I Have the Right to be Alerted:
The Global Policy on Data Breach Disclosure

by

J.R. Robert Real

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Information
at the University of Michigan

Thesis Committee:

Associate Professor Florian Schaub, Chair
Clinical Assistant Professor Sol Bermann

Winter 2023

rgreal@umich.edu

Acknowledgment

I would not have been able to write, research, and finish this thesis without so many, many people who have supported me throughout this process.

First and foremost, I thank my newly minted "Spouse B," the gentleman who has been with me for almost 11 years, and who was crazy enough to marry me. He has supported me every step of the way – for being my emotional backbone, for supporting me again and again to live overseas and enroll in this master's program, for reassuring me that privacy and data protection is a field worth entering, for being my perpetual sounding board, for always reviewing and being critical of my work, and for being an overall great person. I love you very much, Junefe Gilig Payot! You are my forever, my home.

I thank my mother who has been very supportive of my endeavors, of my last-minute decisions, and for always making sure that I'm okay. I thank my father who I know would have been very happy to see my graduate again and become a double Wolverine. I love you, Mama and Papa! I also thank my siblings (Jaymee & Meo, Ross & Pat, and Redge), nephew (Seb), and niece (Penny) for supporting and believing in me.

I thank my MTOP faculty advisor, Prof. Florian Schaub, for introducing me to the field of privacy technologies, for showing me how data privacy is not only about the law, for introducing me to the amazing Security Privacy Interaction Lab (SPILab) team at the University of Michigan, for giving me invaluable advice in formulating my research questions, for giving me insightful feedback on every inch of my paper, and for believing in me. I could not have asked for a better advisor.

I thank Sol Bermann for his thoughtful comments on both the legal, philosophical, and technological aspects of my thesis. Your comments really reassured me of my views on this topic. I also thank Yixin Zou for her comments, suggestions, and feedback, especially during the early stages of my research.

A very huge shout out to my friends Anna Medel, Kat Obrero, and Renz Zamudio for spending your time, energy, resources, and connections so that I can examine and understand 187 legal jurisdictions around the world. Your contribution and feedback are invaluable. I literally would not have been able to write this thesis without you! Special thanks to Aparna Ananthasubramaniam for helping me out with coding basics (you saved me!) and to my Ann Arbor family for helping me keep my sanity: Franko Stojkovic, Devon Kelly, Andrea Leycano, David Fuchs, Reyhan Najafikoupaei, Luise Cornelli, and Lennart Levita.

Table of Contents

Abstract

Law is said to mirror societal values. Following an examination of the personal data breach disclosure rules of 187 legal jurisdictions around the world, this study argues that there is now a global societal expectation that individuals must be informed of data breaches involving their personal information. From a single US State (California) passing a unique and innovative law in 2003, the world has moved towards legally mandating data controllers to reveal the occurrence of a personal data breach. Organizations can no longer conceal a failure in their data security.

World practice also shows that majority of legal jurisdictions regulate when and how individuals are notified. The prevailing global breach notification policy is that individuals should be informed of a breach if it involves their personal data and if there is a risk of harm to them. In turn, majority of legal jurisdictions set a specific timeframe within which to report to the authorities, while a general timeframe within which to notify individuals. Dominant worldwide policy also shows that majority of legal jurisdictions regulate the content of breach notices.

This study concludes by outlining what could be the components of a global model approach to breach disclosure. It argues that breach disclosure rules should be seen as akin to an individual right and a subset of one's right to privacy and right to human dignity – *i.e.*, a right to be alerted.

Keywords: privacy, data breach, breach notification laws, breach disclosure, right to be alerted, risk of harm, content analysis

Chapter 1
Introduction

> *"I almost lost my house and electricity was going to be shut-off."* – In the [Identity Theft] Victims' Words, 2022 Consumer Impact Report, Identity Theft Resource Center (ITRC)[1]

> *"A lot of people have been calling us crying, so worried that their children might find out, that their spouse would react. ... People are worried about employers finding out, insurers and their friends finding out. What's going to happen? Are they going to be blackmailed? Are they going to be threatened? I think there was a lot of fear."* – Avin Tan, Action for Aids Singapore on the leak of Singapore HIV database[2]

In January 2019, thousands of people in Singapore received a call from the Singapore Ministry of Health: their HIV positive status had been leaked.[3] The data breach involved people's name, identification number, phone number and address, HIV test results, and related medical information.[4] In Singapore where there remains strong stigma against HIV such that foreign nationals are tested for the virus before they are allowed to work,[5] one can only begin to fathom how devastating it must have been to receive such a phone call.[6] Living with HIV is already very difficult – imagine how much worse

---

[1] IDENTITY THEFT RESOURCE CENTER (ITRC), 2022 CONSUMER IMPACT REPORT, https://www.idtheftcenter.org/publication/consumer-impact-report/.

[2] Sharanjit Leyl, *Singapore HIV data leak shakes a vulnerable community*, BBC NEWS (22 Feb 2019), https://www.bbc.com/news/world-asia-47288219.

[3] *Unauthorised Possession and Disclosure of Information From HIV Registry*, SINGAPORE MINISTRY OF HEALTH (28 Jan 2019), https://www.moh.gov.sg/news-highlights/details/unauthorised-possession-and-disclosure-of-information-from-hiv-registry; Chang Ai-Lien, Fabian Koh, and Salma Khalik, *Data of 14,200 people with HIV leaked online by US fraudster who was deported from Singapore*, THE STRAITS TIMES (30 Jan 2019), https://www.straitstimes.com/singapore/data-of-14200-singapore-patients-with-hiv-leaked-online-by-american-fraudster-who-was.

[4] Chang, *et. al.*, *supra*.

[5] Health Promotion Board, *Guidelines on Managing HIV/AIDS at the workplace* (2016), https://snef.org.sg/wp-content/uploads/2016/10/hivguidelines.pdf; National Centre for Infectious Diseases, *National HIV Programme HIV Testing Recommendations* (12 Jul 2021), https://www.ncid.sg/About-NCID/OurDepartments/Documents/HIV%20Testing%20Recommendations_clean_FINAL_221021.pdf; Leyl, *supra* note 2; Isaac Stanley-Becker, *An American hid his HIV status to survive in Singapore. Exposed, he allegedly punished thousands living with the virus*, WASHINGTON POST (1 Feb 2019 at 7:24 a.m. EST), https://www.washingtonpost.com/nation/2019/02/01/an-american-hid-his-hiv-status-survive-singapore-exposed-he-punished-thousands-living-with-virus-authorities-say/.

[6] *See* James Griffiths, *HIV status of over 14,000 people leaked online, Singapore authorities say*, CNN (28 Jan 2019, 10:26 PM EST), https://www.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl/index.html; Leyl, *supra* note 2.

it could be when publicly outed with it, especially for those who have not disclosed their status to their employers, family, and friends.[7]

A year before, thousands of miles away, another government database was hacked. An Indian-based newspaper claimed that it had gained access to Unique Identification Authority of India's Aadhaar database for $6.[8] An anonymous group supposedly peddled login credentials, which allowed the newspaper to view the personal data of over a billion Indian citizens, ranging from their names, addresses, postal codes (PIN), photos, phone numbers, and emails.[9] The Indian Government issued Aadhaar cards as part of its biometric ID program, which the citizens could use to avail themselves of crucial government services, including welfare schemes, pensions, school scholarships, free school meals, cooking gas subsidies, fuel subsidies, driving license, passports, and others.[10] These cards were so important that failing to present a valid one could lead to serious, life-threatening harm. In one instance, a woman who had serious illness died after a hospital had allegedly refused to treat her for failing to present an original copy of her Aadhaar card.[11] In another incident, a girl died of starvation after her family was unable to claim their food rations supposedly for failing to have the card.[12] Considered one of the largest in the world,[13] the Aadhaar data breach in India exposed a massive amount of people to identity theft with potentially devastating consequences.[14]

---

[7] Stanley-Becker, *supra* note 5.

[8] Michael Safi, *Personal data of a billion Indians sold online for £6, report claims*, THE GUARDIAN (4 Jan 2018 06.20 EST), https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar; Rachna Khaira, *Rs 500, 10 minutes, and you have access to billion Aadhaar details*, THE TRIBUNE INDIA, (05 Jan 2018 01:58 PM IST), https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.

[9] *Id.*

[10] *Id.*; Mardav Jain, *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*, THE HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES – UNIVERSITY OF WASHINGTON (9 May 2019), https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/.

[11] Jain, *supra*, citing ANI, *No Aadhaar card: Hospital allegedly denies treatment; woman dies in Sonipat*, BUSINESS STANDARD (30 Dec 2017 10:30 IST), https://www.business-standard.com/article/current-affairs/no-aadhaar-card-hospital-allegedly-denies-treatment-woman-dies-in-sonipat-117123000101_1.html.

[12] Jain, *supra*, citing *Jharkhand: Family denied ration over Aadhaar linking, girl starves to death*, DECCAN CHRONICLE (17 Oct 2017), https://www.deccanchronicle.com/nation/current-affairs/171017/jharkhand-girl-starves-to-death-as-family-denied-ration-over-aadhaar-linking.html.

[13] WORLD ECONOMIC FORUM, THE GLOBAL RISKS REPORT 2019 (14th Ed.), https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[14] Vidhi Doshi, *A security breach in India has left a billion people at risk of identity theft*, THE WASHINGTON POST, 4 Jan 2018 at 10:07 a.m. EST, https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/.

Data breaches are not unique to Singapore and India. In fact, these incidents are a global phenomenon. Year after year we hear about the "worst," "biggest," or "massive" data breaches around the world – Yahoo (Global, 2013) involving 3 billion accounts, Equifax (US, 2017) affecting 605 million records, Aadhaar (India, 2018) exposing 1.1 billion identity/biometric information, Alibaba (China, 2019) revealing 1.1 billion pieces of user data, First American Financial Corp. (US, 2019) divulging 885 million financial information, Facebook (Global, 2019) baring over 530 million users, Sina Weibo (China, 2020) involving 538 million accounts, LinkedIn (Global, 2021) affecting over 700 million customer database, and Optus (Australia, 2022) exposing 9.7 million subscribers, to name a very few. In 2022 alone, about 1,802 data breaches involving more than 420 million victims have been publicly reported across the US.[15] It is beginning to feel that these worst, biggest, massive breaches are less of a misfortune and more of a consistent pattern in the digital age, as if everything is happening everywhere all at once. These breaches also involve the same old story – human error.[16]

According to the Identity Theft Resource Center (ITRC), the Top 10 data breach attributes in the US are the individuals' name, social security number, date of birth, current home address, driver's license/state id number, medical history/condition/treatment/diagnosis, bank account number, medical insurance account number, undisclosed records, and medical provider account/record number.[17] Given these data types, the impact of data breaches to individuals can be very serious, resulting in various actual harms. The HIV database leak in Singapore can lead to anguish and concern (psychological harm), loss of income (economic harm), hatred and prejudice (discrimination harm), injury to a reputation or loss of standing in the community (reputational harm), damage to personal relationships (relationship harm), and even coercion or undue influence (autonomy harm).[18]

---

[15] IDENTITY THEFT RESOURCE CENTER (ITRC), 2022 DATA BREACH REPORT, 7, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (hereinafter "ITRC Data Breach Report").

[16] DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (2022); Verizon, *2022 Data Breach Investigations Report*, 33-35, https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

[17] ITRC, 2022 DATA BREACH REPORT, *supra*, note 15.

[18] According to Citron and Solove, harms that individuals can suffer from a privacy violation include **autonomy harms**, such as those that involve restricting, undermining, inhibiting, or unduly influencing people's choices; **discrimination harms**, such as those that involve entrenching inequality and disadvantaging people based on gender, race, national origin, sexual orientation, age, group membership, or other characteristics or affiliations; **economic harms**, such as those that involve monetary losses or a loss in the value of something; **physical harms**, such as those harms that result in bodily injury or death; **psychological harms**, such as those involve anxiety, anguish, concern, irritation, disruption, or aggravation; **relationship harms**, such as those that involve causing damage to important relationships that are important for one's health, well-being, life activities, and functioning in society; and **reputational harms**, such as those that involve injuries to an individual's reputation and standing in the community. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. REV. 703 (2022).

In seeking to address this problem, the majority of the world has introduced legislation mandating disclosure of data breaches to authorities and individuals (which I will collectively refer to as "breach disclosure rules"). One of the supposed purposes of breach disclosure rules is to immediately alert individuals that their personal data may have fallen in the hands of unscrupulous malefactors, and that they should take protective measures against various forms of privacy harms.[19] These breach disclosure rules are, however, far from uniform. Legal jurisdictions define "personal information," "breach," and "notifiable breach" differently in that a data breach might be notifiable in one jurisdiction but not in another. They also differ when it comes to how data breaches are communicated. In the United States alone, all 50 states have their own set of rules on when organizations should notify consumers about personal data breaches.[20] A similar patchwork of data protection laws had existed in Europe until the passage of the General Data Protection Regulation ("GDPR") to unify the fragmented legal rules within the European Union.[21]

In addition to the lack of uniformity, what is more disconcerting is that research[22] also reveals that there is still considerable inaction by individuals when informed of data breaches despite these breach disclosure rules. A US study suggests that this inaction might have been caused by how companies write notices – they were lengthy and difficult to understand, and downplayed the consequences and risks of data breach.[23] In another US study, the ITRC uncovered that the number of breach notifications that contained detailed information about the victim and how the data breach was perpetrated had been reduced by more than 50% since 2019 (*see* Figures 1.1 and 1.2).[24] This downward trend suggests that individuals, businesses, and government officials are receiving fewer

---

[19] SOLOVE & HARTZOG, *supra*, note 16; Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub, *You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data breach notifications*, CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS PROCEEDINGS (CHI 2019), https://doi.org/10.1145/3290605.3300424 (hereinafter "Zou, et. al., You 'Might' Be Affected, (2019)"); Lillian Ablon, Paul Heaton, Diana Catherine Lavery, Sasha Romanosky, *Consumer attitudes toward data breach notifications and loss of personal information* (2016); Fabio Bisogni, *Proving Limits of State Data breach notification Laws: Is a Federal Law the Most Adequate Solution?*, 6(1) J. INFORMATION POL. 154 (2016).

