind its creation was to treat people equally, yet the program is plagued with implementation issues. On the anonymization front, the Aadhaar numbers are easily identifiable and not as anonymous as initially thought. India's non-commercial and non-governmental organization was about twenty years in the making, and remains a strategic policy tool for social and financial inclusion by issuing every single person with a unique identity. With the stress of being the most extensive biometrics-based identification system in the world, there are still small issues that have to be worked out before the system can be deemed a success.

China differs from the EU and India in that its communist government tends to pass vague laws that appear to be enacted without thought toward possible interpretations or long-term outcomes, thus creating potential for messes when it comes to implementation and enforcement. These messes seem to be left unaddressed until the Chinese government passes new laws to fix the old ones. China defines personal data as all kinds of information recorded by electronic means or otherwise that can be used to independently identify or be combined with other information to identify a natural person's information. China is an interesting state when it comes to privacy because it already imposes strict internet laws on their citizens. China is also a surveillance state, which means it gathers more public information than countries that are not surveillance states. A popular feature of its government is the use of facial recognition and big data to control and monitor citizens. When China drafted its data protection and privacy laws, it looked to the GDPR as a model, but ensuring anonymization was not as highly prioritized.

Finally, the international community wrongfully conceptualizes anonymization. The focus on anonymization should no longer be on anonymization through stripping away identifying information; it should instead position accountability as the primary focus. With accountability, there will be more opportunity to control which information data sets use. This will be beneficial because then the data sets can be linked to their origins. With this new branding of anonymization, identifiable

information will still be gathered, but instead of being stripped away, it will remain present yet unavailable to the public. This will help hold companies, corporations, and governments accountable for the type of information they collect, while allowing citizens to maintain a level of individual privacy.