[20] DLA Piper, *Data Protection Laws of the World: Full Handbook* (2023), https://www.dlapiperdataprotection.com; PRIVACY RIGHTS CLEARING HOUSE, DATA BREACH NOTIFICATION LAWS IN THE UNITED STATES (2022), https://privacyrights.org/resources/data-breach-notification-2022; PETER SWIRE AND DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS (3RD ED., 2020).

[21] Sian Rudgard, *Origins and Development of European Data Protection Law*, *in* EUROPEAN DATA PROTECTION LAW AND PRACTICE (EDUARDO USTARAN ED., 2ND ED., 2019).

[22] Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; PONEMON INSTITUTE, THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT (TECHNICAL REPORT) (2014).

[23] Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; Yixin Zou & Florian Schaub, *Beyond Mandatory: Making Data breach notifications Useful for Consumers*, 17(2) IEEE Security & Privacy 67 (2019), DOI: 10.1109/MSEC.2019.2897834 (hereinafter "Zou, *et. al.*, *Beyond Mandatory*, (2019)"); Bisogni, *supra*, note 19.

[24] ITRC, 2022 DATA BREACH REPORT, *supra*, note 15.

information, which would have allowed them to ascertain the risk of the data breach and then make informed decisions as to the necessary protective countermeasures that they need to perform.[25]

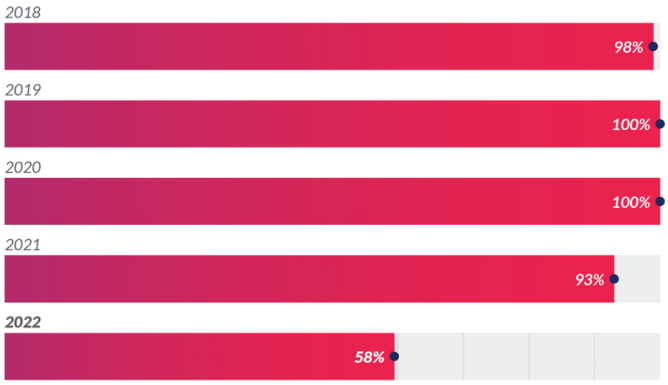

Figure 1.1: Percentage of breach notices with attack details.

(Source: 2022 Data Breach Report, Identity Theft Resource Center)

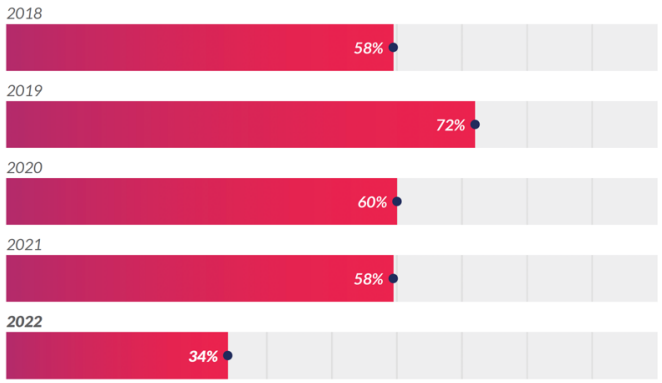

Figure 1.2: Percentage of breach notices with attack and victim details.

(Source: 2022 Data Breach Report, Identity Theft Resource Center)

As it appears that one of the purposes behind breach disclosure rules is not being fully served, researchers have suggested the need to improve the readability, emphasis, and manner with which such notices are made,[26] as well as the need to ease the costs and difficulties associated with protective measures.[27] For them, the government has a crucial role in achieving these objectives. Law can be one of the tools for accomplishing such goals.

[25] ITRC, 2022 DATA BREACH REPORT, *supra*, note 15.
[26] Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; Zou, *et. al.*, *Beyond Mandatory*, (2019), *supra*, note 23.
[27] Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; Bisogni, *supra*, note 19.

The argument to effectively alert individuals is even more compelling if we look at how Equifax got off lightly for its 2017 data breach. Individuals who were unable to show that they had suffered a direct loss received roughly between $3-$15 as compensation for time spent remedying fraud, identity theft, or other misuse of their personal data, for purchasing credit monitoring, or for freezing credit reports.[28] Such is the kind of reparation that individuals can expect from a government-led settlement of an incident that exposed about 605 million records of 147 million people. If individuals are only likely to receive a token sum for a potentially serious, life-threatening data breach, there is no strong incentive for them to act. Neither is there a strong deterrent effect on accountable organizations. Then it becomes even more critical to understand the current global policy (if any) on breach disclosure and to see whether there are gaps and best practices when it comes to alerting individuals and effectively nudging them to protect themselves against privacy harms.

1.1 Research Questions

In this study, I will investigate the breach disclosure rules in 187 legal jurisdictions across the globe. In particular, I will look into the following research questions:

1. What are the global trends on whether there is a legal requirement for data controllers to disclose personal data breaches?
2. What are the global trends in trigger requirements for when data controllers are legally required to notify individuals?
3. What are the global trends on the legally mandated timeframes within which individuals should be notified?
4. What are the global trends on legally requiring data controllers to communicate certain information when notifying individuals?

[28] Shahar Ziv, *I Got A Measly $14.90 From Equifax's Data Breach Settlement*, FORBES (22 Feb 2023,08:45am EST), https://www.forbes.com/sites/shaharziv/2023/02/22/i-got-a-measly-1490-payment-from-equifaxs-data-breach-settlement/?sh=31654b6367b4; *Equifax Data Breach Settlement*, FEDERAL TRADE COMMISSION, (Dec 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (hereinafter "FTC, *Equifax Data Breach Settlement*"). *See* In re Equifax Inc. Customer Data Security Breach Litigations, No. 20-10249 (11th Cir. Jun. 3, 2021).

While various institutions have compiled existing breach disclosure rules around the world,[29] I ask the first three research questions because very little research exists that examine the global trends on substantive trigger requirements for notification, as well as on temporal notice requirements when breaches occur. The same is true for the fourth research question, since there is also very little research investigating the global trends on what information are data controllers legally required to communicate when notifying individuals. Considering studies suggesting that consumers still do not take protective action despite receiving breach notifications,[30] an analysis of global breach disclosure rules can shed light on the various policy approaches that deal with the type and amount of information that these notices should contain. Further, it is also important because there is a dearth of research on global trends regarding what remedial measures companies are mandated to communicate to individuals to protect them from privacy harms. As research have suggested that the prohibitively difficult and high costs of consumer-initiated protective action can stifle individual response,[31] this study of global laws sheds light on the various policy approaches on the role of companies in providing remediation measures to protect the individuals' personal information. Overall, this study can set the foundation for a future study on how the overall approach to crafting breach notices could influence individual response.

1.2 Relevance of the Study

Law is said to mirror societal values – "the intellectual, social, economic, and political climate of its time."[32] As Friedman emphatically asserts: "legal systems do not float in some cultural void, free

---

[29] DLA Piper, *supra*, note 20; Practical Law Data Privacy Advisor, *Global Data breach notification Laws Chart: Overview*, THOMSON REUTERS, https://uk.practicallaw.thomsonreuters.com/w-016-6863?originationContext=knowHow&transitionType=KnowHowItem&contextData=(sc.DocLink)&firstPage=true (12 Nov. 2021) (on file with author); WORLD LAW GROUP, GLOBAL GUIDE TO DATA BREACH NOTIFICATIONS (2016), https://iapp.org/media/pdf/resource_center/WLG_Global_Guide_Breach_Notifications_2016.pdf; PRIVACY RIGHTS CLEARING HOUSE, *supra*, note 20; Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 PRIV. L. & BUS. INT'L. REP. 10 (2017).

[30] *See*, *e.g.*, Peter Mayer, Yixin Zou, Florian Schaub, & Adam J. Aviv, *Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them*, 30th USENIX SECURITY SYMPOSIUM 2021, https://www.usenix.org/conference/usenixsecurity21/presentation/mayer; Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub, *I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach*, PROCEEDINGS OF THE FOURTEENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 2018, https://www.usenix.org/conference/soups2018/presentation/zou; Ablon, *et. al.*, *supra*, note 19; Bisogni, *supra*, note 19.

[31] *See*, *e.g.*, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, 30(4) J. CONSUMER PSYCH. 736 (2020); Zou, *et. al.*, *I've Got Nothing to Lose* (2018), *supra*, note 30.

[32] STEVEN VAGO AND STEVEN E. BARKAN, LAW AND SOCIETY 5 (2018, 11th ed.). *See* BRIAN TAMANAHA, A GENERAL JURISPRUDENCE OF LAW AND SOCIETY (2001).

of space and time and social context; necessarily, they reflect what is happening in their own societies. In the long run, they assume the shape of these societies, like a glove that molds itself to the shape of a person's hand."[33] In the famous words of Oliver Wendell Holmes, Jr.:

> "The life of the law has not been logic: it has been experience. The felt necessities of the time, the prevalent moral and political theories, intuitions of public policy, avowed or unconscious, even the prejudices which judges share with their fellow-men, have had a good deal more to do than the syllogism in determining the rules by which men should be governed. The law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained only the axioms and corollaries of a book of mathematics." [34]

If law is indeed a reflection of society,[35] then this study on global breach disclosure rules can provide evidence of global societal expectations when it comes to informing individuals about data breaches. Studying these rules can give a sense of whether, and to what extent, governments have assumed a role in ensuring that individuals are informed of data breaches. Examining these rules can also provide us evidence of the worldwide formation of a right to be alerted.

I also aim to contribute to the cross-fertilization of ideas, legal principles, and judicial decisions[36] in the field of privacy and data protection. Judges and national courts from various jurisdictions cross-cite each other's decisions, whether to support an argument, reject an interpretation, compare and contrast different principles, provide an example, and others. Ann Marie Slaughter identifies this increasing interface among judiciaries as "judicial globalization," or the process of "judicial interaction across, above and below borders, exchanging ideas and cooperating in cases involving national as much as international law."[37] This can occur especially when judges act outside the boundaries of their respective domestic legal systems by looking at each other's work and engaging in a "conversation" to address seemingly common Issues. She explained that this "common global

---

[33] Lawrence M. Friedman, *Borders: On the Emerging Sociology of Transnational Law*, 32 STAN. J. INT'L. L. 65, 72 (1996); *See* TAMANAHA, *supra*, note 32.
[34] OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1 (1881); *See* TAMANAHA, *supra*, note 32.
[35] *See generally*, TAMANAHA, *supra*, note 32.
[36] *See* Anne-Marie Slaughter*, A Global Community of Courts*, 44 HARV. INT'L L.J. 191 (2003); Anne-Marie Slaughter, *Judicial Globalization*, 40 VA. J. INT'L L. 1103 (1999).
[37] Slaughter, *Judicial Globalization*, *supra*, at 1104.

enterprise of judging" can happen in various situations – when national courts and regional and supranational courts interact through decision making; when judiciaries recognize the concept of "judicial comity" in transnational litigation; when national courts engage in constitutional cross-fertilization; or when judges around the world meet face-to-face in conferences. If judges have engaged in this transnational discourse in the fields of constitutional law and human rights law (to name a few), it is not impossible for national courts or data protection authorities to start looking at each other's decisions and opinions in interpreting common privacy and data protection-related issues, especially in the light of the increasing cross-border data flows in this digital age.[38] For example, I will explain later how some jurisdictions require the existence of a risk of harm before notifying individuals, while other jurisdictions do not. Among those that require a risk of harm are a number of jurisdictions that further require the possibility of "serious" harm before a breach would warrant notification. Given these, my study will contribute to international legal discourse on data breach disclosure by providing a general guide to national courts[39] and data protection agencies[40] when they look at their foreign peers in assessing the types of "harm" and "serious harm" that can result from a data breach. Knowledge of various policy approaches and legal frameworks in the field of privacy and data protection, especially in breach disclosure, would inform legal researchers as to the number of factors to consider before they begin comparing, cross-citing, and developing domestic rules. Transnational privacy professionals and academics, too, can benefit from this project for these same reasons.

To be clear, the aim of this project is not mainly to state comprehensively what the legal requirements are in each legal jurisdiction although it does present snapshots of breach disclosure rules in certain jurisdictions. Rather, it provides an analysis of concepts as well as trends across jurisdictions, while the snapshots from certain jurisdictions are presented for illustrative purposes. If there is one thing that came out of this research, it is that privacy and data protection laws are constantly evolving. As such, my motivation is not to assist legal practitioners in advising their clients

---

[38] *See generally*, WORLD BANK, WORLD DEVELOPMENT REPORT 2021: DATA FOR BETTER LIVES (2021), https://doi.org/10.1596/978-1-4648-1600-0.

[39] *See*, *e.g.*, Elaine Mak, "The US Supreme Court and the Court of Justice of the European Union: Emergence, Nature and Impact of Transatlantic Judicial Communication" *in* A TRANSATLANTIC COMMUNITY OF LAW LEGAL PERSPECTIVES ON THE RELATIONSHIP BETWEEN THE EU AND US LEGAL ORDERS (Elaine Fahey & Deirdre Curtin eds., 2014).

[40] For example, the California Privacy Protection Agency (CPPA) was recently admitted as a full voting member of the Global Privacy Assembly (GPA), which is a forum of over 130 data protection and privacy authorities around the world. *See: California Privacy Protection Agency Admitted into Global Privacy Assembly*, 27 Oct 2022, California Privacy Protection Agency, https://cppa.ca.gov/announcements/. *See also* Graham Greenleaf, *Global Data Privacy 2021: DPAs Joining Networks Are the Rule*, 170 PRIV. L. & BUS. INT'L. REP. 23-26 (2021).

on whether they need to report a personal data breach to the authorities and notify data subjects. For that, legal practitioners should refer to commercial databases that are constantly being updated. Rather, my intention is to research and understand global breach disclosure rules, do comparative law analysis to highlight trends, and ultimately use insights from my analysis to contribute to judicial globalization in the field of privacy law. I want to see if there are trends in global breach notification rules and if there is a movement towards a particular policy direction. I want to understand the extent of their similarities and differences.

1.3 Key Findings

Throughout this research study, four key findings emerged that describe the current, worldwide approach to breach disclosure. First, most legal jurisdictions adopted a full breach disclosure policy in which data controllers are legally mandated to inform individuals and report to data protection authorities about the personal data breach. This indicates that breach disclosure has become a global policy. The second key finding is that not all data breaches must be disclosed. The global trend is that the incident must have involved personal data (broadly defined) and that the incident must have created a risk of harm to individuals. Without these two factors, most data controllers would not be required to disclose the data breach. The next key finding is that most legal jurisdictions across the world require data controllers to report the breach to data protection authorities within a specific timeframe, usually not more than 60 days; and to notify individuals within a general timeframe, usually within a reasonable time to enable the individuals to employ mitigation measures. The fourth key finding is that most legal jurisdictions regulate the content of breach notices, such that data controllers must ensure that they communicate certain information to individuals, including the measures they have implemented to mitigate the impact of the breach.

1.4 Overview of Thesis Chapters

This thesis presents a research study with the goal of understanding the global trends surrounding breach disclosure rules. In Chapter 1 (Introduction), I established the importance of understanding the various policy approaches surrounding breach disclosure. Meanwhile, in Chapter 2 (Related Work), I provided a summary of the current research in the field of breach disclosure rules and the issues surrounding breach notices. I then detailed in Chapter 3 (Research Method) how I

employed systematic content analysis in performing this study as well as the limitations of this research. Chapter 4 (Findings and Analysis) detailed the study's findings, which I presented in themes, as well as my analysis, which I presented according to my research questions. I then offered in Chapter 5 (Conclusion) my conclusions on the current global trends in breach disclosure rules, the implications of my findings and analysis, and what I believe should be the components of a global model approach to breach disclosure. Finally, I included in the Appendix the survey questions, the codebook, and the dataset that I used throughout this thesis.

1.5 Definitions

Each legal jurisdiction has its own way of defining common terms such as "personal information," "personal data," "data breach," and so on. For the sake of clarity and uniformity, I will use the terms and general definitions below. These are not meant to reflect legal definitions.

Term	Definition
breach disclosure	This collectively refers to both breach notification and breach reporting.
breach disclosure rule	This refers to a legal text that requires organizations to report to various government authorities and notify affected individuals about the occurrence of a personal data breach.
breach notification	This refers to disclosure of a data breach to individuals.
breach reporting	This refers to disclosure of a data breach to the relevant Data Protection Authority or other government agencies.
data controller	This refers to an individual or an organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
data processor	This refers to an individual or an organization, which processes personal data on behalf of the Data Controller.
data protection authority or authority	This refers to the governmental authority in charge of implementing the applicable legal text. This includes privacy enforcement agencies and other governmental agencies that exercise similar functions.
incident	A security event that compromises the integrity, confidentiality or availability of an information asset.
individuals	This generally refers to the individual person to whom the data pertains, subject to how the relevant legal jurisdiction defines it (*e.g.*, consumer, data owner, data subject, *etc.*).

legal jurisdiction	This refers to the physical territory where a particular legal text applies, regardless of whether such territory covers an entire state or one of its components.
legal text	This refers to laws, regulations, and guidelines issued by the relevant legislative or rule-making body in a legal jurisdiction. This excludes judicial decisions, law journal articles, and legal commentaries.
personal data breach	This refers to an incident that results in the confirmed disclosure—not just potential exposure—of personal data to an unauthorized party.
personal data	This refers to any information relating to an identified or identifiable individual.

Table 1.1: Definition of terms used in this study.

Chapter 2
Related Works

Having introduced in Chapter 1 the context which motivated my research on breach disclosure rules and having laid out the specific research questions as well as their importance, I will now discuss in Chapter 2 what relevant prior work have been done on the subject. I highlight their limitations in terms of the scope and depth of analysis they undertook, given their varying purposes as well as intended audience. In discussing previous research on the subject, I also note the need to update their findings given the fast pace of developments in the field of data breach disclosure. These are the gaps that this study aims to fill.

I also explore in this chapter the different variables and their relationships that previous studies have noted which lay the conceptual basis for answering the research questions in Chapter 1. For instance, I discuss what related literature has highlighted as factors which foster or hinder consumer reaction to protect themselves after a data breach.

2.1 Privacy and data protection law compilations

There is no scarcity of privacy and data protection law compilations. In fact, various universities, research institutions, and organizations have released their own collections such as the *Global Tables of Data Privacy Laws and Bills* of Prof. Graham Greenleaf,[41] the *Privacy Law Corpus* of Gupta *et al.*,[42] the *National Data Privacy Legislation Database* by the World Legal Information Institute,[43] the *Global Comprehensive Privacy Law Mapping Chart* of the International Association of Privacy Professionals (IAPP),[44] the *Data Breach Notification in the United States 2022 Report* by the Privacy Rights Clearing

[41] Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills* (7th Ed, January 2021), 169 PRIV. L. & BUS. INT'L. REP. (2021).
[42] Sonu Gupta, Ellen Poplavska, Nora O'Toole, Siddhant Arora, Thomas Norton, Norman Sadeh, and Shomir Wilson, *Creation and Analysis of an International Corpus of Privacy Laws*, arXiv:2206.14169 cs.CL (2022), https://doi.org/10.48550/arXiv.2206.14169 (hereinafter "Gupta *et al.*, *Privacy Law Corpus* (2022)").
[43] WORLD LEGAL INFORMATION INSTITUTE, LEGAL DATABASE: NATIONAL DATA PRIVACY LEGISLATION, http://www.worldlii.org/int/other/NDPrivLegis/.
[44] International Association of Privacy Professionals, *Global Comprehensive Privacy Law Mapping Chart*, https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/.

House,[45] the *US Security Breach Notification Laws* of the National Conference of State Legislatures,[46] the *Data Protection Africa* database by ALT Advisory,[47] and the *Data Protection and Privacy Legislation Worldwide* of the United Nations Conference on Trade and Development ("UNCTAD").[48] The international law firm DLA Piper also published its *Data Protection Laws of the World Handbook* online,[49] while commercial databases have been offered by Thomson Reuters (Practical Law Data Privacy Advisor)[50] and OneTrust (Data Guidance).[51]

While collections of global privacy and data protection laws abound, there are only a few studies on what these developments represent. For example, Prof. Greenleaf observed the global trajectory towards the adoption of privacy data protection laws and that GDPR appears to be a global influencer of these laws;[52] the establishment of national data protection authorities and how they appear to be creating transnational networks with varying purposes;[53] and the possible development of an international privacy standards based on regional or global international agreements.[54] Meanwhile, Gupta *et al.*, whose team examined about 1,043 privacy laws, regulations, and guidelines, covering 182 jurisdictions, found that there has been a considerable increase in privacy legislation in the last 50 years; and that there appears to be an increased attention to various aspects of consumer privacy.[55] All these analyses, however, mostly applied quantitative approaches to analyzing global trends in privacy and data protection laws without going into a deeper, qualitative, content analysis. Neither did they focus on any global trends pertaining to breach notification. Banisar and Davies[56] did delve into a more qualitative analysis of privacy and data protection laws in more than 50 legal jurisdictions, but their work is now outdated (circa 1999) considering Gupta *et al.*'s findings of

[45] PRIVACY RIGHTS CLEARING HOUSE, *supra*, note 20.
[46] National Conference of State Legislatures, *US Security breach notification Laws*, https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.
[47] https://dataprotection.africa/
[48] United Nations Conference on Trade and Development, *Data Protection and Privacy Legislation Worldwide*, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
[49] DLA Piper, *supra*, note 20; SWIRE AND KENNEDY-MAYO, *supra*, note 20.
[50] THOMSON REUTERS, Practical Law Data Privacy Advisor, *supra*, note 29.
[51] OneTrust, *Data Guidance Regulatory Research Software*, https://www.dataguidance.com.
[52] Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, 169(1) PRIV. L. & BUS. INT'L. REP. 3 (2021); *See* Gupta *et al.*, *Privacy Law Corpus* (2022), *supra* note 42.
[53] Greenleaf, *Despite COVID Delays, 145 Laws Show GDPR Dominance, supra. See* Gupta *et al.*, *Privacy Law Corpus* (2022), *supra*, note 42.
[54] *Id.*
[55] Gupta *et al.*, *Privacy Law Corpus* (2022), *supra* note 42.
[56] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1 (1999).

exponential growth in the 21st century – in fact, about 62 jurisdictions enacted their first privacy and data protection laws between 2010 and 2019.

In contrast, the body of research produced by non-academic institutions appears to be geared towards privacy professionals. For example, global law firm DLA Piper's *Data Protection Laws of the World Handbook* provided an overview of key privacy and data protection laws across more than 100 different jurisdictions as well as briefly identified privacy law trends. While IAPP's *Global Comprehensive Privacy Law Mapping Chart*, Thomson Reuters's Practical Law Data Privacy Advisor and OneTrust's *Data Guidance* did go into a content analysis of breach notification laws, none of them provided an in-depth analysis of global trends. Their charts were more of quick guides for practitioners.

2.2 Form of breach notification

There have been studies suggesting the need to have adequate breach notification laws, especially those dealing with the content and timing of such notifications. Bisogni,[57] for example, conducted a qualitative analysis of actual notices and found that there seemed to be underreporting of breaches. To address this issue, he argued that it may be necessary to require notification for all types of personal data breaches and that there should be strict regulation of the content of these notices to ensure that firms do not downplay the actual risks to consumers. He also noted the importance of when the notices are sent out to foster consumer reaction to protect their personal information. Given these proposals, he highlighted the pivotal role of government in setting the policy on breach notifications.

Proceeding from Bisogni's findings, Zou *et al.* (2019)[58] performed a content analysis of the notices sent to US consumers. The purpose of their content analysis was to examine their readability, structure, risk communication, and presentation of potential actions. The authors found the notifications to be long, unclear, and required advanced reading skills. Further, the companies that sent the notification appeared to have toned down the language about the breach's magnitude and consequences, so much so that the affected individual might not fully grasp the various risks of a personal data breach as well as the urgency of taking protective action.

[57] Bisogni, *supra*, note 19.
[58] Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19.

2.3 Mandatory remedial measures

Acquisti *et al.*'s findings[59] that consumers might find it "prohibitively difficult" to protect their personal data segues into the discussions on remedial measures that companies should employ following a data breach. For example, in a study on consumer awareness, perception, and responses to breaches, Mayer *et al.* found[60] that most of the study participants felt that the breach would not affect them and so they had not intended on taking measures to protect their information. The authors thus suggested the need to improve resilience against breaches as well as the need to make organizations accountable by having a positive obligation to communicate and mitigate the effects of breaches.

In another study, Zou *et al.* (2018) investigated[61] the actions taken by consumers following knowledge of a personal data breach affecting them. The authors learned that only few of them employed measures to protect themselves even though they expressed concern about the privacy violations and the risks of identity theft. The authors posited that such inaction may have been influenced by the costs associated with protective measures, optimism bias in estimating one's likelihood of victimization, sources of advice, and a general tendency towards delaying action until harm has occurred.

Ablon *et al.*[62] also examined consumer response towards a breach notification as well as the company's follow-on actions after a breach. They eventually found that 62% of their survey respondents accepted offers of free credit monitoring, 11% ceased dealing with the company following a breach, and 77% felt that they were highly satisfied with the company's post-breach response. Their study seemed to suggest that reducing costs associated with protective measures by offering free credit monitoring facilitates positive consumer reaction.

The discussion of the relevant background shows the following: (1) there are numerous policies on when consumers should be notified of a personal data breach event; (2) the manner by which a breach is communicated is crucial in nudging consumers to take protective action; and (3) the

[59] Acquisti, *et. al.*, *supra*, note 31.
[60] Mayer, *et. al.*, *supra*, note 30.
[61] Zou, *et. al.*, *I've Got Nothing to Lose* (2018), *supra*, note 30.
[62] Ablon, *et. al.*, *supra*, note 19.

prohibitively difficult and high costs of consumer-initiated protective action can stifle individual response. As prior works seem to recognize the crucial role of government in setting policy towards an effective breach notification that would prod consumer reaction,[63] in the next chapter, I will describe the research method I used to gather data on and to analyze the relevant laws in various legal jurisdictions across the globe.

[63] Acquisti, *et. al.*, *supra*, note 31; Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; Bisogni, *supra*, note 19.

Chapter 3
Research Design and Method

3.1 Content Analysis

I adopted systematic content analysis ("SCA") as my primary research methodology. As Hall and Wright posit,[64] the application of SCA as an empirical methodology for conducting legal research can imbue our understanding of the law with "the rigor of social science," creating a "distinctively legal form of empiricism"[65] such that it would generate an "objective, falsifiable, and reproducible knowledge about what courts do and how and why they do it."[66] Although it resembles conventional legal analysis, SCA focuses on discovering overall patterns across a large collection of "similarly weighted" cases (or laws, in this case) instead of acutely delving into select pivotal or landmark cases. Unlike conventional legal analysis that depends on the authoritative expertise of legal scholars to choose the relevant cases and extract notable themes, Hall and Wright explain that SCA obliges legal researchers to lay out in sufficient detail how to choose the cases and themes as well as the reasons for choosing them in order to allow others to reproduce the research (replicability).

Branscum and Fallik provides an example of how SCA can be applied in legal research, particularly in analyzing laws. In their work,[67] they gathered and examined about 982 human trafficking state laws to explain the landscape of human trafficking legislation in the United States. By using SCA, they were able to discover patterns and trends among human trafficking laws that had an impact to the survivors, and eventually to propose policy recommendations aimed at improving case outcomes and the experiences of survivors. Given the similarity of our research questions and aims, I chose SCA as my primary research methodology.

Following SCA, I will discuss below how I – (1) systematically chose the legal texts that will be studied; (2) coded the legal texts to take note of consistent information, elements, and other

[64] Mark A. Hall and Ronald F. Wright, *Systematic Content Analysis of Judicial Opinions*, 96 CAL. L. REV. 63 (2008).
[65] Hall and Wright, *supra* note 1, at 64.
[66] Hall and Wright, *supra* note 1.
[67] Caralin Branscum & Seth Wyatt Fallik, *A content analysis on state human trafficking statutes: how does the legal system acknowledge survivors in the United States (US)?*, 76 CRIME L. & SOC. CHANGE 253 (2021).

quantitative and qualitative features about each of them; and (3) analyzed the coded data through statistical methods in order to draw inferences about the meaning and use of the recorded information, elements, and features.[68]

3.2 Selection and Collection

Main Reference for Selecting the Jurisdictions to be Included	Primary Source of Data on the Privacy Laws in the Jurisdictions Selected	Secondary Sources of Data	Third-Party Reference for Validation
Global Data Breach Notification Laws Chart prepared (by Thomson Reuters)	*Privacy Law Corpus* (by Gupta et al.)	*National Data Privacy Legislation Database* by the World Legal Information Institute	Official websites of Data Protection Agencies
		Data Protection and Privacy Legislation Worldwide (United Nations Conference on Trade and Development)	*Data Protection Laws of the World Handbook* (DLA Piper)
		US Security Breach Notification Laws (National Conference of State Legislatures)	*Data Guidance* (OneTrust)
			Global Comprehensive Privacy Law Mapping Chart of the International Association of Privacy Professionals (IAPP)
			Data Protection Africa database (ALT Advisory)

Table 3.1: Summary of the sources of data used in this study, as well as the third-party references used to validate the data.

Chapter 2 mentioned several researchers, groups, and institutions that have compiled national breach notification laws. I opted to use the *Global Data Breach Notification Laws Chart* prepared by Thomson Reuters[69] as the starting point for my data collection process for two reasons: first, the chart already identified 112 jurisdictions[70] that have breach notification laws; and second, the chart already

[68] *See* Hall and Wright, *supra* note 1; Maryam Salehijam, *The Value of Systematic Content Analysis in legal Research*, 23(1) TILBURG L. REV. 34 (2018), DOI: https://doi.org/10.5334/tilr.5. *See*, *e.g.*, Branscum & Fallik, *supra*, note 67.

[69] THOMSON REUTERS, Practical Law Data Privacy Advisor, *supra*, note 29.

[70] The coded jurisdictions are as follows: Albania, Angola, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahrain, Bangladesh, Belarus, Belgium, Bermuda, Bolivia, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Cayman Islands, Chile, China, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Dubai International Financial Centre, Ecuador, Egypt, Estonia, Ethiopia, Finland, France, Georgia, Germany, Ghana, Gibraltar, Greece, Guatemala, Hong Kong - PRC, Hungary, Iceland, India, Indonesia, Ireland, Isle of Man, Israel, Italy, Jamaica, Japan,

collected information on whether or not – (a) authorities are required to be informed in case of breach; (b) individuals are required to be notified in case of breach; (c) there is a harm threshold before authorities and individuals are required to be informed; (d) timing was set within which breach disclosure must be made; and (e) a data protection authority was named for the purposes of breach notification. The first reason was an important consideration, since Thomson Reuters effectively confirmed that these jurisdictions had breach disclosure rules and that such rules contained information, which would be necessary in answering my research questions. As regards the second reason, choosing Thomson Reuters's work meant that I would have a resource which I can refer to when I compare and validate my independent analysis of the legal texts I found.

The next stage in my data collection process was to look for copies of the relevant privacy laws and administrative issuances in the legal jurisdictions identified by Thomson Reuters. In this regard, I primarily used Gupta *et al.*'s *Privacy Law Corpus*, which is a compendium of 1,043 privacy laws, regulations, and guidelines across the globe.[71] The documents in the compendium were both in their original language(s) and in English (official or unofficial translation). One limitation in using this compilation was that the documents were only up to date as of 31 December 2020. To address this limitation, I looked at other sources such as the World Legal Information Institute's *National Data Privacy Legislation Database*, the United Nations Conference on Trade and Development's *Data Protection and Privacy Legislation Worldwide Database*, and the National Conference of State Legislatures' *US Security Breach Notification Laws Database*.

To validate the accuracy of the gathered data, I referred to DLA Piper's *Data Protection Laws of the World Handbook*, OneTrust's *Data Guidance*, IAPP's *Global Comprehensive Privacy Law Mapping Chart*, the websites of the jurisdiction's data privacy agency (if available), and the Internet to check which legal jurisdictions had new issuances or amendments to their legal texts as of the time of my data collection, *i.e.*, as of 31 December 2022. If there were indeed updates, I searched online for copies

Kazakhstan, Kenya, Latvia, Liechtenstein, Lithuania, Luxembourg, Macau, Malaysia, Malta, Mauritius, Mexico, Monaco, Mongolia, Montenegro, Morocco, Mozambique, New Zealand, Nicaragua, Nigeria, North Macedonia, Norway, Pakistan, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Qatar Financial Centre, Romania, Russian Federation, Saudi Arabia, Senegal, Serbia, Seychelles, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Tanzania, Thailand, The Netherlands, Trinidad and Tobago, Tunisia, Turkey, Uganda, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay, Uzbekistan, and Vietnam.

[71] Gupta *et al.*, *Privacy Law Corpus* (2022), *supra* note 42.

using these same sources and based on the document type criteria[72] and translation technique[73] used by Gupta *et al*. I used the legal texts in the *Privacy Law Corpus* if there were no updates.

As soon as I finished updating all the 112 legal jurisdictions identified by Thomson Reuters, I expanded the list by adding 75 more jurisdictions listed in the *Privacy Law Corpus*. I then developed the chart by annotating the entries as well as by looking for and including additional concepts that were necessary to answer my research questions – how the breach disclosure rules delineate what constitutes personal data, whether the content of breach notifications was being regulated, and whether data controllers are required to communicate the performance or offer of remedial measures. I chose Gupta *et al*.'s work as the basis for expanding and developing the chart, because they already compiled the relevant legal texts. Given the temporal limitation of their work (31 December 2020), I adopted the same approach I used above – I checked DLA Piper's *Data Protection Laws of the World Handbook*, OneTrust's *Data Guidance*, IAPP's *Global Comprehensive Privacy Law Mapping Chart*, the websites of the jurisdiction's data privacy agency (if available), and the Internet to see whether there were new issuances or amendments to the legal texts in the *Privacy Law Corpus*.

As to the term "legal jurisdiction," I referred to the relevant definition under Oxford's A Dictionary of Law: "The territorial scope of the legislative competence of Parliament."[74] In the context of this research, I considered the term legal jurisdiction as that physical territory where a particular law or legal regime applies, regardless of whether such territory covers an entire state (within the meaning

[72] Gupta *et al*., *Privacy Law Corpus* (2022), *supra* note 42, at 3-7. They explained their criteria as follows: "Criteria based on document type — Each document must meet at least one of the following inclusion criteria: (1) The document is legally enforceable (or once-enforceable and now defunct, or assumed to be enforceable upon some future date of effect), which is promulgated in a complete state to the general public for the purposes of awareness of the law and enforcement if it is in force, which may include laws and regulations. (2) The document contains rules, clarification, or similar resources directed towards lawmakers or law enforcement for the purposes of enforcing the aforementioned document. (3) The document contains a non-enforceable list of guidelines, which serve as official guidance directed towards the general public, or specific sectors of the public, for the purposes of advising them on how to comply with a document of another type."

[73] Gupta *et al*., *Privacy Law Corpus* (2022), *supra* note 42, at 3-7. They described their technique as follows: "We attempt to create English translations for all the non-English documents in the corpus, to establish a uniform natural language for text analysis. Based on the translation, we divide the corpus into four classes: (1) Originally in English, (2) Official translation, (3) Unofficial translation, and as the name suggests, and (4) Google translation. If a document is in a language other than English, we seek an official English translation provided by the source of the official non-English document. Sometimes, official sources provide a translated version but call it an unofficial document for legal purposes. In the absence of the availability of such translations, we turn to international privacy expert sites, with exact sources noted in the corpus metadata. However, if the translation is still unavailable, we use translation tools like Google Translate. … However, Google Translate fails to provide a usable translation for a few titles in the Russian language. Therefore, we turn to Yandex Translate."

[74] OXFORD'S A DICTIONARY OF LAW (Jonathan Law, 10th ed. 2022).

of international law)[75] or one of its components. For example, I treated the following legal jurisdictions as separate, as they all have separate breach disclosure rules:

1. the Canadian Province of Alberta and the Government of Canada;
2. each of the states within the United States, the United States Federal Government, the District of Columbia, and the overseas territories of the United States, *i.e.*, Guam, Puerto Rico, and the Virgin Islands;
3. the People's Republic of China, Hong Kong Special Administrative Region, Macao Special Administrative Region, and Republic of China (Taiwan);
4. Qatar and the Qatar Financial Centre; and
5. the United Arab Emirates, the Abu Dhabi Global Market, and the Dubai International Finance Centre.[76]

Due to resource and time constraints, I chose not to study every state in the US. Instead, I focused on laws enacted by or within the following:

1. The five states that passed comprehensive privacy and data protection laws (*i.e.*, California, Colorado, Connecticut, Utah, and Virginia), but still retained their separate breach notification laws. I considered such separation notable, especially after discovering how most of the legal jurisdictions that had comprehensive privacy and data protection laws typically incorporated breach disclosure rules into such laws.
2. The District of Columbia and the three US overseas territories, *i.e.*, Guam, Puerto Rico, and Virgin Islands, since these four legal jurisdictions do not have the status of states, but are still enjoying a certain degree of autonomy.
3. Three states that passed breach notifications laws, which expressly and clearly included a harm threshold before entities can be required to perform breach notification, *i.e.*,

[75] In this context, a "state" refers to "a sovereign and independent entity capable of entering into relations with other states (compare protected state) and enjoying international legal personality." Oxford's A Dictionary of Law (Jonathan Law, 10th ed. 2022).

[76] Gupta *et al.* lists Dubai Healthcare City (DHCC) as another legal jurisdiction within the United Arab Emirates. Due to time constraints and minimal value, I no longer examined this jurisdiction.

Alabama, Alaska, and Oregon.[77] These states do not have their own comprehensive privacy and data protection laws. They were randomly selected from the 36 other US States and overseas territories that have risk-of-harm thresholds in their breach notification laws.

4. The United States Federal Government's sectoral breach notification laws (*e.g.*, HIPAA, GLBA).

I determined that examining the remaining states would not add value to my research, as the main point of my study is not just to count the number of legal jurisdictions that have breach disclosure rules. Rather, the emphasis of my research is to get a sense of the existing trends in global breach disclosure rules. Also, I believe that adding more legal jurisdictions from the United States could result in a trend analysis that is heavily influenced by American policy (*e.g.*, analyzing the breach notification rules of all the 50 states, the Federal Government, and the other United States Territories could account for around one-fourth of the data).

3.3 Coding

After selecting and collecting the relevant documents, I next examined Thomson Reuters's *Global Data Breach Notification Laws Chart* to see if the data from the answers to the existing questions in the chart were sufficient to answer my overall research questions. Given my review of related literature on global breach disclosure rules as reflected in Chapter 2, I eventually decided to include additional information that would be necessary to answer each one of my four research questions. I did so, as I noted that the scope of the said research questions goes beyond what the existing responses recorded in the Thomson Reuters' chart could address. The enhanced chart I developed is based on the refined survey questions which can be found in **Annex 1**.

I proceeded to scrutinize the legal texts per jurisdiction, searched for the relevant provisions that would help me answer these questions, and coded the responses verbatim using the finalized codebook. I adopted the "textual approach" in deciding and selecting the relevant provisions, which

[77] The other U.S. States that expressly and clearly included a harm threshold include the following: Arkansas, Colorado, Connecticut, Delaware, Florida, Hawaii, and Washington. *See* DIGITAL GUARDIAN, THE DEFINITIVE GUIDE TO U.S. STATE DATA BREACH LAWS (2018), https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf.

meant that I relied on the "fair meaning of the words of the text" without considering other factors and documents that may have limited or expanded the meaning of the text, such as court interpretations of the provisions.[78] Given possible translation issues and since the scope of my data collection does not include judicial decisions, I limited my analysis to express and clear statements in the legal texts without regard to how judicial and administrative institutions may have interpreted the relevant texts. My analysis was thus broad surfaced in structure, *i.e.*, manifest analysis or "what has been said" as opposed to "what was intended to be said."[79] I treated the selected provisions as "open-ended" responses and copied them onto an excel file.

Once I had finished selecting the relevant provisions (*i.e.*, responses) per jurisdiction, I developed a standardized response to some of the questions to enable me to conduct a quantitative analysis of the answers. I then iteratively developed the chart below with the initial chart using thematic coding and affinity diagramming. I continuously evaluated the chart, eventually turning it into a codebook, to find a good fit in terms of the categories, codes, and sub-codes. I explain in detail the developed codebook in **Annex 2**.

After developing the standard responses, I proceeded to my second round of coding. I transferred the full text of the legal provisions to the notes section of the chart and then used the standard responses (see Annex 2) in coding the answers to the questions. The dataset I ultimately used in my data analysis can be found in **Annex 3**.

3.4 Data Analysis

For the quantitative aspect of my analysis, I focused on ascertaining the existing policies surrounding breach disclosure across the globe, such as those that indicate the presence of breach disclosure rules, whether there is a preference in favor of mandatory disclosure (versus optional disclosure), whether there is any trend in regulating the content of breach notification itself, and whether there are policies requiring companies to communicate the remedial measures undertaken or

[78] *See* PHILIP BOBBITT, CONSTITUTIONAL FATE: THEORY OF THE CONSTITUTION 25 (1982).
[79] Mariette Bengtsson, *How to plan and perform a qualitative study using content analysis*, 2 NURSINGPLUS OPEN 8 (2016), https://doi.org/10.1016/j.npls.2016.01.001.

to be undertaken to protect consumers. I also performed other statistical analyses on the standard responses using *R Studio*.

With respect to the qualitative aspect of my analysis, I examined the responses and scrutinized the selected legal provisions to see if there are key similarities and differences. I then adopted a "textual approach" in conducting my qualitative analysis to avoid searching for a hidden or implied meaning beyond the express words of the law. This, too, meant that I chose not to search for judicial decisions and legal commentaries that might have clarified how the legal texts should be interpreted. I made this decision primarily because of my lack of familiarity with the various legal systems, judicial hierarchy, and legal cultures around the world.

To add depth to the quantitative and qualitative aspects of my analysis, I grouped legal jurisdictions according to geographical regions using the *Standard Country or Area Codes for Statistical Use* or the *M49 Standard* prepared by the Statistics Division of the United Nations Secretariat.[80]

3.5 Limitations

In answering all the questions, I examined only the English-language copy of the legal texts, as my language proficiency is limited to legal English. To remedy the potential inaccuracies in solely relying on translations, I counterchecked my work using the independent analyses of DLA Piper, OneTrust, and Thomson Reuters, as well as any relevant information available on the website of the legal jurisdiction's data protection authority (if any).

As I mentioned earlier, I adopted the textual approach in analyzing the legal texts in which I relied on the "fair meaning of the words of the text." The implication of this is that I did not examine other documents that are typically used in legal analysis, which may have limited, expanded, or clarified the meaning of the text, such as court decisions, rulings of data protection agencies, and scholarly works in the field of privacy and data protection.[81]

[80] *United Nations Secretariat Statistics Division, Standard Country or Area Codes for Statistical Use*, UNITED NATIONS, https://unstats.un.org/unsd/methodology/m49/

[81] *See, e.g.,* BOBBITT, *supra*, note 78 at 25 on various approaches in interpreting and understanding the US Constitution.

Chapter 4
Findings and Analysis

4.1 Findings

This study conducted a systematic content analysis of 187 legal jurisdictions from the following geographical regions (*see also* Figure 4.1):

Region	Count	Region	Count
1. Australia and New Zealand	2	12. Northern America	14
2. Caribbean	14	13. Northern Europe	14
3. Central America	7	14. South America	11
4. Central Asia	5	15. Southeast Europe	1
5. Eastern Africa	12	16. Southeastern Asia	9
6. Eastern Asia	7	17. Southern Africa	4
7. Eastern Europe	10	18. Southern Asia	9
8. Melanesia	1	19. Southern Europe	15
9. Micronesia	1	20. Western Africa	13
10. Middle Africa	7	21. Western Asia	18
11. Northern Africa	4	22. Western Europe	9

Table 4.1: List of geographical regions examined in this study.

I will discuss in Section A that an overwhelming number of legal jurisdictions adopted some form of a mandatory breach disclosure policy, whether it be a ***full breach disclosure policy***, a ***government-centered reporting policy***, or a ***data subject-centered notification policy***. Meanwhile, Section B will show how legal jurisdictions have adopted various ways of distinguishing which security incidents would trigger breach disclosure, from defining what constitutes personal data for the purpose of breach disclosure to setting the level of risk and severity of harm that individuals will have to suffer before the need for breach disclosure would arise. Section C will then discuss how majority of the world imposes stricter timeframe when reporting data breaches to data protection authorities (which I will refer to as "breach reporting"), while affording leeway to data controllers when it comes

to notifying individuals (which I will refer to as "breach notification"). Finally, Section D will describe how an overwhelming majority of the world requires data controllers to include specific information in their breach notices to individuals. Table 4.2 summarizes the distinctions made by breach disclosure rules, which I will discuss in greater detail in this section.

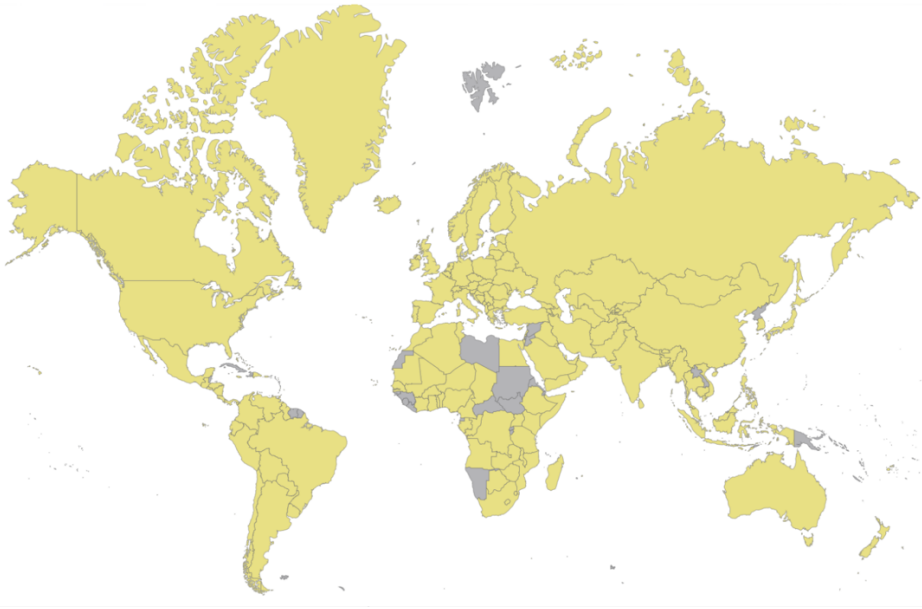

Figure 4.1: A map view highlighting the location of the 187 legal jurisdictions examined in this study (in yellow).

Who gets informed	What personal data types are covered	When to inform
1. full breach disclosure	1. broad scope	1. reporting (R) and notification (N) have specific timeframes (S) (**RS + NS**)
2. government-centered reporting policy	2. narrow scope	2. reporting (R) and notification (N) have general timeframes (G) (**RG + NG**)
3. data subject-centered notification policy		3. reporting (R) has a specific timeframe (S) while notification (N) has a general timeframe (G) (**RS + NG**)

		4. reporting (R) has a general timeframe (G) while notification (N) has a specific timeframe (S) (**RG + NS**)

Table 4.2: A summary of the distinctions made by the various breach disclosure rules around the world.

A. Breach disclosure is a global policy.

This section analyzes the various breach disclosure policies across the world, which I categorized as a ***full breach disclosure policy***, a ***government-centered reporting policy***, and a ***data subject-centered notification policy*** (which I will collectively refer to as "breach disclosure policies"). In arriving at the conclusions in this section, I examined the responses to the following questions:

1. (a) whether the law requires reporting to authorities in case of a personal data breach and (b) whether the law requires notification of data subjects in case of a personal data breach; and

2. (a) whether the law provides a timeframe to report to authorities in case of a personal data breach and (b) whether the law provides a timeframe within which to notify data subjects in case of a personal data breach.

One of the goals of these questions is to see whether there are global trends when it comes to requiring data controllers to inform data protection authorities and individuals about the occurrence of a data breach.

Figure 4.2 shows that an overwhelming number of legal jurisdictions (67.91% or 127 out 187) adopted some form of a mandatory breach disclosure policy. Of these 127 legal jurisdictions, 83.46% (106) adopted a full breach disclosure policy; 11.02% (14) adopted a government-centered reporting policy; and 5.51% (7) adopted a data subject-centered notification policy. In contrast, only 31.02% of legal jurisdictions examined (58 of the 187) have no clear, mandatory breach disclosure policy of any

form, while the remaining 1.07% (2) adopted a more recommendatory approach to breach disclosure. In terms of global trends, these numbers suggest that mandatory breach disclosure is already a world-wide phenomenon.

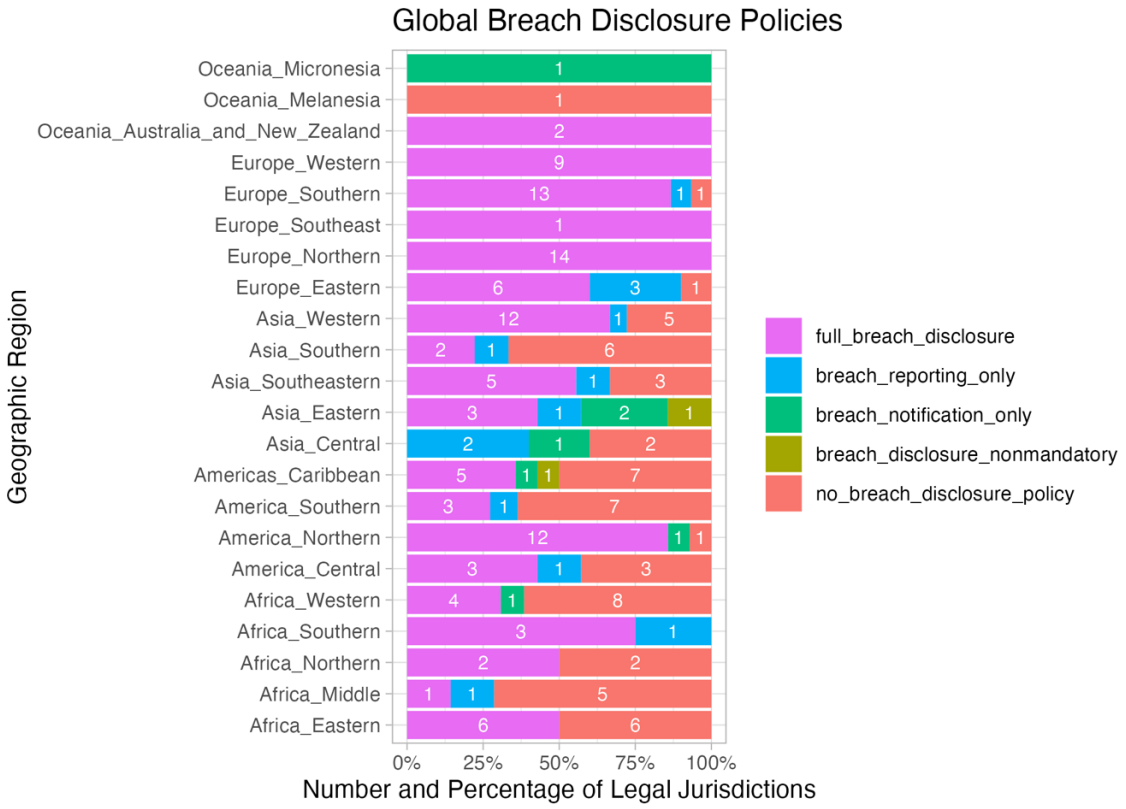

Figure 4.2: A visual representation of the various breach disclosure policies in the world, grouped by geographic region.

Zeroing in on the policy concerning breach reporting to data protection authorities, Figure 4.3 shows that 94.49% of the legal jurisdictions that adopted a mandatory breach disclosure policy (120 out of 127) require breach reporting, while only 5.51% (7 out of 127) do not require it. In contrast, with respect to the policy on breach notification to individuals, Figure 4.4 suggests that 88.98% of the total number of legal jurisdictions examined (113 out of 127) require breach notification, while only 11.02% do not require notification (14 out of 127).

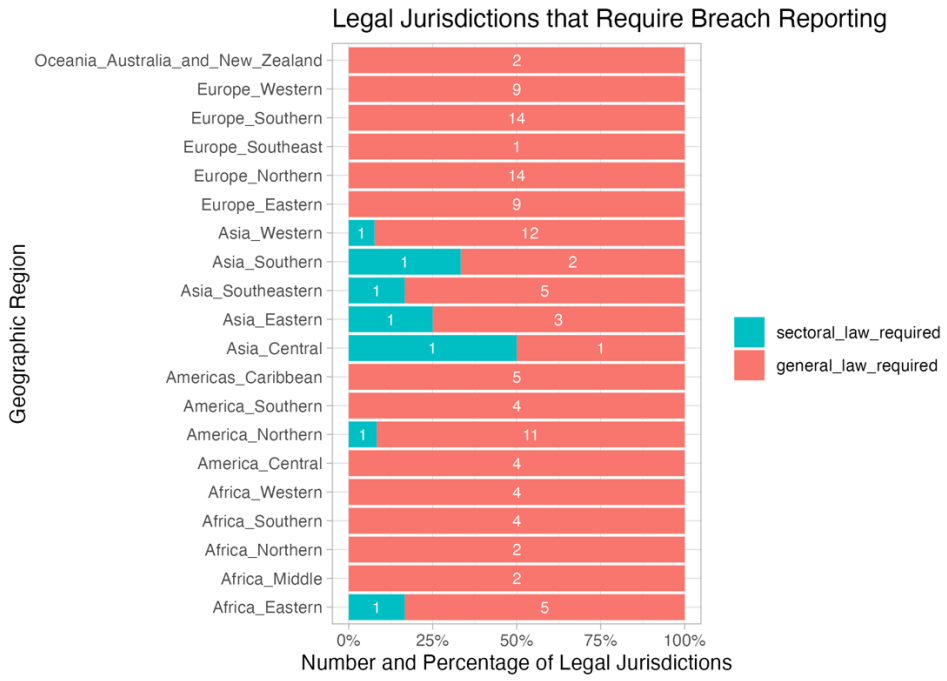

Figure 4.3: A visual representation of the 120 legal jurisdictions that mandate breach reporting, grouped by geographic region.

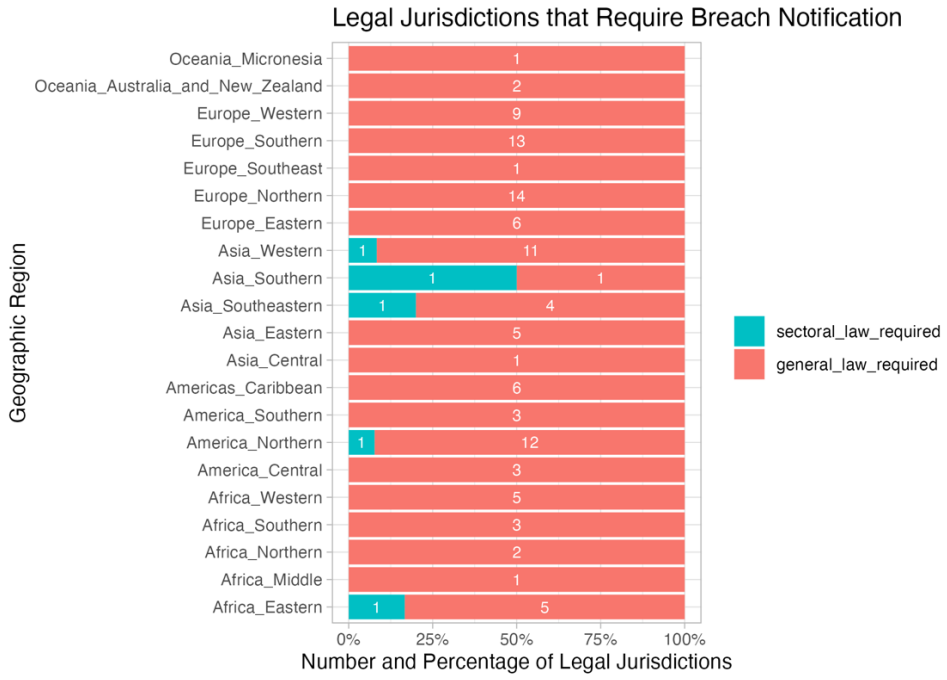

Figure 4.4: A visual representation of the 113 legal jurisdictions that mandate breach notification, grouped by geographic region.

We can gather from these data that there are three types of breach disclosure policies across the world: first, ***full breach disclosure policy***, or that which requires both breach reporting to governmental authorities and breach notification to individuals; second, ***government-centered reporting policy***, which mandates breach reporting only to governmental authorities (breach notification to individuals is either not required or merely recommended); and (c) ***data subject-centered notification policy***, which mandates breach notification only to individuals (breach reporting to governmental authorities is either not required or merely recommended). While the data suggests that the world almost equally values the need to disclose personal data breaches to both authorities and individuals, it is interesting that there are 14 legal jurisdictions[82] (about 7.49% of the total number of examined legal jurisdictions) that adopted a breach disclosure policy that does not directly warn individuals about the data breach. If we are to plot all these data onto the world map, we will be able to see which legal jurisdictions impose breach reporting to data authorities (*see* Figure 4.5) and which ones impose breach notification to individuals (*see* Figure 4.6). You may also notice that an overwhelming number of countries are in both maps so that if you overlay them, you will see a significant overlap.

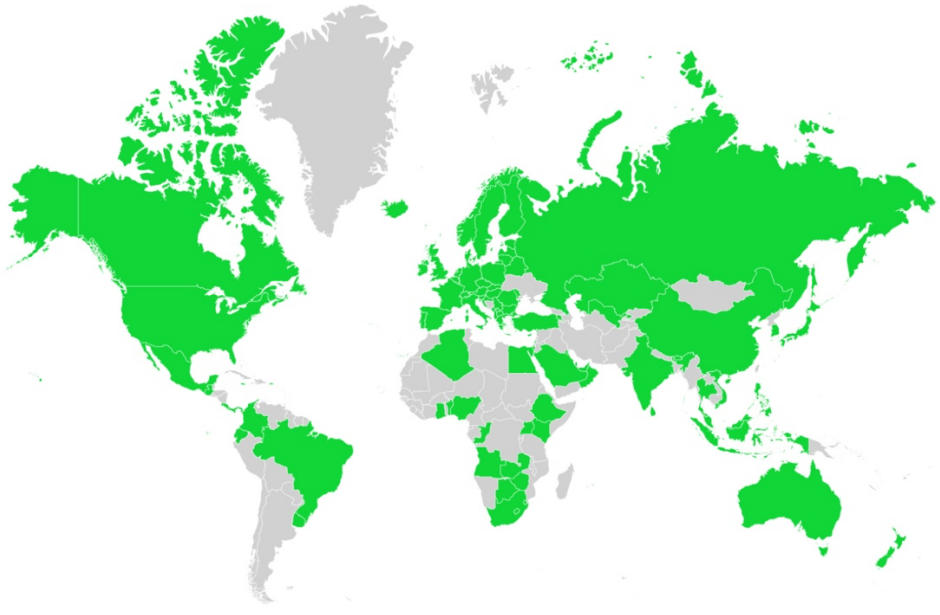

Figure 4.5: A map view highlighting the location of the 120 legal jurisdictions that have mandatory breach reporting to authorities (in green).

[82] These legal jurisdictions are the following: Albania, Angola, Belarus, Botswana, Colombia, Guatemala, India, Kazakhstan, Macau, Moldova, Russia, Saudi Arabia, Uzbekistan, and Vietnam.

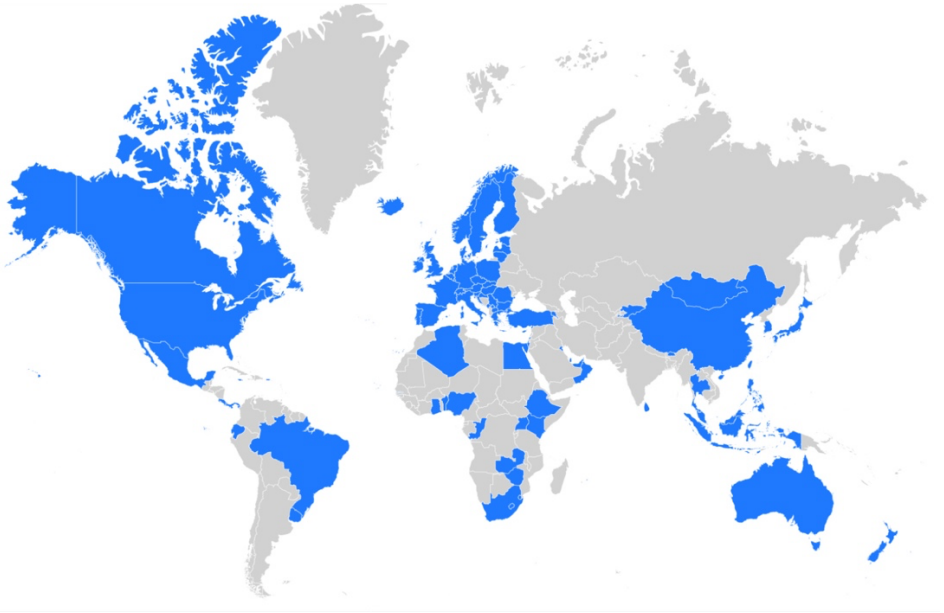

Figure 4.6: A map view highlighting the location of the 113 legal jurisdictions that have mandatory breach notification to individuals (in blue).

B. Data breach does not automatically trigger breach disclosure rules.

After showing how a majority of legal jurisdictions require some form of breach disclosure (either breach reporting, breach notification, or both), I will now discuss in this section how trigger requirements for disclosure vary across legal jurisdictions. Sub-section 1 focuses on how legal jurisdictions classify the types of personal data that must have been involved in a data breach, while sub-section 2 centers on the level of risk and severity of harm that may be suffered by individuals before the need for breach disclosure would arise. As I will show, I gathered from the data that legal jurisdictions do not mandate indiscriminate breach disclosure.

1. The breach must involve the right kind of personal data.

This sub-section analyzes how legal jurisdictions delineate the scope of their breach disclosure rules, particularly the materiality of the type of data that must have been involved in a breach. As I will discuss, legal jurisdictions adopted either a ***broad scope*** or a ***narrow scope*** of data types for breach disclosure purposes. I classified the scope as ***broad*** if the breach disclosure rule contemplates data

breach involving a wide range of personal data types without any kind of distinction. Here, the breach disclosure requirement must not have been limited to those that fall under specific types or categories of personal data. Those that adopted a broad scope of personal data types typically espoused a definition of personal data that is open-ended and unconfined. Meanwhile, I classified the scope as ***narrow*** if the personal data type that is subject of a breach notification is confined within a list of data types or categories (*e.g.*, data must include name or last name, or must be a "sensitive" personal data). This is typically demonstrated by legal jurisdictions adopting a closed-ended definition of personal data or those with an open-ended definition but introduced a sub-category of personal data that is subject to the breach notification rule. Tables 4.3, 4.4, and 4.5 provide examples of how the legal texts delineated the scope of the data types.

To arrive at the conclusions in this section, I asked the following questions:

(1) What is the relevant definition of personal data in the breach notification law?
(2) Was the definition of personal data for the purpose of breach notification open-ended or closed-enumerated?
(3) Did the law distinguish the types of personal data subject to breach notification?

These questions were meant to explore whether the category or type of data involved is material when it comes to any obligation to perform breach disclosure.

Delineating the extent of breach disclosure rules by defining what constitutes personal data

A common theme that I saw from the legal texts is that not all data breaches trigger breach disclosure. At the most fundamental level, the data must first and foremost pertain to an individual, *i.e.*, personal data. This means that a data breach resulting in the theft of trade secrets, for example, does not *per se* trigger breach disclosure if it does not involve personal data.

In turn, legal jurisdictions with mandatory breach disclosure rules vary their approach when it comes to delineating what constitutes personal data for purposes of triggering breach disclosure. On the one hand, an overwhelming number among them embrace an open-ended definition of personal

data (88.98% or 113 out of 127), that is, when data is deemed personal data if it satisfies a set of criteria usually requiring a factual determination and analysis (*e.g.*, data must eventually lead to identification of a person). Meanwhile, only 11.02% (14) had a closed-ended definition of personal data, that is, when data will be considered personal data if it falls under a confined list of data types or categories (*e.g.*, data must include name or last name). Below are examples of an open-ended and a closed-ended definitions of personal data for breach disclosure purposes:

Type	Jurisdiction	Provision
Open-ended	**United Kingdom**	"Personal data" means **any information** relating to an **identified or identifiable living individual**.
Closed-ended	**US – Virginia**	"Personal information" means the **first name or first initial and last name in combination with and linked to any one or more of the following data elements** that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number.

Table 4.3: Excerpts of legal provisions, which illustrate how "open-ended" and "closed-ended" definitions of personal are typically phrased.

Figure 4.7 shows that an overwhelming majority of legal jurisdictions adopted an expansive, open-ended definition of personal data like that of the United Kingdom in the example above, whereas only a few adopted a confined, closed-ended definition like that of the United States – Virginia. Out of 127 legal jurisdictions with breach disclosure rules, 88.98% (113) had an open-ended definition while 11.02% (14) had a closed-ended definition.

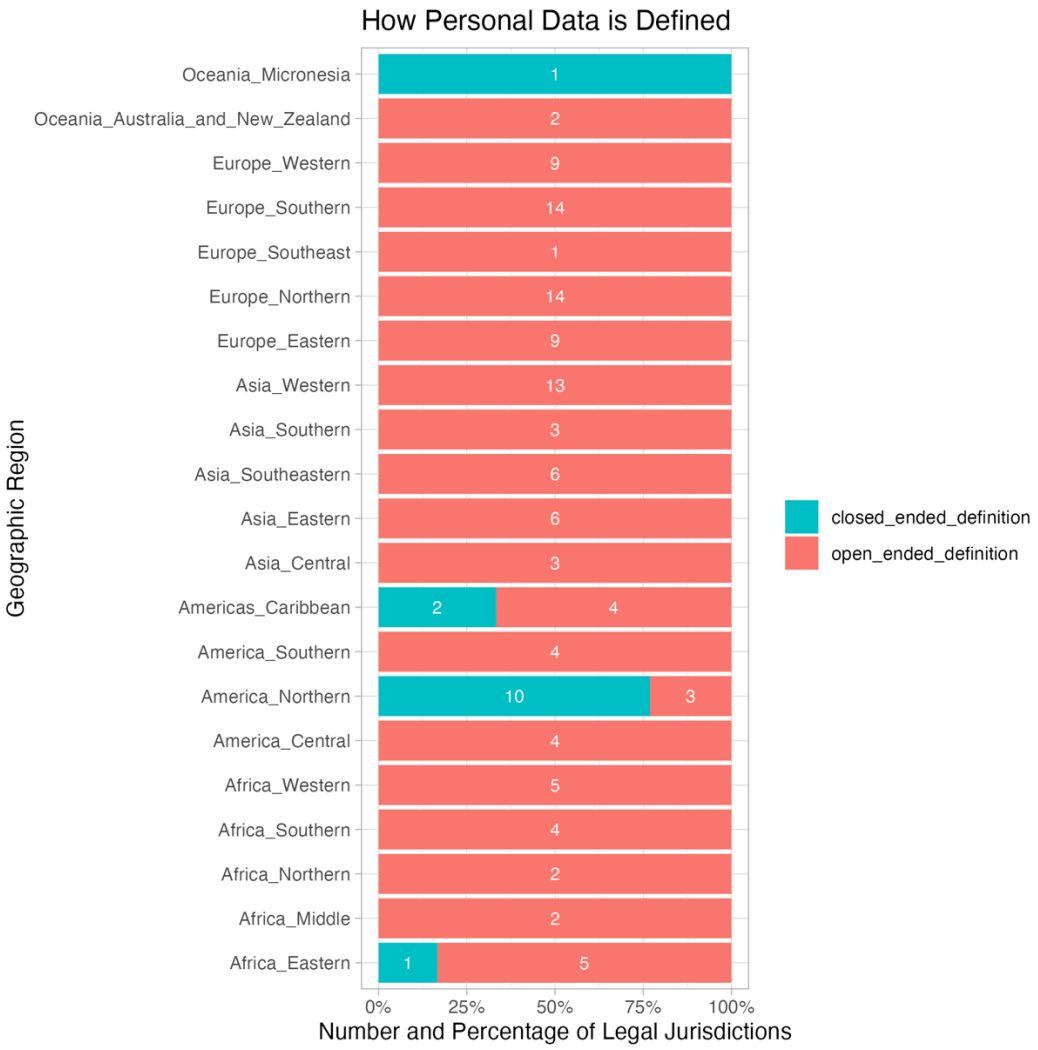

Figure 4.7: A visual representation of how legal jurisdictions defined personal data (i.e., an expansive, open-ended definition and a confined, closed-ended definition), grouped by geographical region.

It is notable that 13 of the 14 legal jurisdictions that had a confined, closed-ended definition were in the United States, while the other is Zimbabwe:

1. United States Alabama
2. United States Alaska
3. United States California
4. United States Colorado
5. United States Connecticut
6. United States District of Columbia
7. United States Federal
8. United States Guam
9. United States Oregon
10. United States Puerto Rico
11. United States Utah
12. United States Virgin Islands
13. United States Virginia
14. Zimbabwe

What is interesting is that five of these legal jurisdictions passed comprehensive privacy and data protection laws (*i.e.*, California, Colorado, Connecticut, Utah, and Virginia) introducing a second definition of personal data that is expansive and open-ended. Table 4.3 shows that these five US States effectively created two definitions of personal data: one for the purpose of individual privacy protection; and another for the purpose of breach disclosure.

State	Text
California	California Civil Code § 1798.82 breach notification Law. (h) For purposes of this section, "**personal information**" means either of the following: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number. (B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5. (H) Genetic data. (2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.
	California Civil Code (California Consumer Privacy Act of 2018) § 1798.140. (v) (1) "**Personal information**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. (B) Any personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. (L) Sensitive personal information.

Colorado	Colorado Revised Statutes Annotated breach notification Law, § 6-1-716(g)(I)(A) "**Personal information**" means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data; (B) A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or (C) A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
	Colorado Revised Statutes Annotated Colorado Privacy Act, § 6-1-1303(17) "**personal data**": (a) means information that is linked or reasonably linkable to an identified or identifiable individual.
Connecticut	Connecticut General Statute breach notification Law § 36a-701b(a)(2) "**personal information**" means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (A) Social Security number; (B) driver's license number or state identification card number; (C) credit or debit card number; or (D) financial account number in combination with any required security code, access code or password that would permit access to such financial account.
	Public Act No. 22-15 (The Connecticut Data Privacy Act), § 1(18) "**Personal data**" means any information that is linked or reasonably linkable to an identified or identifiable individual.
Utah	Utah Code (Chapter 44, Protection of Personal Information Act), § 13-44-102(4) (a) "**Personal information**" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii) (A) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that would permit access to the person's account; or (iii) driver license number or state identification card number.
	Utah Code (Consumer Privacy Act), § 13-61-101(24) (a) "**Personal data**" means information that is linked or reasonably linkable to an identified individual or an identifiable individual.
Virginia	Code of Virginia breach notification Law § 18.2-186.6(A) "**Personal information**" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number.
	Code of Virginia (Consumer Data Protection Act) § 59.1-575. "**Personal data**" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

Table 4.4: Excerpts of the two definitions of personal data adopted by the five U.S. States (i.e., *California, Colorado, Connecticut, Utah, and Virginia).*

Limiting the extent of breach disclosure rules by creating sub-categories of personal data.

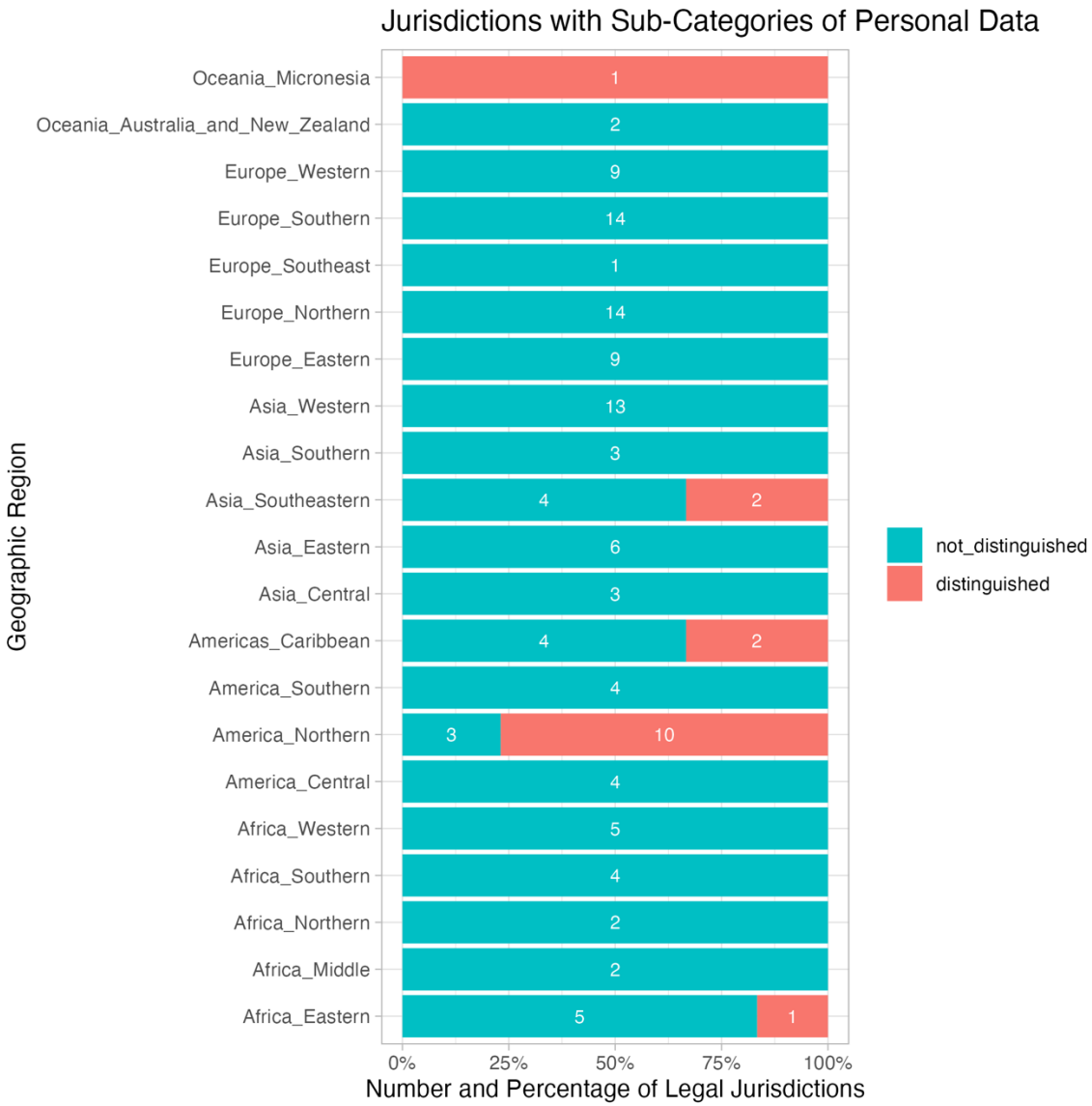

Figure 4.8: A visual representation of legal jurisdictions that created sub-categories of personal data, grouped by geographical region.

Data suggests that having an open-ended definition of personal data does not necessarily mean that a legal jurisdiction has adopted the broad scope approach. Instead of adopting a closed-ended definition of personal data, some legal jurisdictions created sub-categories of personal data to distinguish the data that would be covered by their breach notification rules (*see* Figure 4.8).

Out of 127 legal jurisdictions that adopted breach disclosure rules, there were 87.40% (111) that made no distinction and 12.60% (16) that made a distinction. Insofar as the legal jurisdictions that made a distinction is concerned, 13 of the 16 legal jurisdictions were in the United States, while the others are Malaysia, the Philippines, Zimbabwe:

1. Malaysia
2. Philippines
3. United States Alabama
4. United States Alaska
5. United States California
6. United States Colorado
7. United States Connecticut
8. United States District of Columbia
9. United States Federal
10. United States Guam
11. United States Oregon
12. United States Puerto Rico
13. United States Utah
14. United States Virgin Islands
15. United States Virginia
16. Zimbabwe

I mentioned earlier that US States and Zimbabwe confined the coverage of breach disclosure rules by adopting a close-ended definition of personal data. Meanwhile, legal jurisdictions such as Malaysia, the Philippines, and the US Federal Government created sub-categories of personal data for the purpose of breach disclosure (among others), as Table No. 4.5 below shows. I found that the Philippines created a sub-category (*i.e.*, sensitive personal data) within its own comprehensive privacy and data protection law, whereas the sub-categorization in Malaysia (*e.g.*, customer information) and the US Federal Government (*e.g.*, protected health information) were done through sector-specific laws:

Legal Jurisdiction	Legal Text
Malaysia	*Management of Customer Information and Permitted Disclosures – Central Bank of Malaysia, § 5.2.* "**customer information**" refers to any information relating to the affairs or, in particular, the account, of any particular customer of the FSP in whatever form including in the form of a record, book, register, correspondence, other document or material;
	Management of Customer Information and Permitted Disclosures – Central Bank of Malaysia. § 11.1. FSPs must have in place a **customer information breach** handling and response plan in the event of theft, loss, misuse or unauthorized access, modification or disclosure by whatever means of customer information. *§ 11.12.* In the event the customer information breach affects a large number of customers, FSPs must assess the potential impact and take appropriate actions to avoid or reduce any harm on the affected customers. *§ 11.13.* The actions referred to in paragraph 11.12 may include the following: (a) making a public announcement to notify the customers promptly to regain customers' confidence; (b) providing contact details for customers to obtain further information or raise any concern with regard to the breach; or (c) providing advice to affected customers on protective measures against potential harm that could be caused by the breach.

The Philippines	*Republic Act No. 10173 (Data Privacy Act of 2012), § 3(l).* **Sensitive personal information** refers to personal information: (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified. (Emphasis added)
	Republic Act No. 10173 (Data Privacy Act of 2012), § 20(f). The personal information controller shall promptly notify the Commission and affected data subjects when **sensitive personal information** or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. (Emphasis added)
Federal Government of the United States	*HIPAA Administrative Simplification Regulation Text, § 160.103.* **Health information** means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. *HIPAA Administrative Simplification Regulation Text, § 160.103.* **Protected health information** means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
	HIPAA Administrative Simplification Regulation Text, § 164.402. Breach means the acquisition, access, use, or disclosure of **protected health information** in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

Table 4.5: Excerpts from legal texts that illustrate how legal jurisdictions distinguish personal data by creating sub-categories.

Consequently, those that I had considered to have adopted a narrow scope of personal data types are these 16 legal jurisdictions that either had a closed-ended definition of personal data or had introduced a sub-category of personal data that will be subject to breach disclosure rules. I then categorized the rest of the legal jurisdictions as adopting a broad scope of personal data types.

In summary, my analysis in sub-section 1 suggests that merely relying on how the legal text defines personal data as open- or closed-ended would not be enough to determine whether breach disclosure rules would be triggered. I found that it is also crucial to understand if the legal jurisdiction created sub-categories of personal data types. To illustrate, there are legal jurisdictions like California that introduced two definitions of "personal information": (1) a closed-ended definition for the

purpose of breach notification;[83] and (2) an open-ended definition for the purpose of individual privacy protection.[84] There are also legal jurisdictions like Brazil that adopted a common definition for "personal data" for both breach notification and individual privacy protection.[85] Finally, there are legal jurisdictions like the Philippines that created a sub-category of personal information such that breach disclosure rules would only be triggered if the information involved falls under such sub-category (*e.g.*, sensitive personal information).[86]

The significance of having a ***broad scope*** versus a ***narrow scope*** goes into the determination of the personal data type that must have been involved in a data breach before breach disclosure rules are triggered. The broader the scope, the likelier that a data controller would need to inform data protection authorities and individuals about a breach.

2. The breach must create a risk harm.

In line with the study's focus on breach notification, I will now explore whether the law requires a harm threshold before individuals are notified of personal data breaches. I ask this question because of the seeming importance of the existence of harm before privacy violations are remedied in the United States. Citron and Solove[87] observed that the existence of harm has been firmly recognized as a necessary element of many causes of action, such that harm became a gatekeeper in privacy violation litigation. As such, "[c]ountless privacy violations are left unremedied not because they are unworthy of being addressed but because of the failure to recognize harm."

Figure 4.9 suggests that an overwhelming number of legal jurisdictions that mandate breach notification, *i.e.*, 70.80% (80 out of 113) require the existence of a possibility of harm before data controllers are obliged to notify individuals of a data breach. This number is composed of 70 legal jurisdictions that require the possibility of harm regardless of how severe the harm is, 9 that require a

[83] California Civil Code, §1798.82(i).
[84] California Civil Code (California Consumer Privacy Act of 2018), §1798.140(v)(1).
[85] Brazilian Data Protection Law (as amended by Law No. 13,853/2019), art. 5.
[86] Brazilian Data Protection Law (as amended by Law No. 13,853/2019), art. 5.
[87] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. REV. 703 [2022]; Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018).

certain level of severity, and 1 that require varying harm requirements, depending on the type of personal data that was involved.

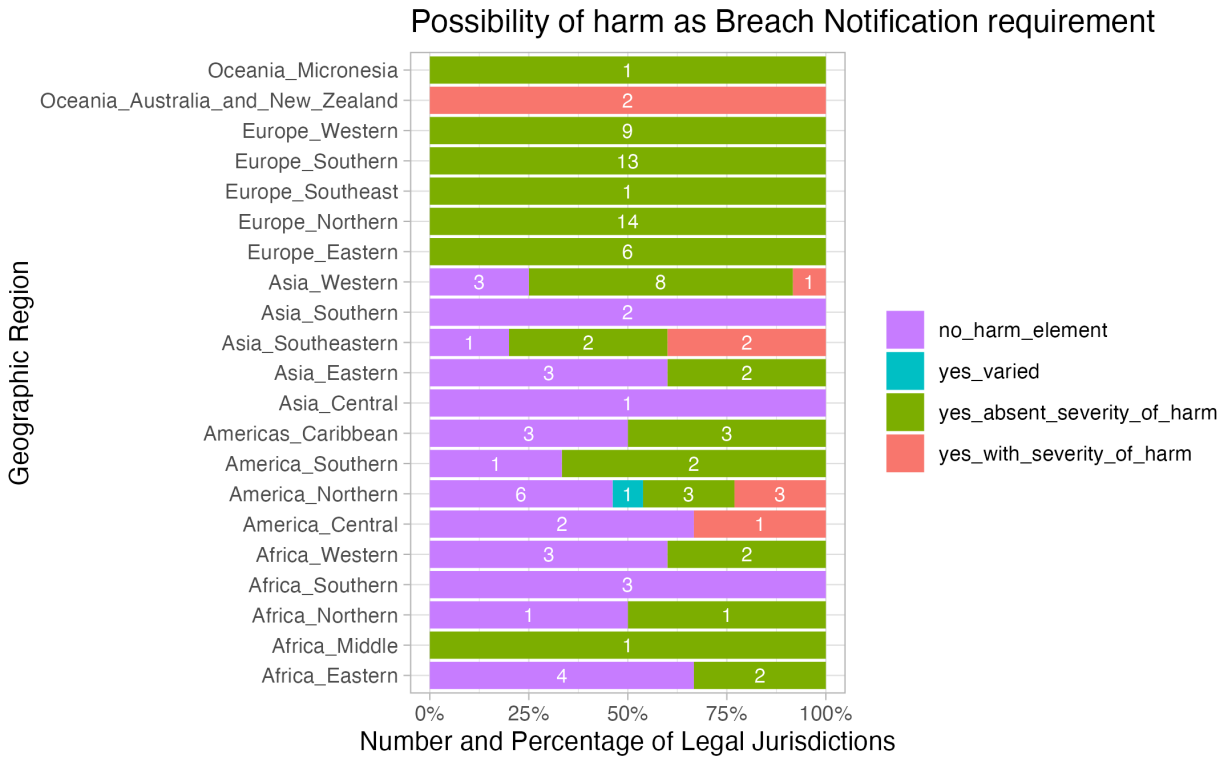

Figure 4.9: A visual representation of the legal jurisdictions that require the existence of a possibility of harm before individuals are notified of a breach, grouped by geographic region.

	Jurisdiction	Provision
No harm	**South Africa**	Where there are reasonable grounds to believe that the **personal information of a data subject has been accessed or acquired** by any unauthorised person, the responsible party must notify …
With harm	**Germany**	If a personal data breach is likely to result in a **substantial risk to the legally protected interests of natural persons**, the controller shall notify the data subject of the personal data breach without delay.
With harm + level of severity	**Australia**	if: (a) both of the following conditions are satisfied: (i) there is unauthorised access to, or unauthorised disclosure of, the information; (ii) a reasonable person would conclude that the **access or disclosure** would be **likely to result** in **serious harm** to any of the individuals to whom the information relates; ... then: (c) the access or disclosure covered by paragraph (a) ... is an eligible data breach ...

Table 4.6: Excerpts from legal texts that illustrate how legal jurisdictions adopt varying harm requirements before breach notification is triggered.

Table 4.6 provides a variety of examples of how legal jurisdictions frame their breach notification laws depending on whether there would be a harm requirement and, if there was, the threshold of harm required before individuals are informed of a data breach. For example, the wording of South Africa's Protection of Personal Information Act[88] suggests that mere existence of reasonable grounds to believe that the individual's personal data has been accessed or acquired by an unauthorized person would trigger the data controller's breach notification obligation. In contrast, Germany's Federal Data Protection Act[89] suggests that mere existence of a data breach is not enough to trigger the data controller's breach notification obligation; further, there must be an examination as to whether the said breach "is likely to result in a substantial risk to the legally protected interests of natural persons." Finally, the breach notification policy in Australia (textually) appears to set an even higher threshold than the substantial exposure to danger required in Germany, *i.e.*, that the data breach should be likely to result in "serious harm."

I observed that all the 9 legal jurisdictions that set a "severity of harm" threshold require a more stringent level of harm, *i.e.*, the harm must be "serious," "significant," or "substantial" (*see* Table 4.7).

Jurisdiction	Year Introduced	Title of Law	Severity of Harm Threshold
Canada (Alberta)	Nov 2009	Personal Information Protection Act of 2003[90]	significant harm
Philippines	Aug 2012	Data Privacy Act of 2012[91]	serious harm
Canada (Federal)	Jun 2015	Privacy Act of 1993[92]	significant harm
Qatar	Nov 2016	Data Protection Law of 2016[93]	serious damage

[88] Protection of Personal Information Act (Act 4 of 2013), South Africa, : https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-act-2013-004.pdf.
[89] Federal Data Protection Act of 30 June 2017, as amended by Article 10 of Act of 23 June 2021, Germany, : https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf.
[90] Province of Alberta Canada's Personal Information Protection Act of 2003, https://www.canlii.org/en/ab/laws/astat/sa-2009-c-50/latest/sa-2009-c-50.html.
[91] Philippines' Data Privacy Act of 2012, https://www.privacy.gov.ph/data-privacy-act/.
[92] Federal Government of Canada's Privacy Act of 1993, https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html.
[93] Qatar's Data Protection Law of 2016, https://compliance.qcert.org/en/library/privacy.

Mexico	Jan 2017	General Law on Protection of Personal Data held by Mandated Parties[94]	significantly affect
Australia	Feb 2017	Privacy Act of 1988[95]	serious harm
US (Alabama)	Mar 2018	Data Breach Notification Act of 2018[96]	substantial harm
New Zealand	Jun 2020	Privacy Act of 2020[97]	serious harm
Singapore	Nov 2020	Personal Data Protection Act of 2012[98]	significant harm

Table 4.7: Summary of legal jurisdictions that impose a severity of harm threshold before breach notification is triggered.

I did not find a clear explanation or indication from the legal texts why some legal jurisdictions had adopted a higher threshold of harm before notifying individuals. Nevertheless, I looked at other sources to seek guidance on the possible reasons why this approach was adopted. In this regard, the Australian Attorney-General's "Discussion Paper" on mandatory data breach notification is enlightening. He explained that Australia's adoption of "a relatively higher notification threshold than schemes in many other jurisdictions in that notification would only be required in serious cases" was intended to "help avoid the risk of individuals experiencing 'notification fatigue', and will also help avoid unnecessary administrative costs for business."[99]

C. Majority of the world imposes a stricter timeframe when reporting data breaches to data protection authorities.

Breach disclosure policies vary in terms of the timeframes given to data controllers to report to authorities and notify individuals about a personal data breach. I will discuss in this section the global trend on breach reporting is that data controllers are required to inform data protection authorities within a specified timeframe. Meanwhile, when it comes to breach notification to individuals, generality and not specificity of timeframe seems to be the global trend.

[94] Mexico's General Law on Protection of Personal Data held by Mandated Parties of 2017, https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017.
[95] Australia's Privacy Act of 1988, https://www.legislation.gov.au/Details/C2017A00012.
[96] US State of Alabama's Data Breach Notification Act of 2018, https://www.legislature.state.al.us/legacy/CodeOfAlabama/1975/174919.htm.
[97] New Zealand's Privacy Act of 2020, https://www.legislation.govt.nz/act/public/2020/0031/69.0/whole.html.
[98] Singapore's Personal Data Protection Act of 2012, https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210170000?DocDate=20201210170000.
[99] Australian Attorney-General's Department, *Discussion Paper: Mandatory data breach notification* (December 2015).

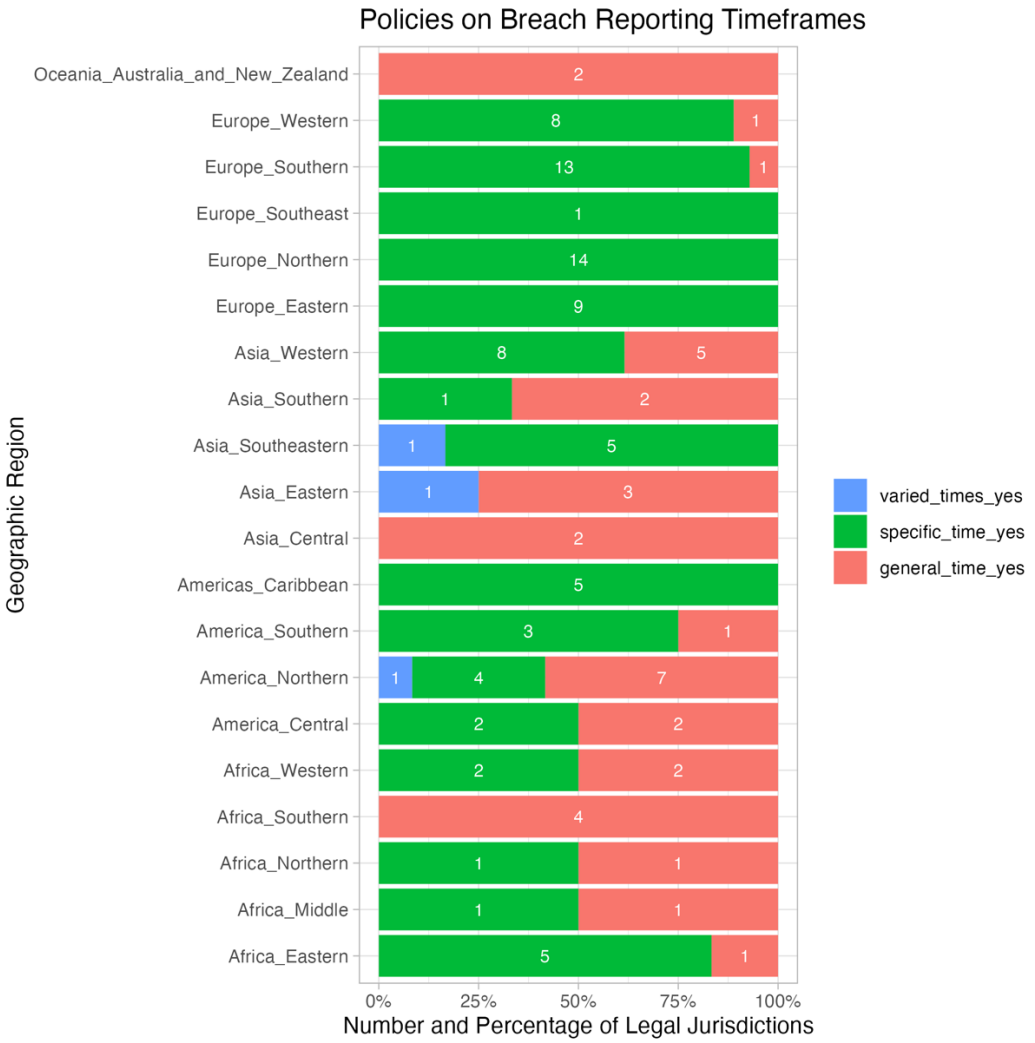

Figure 4.10: A visual representation of how legal jurisdictions impose a timeframe within which to perform breach reporting to authorities, grouped by geographic region.

Breach reporting. The data in Figure 4.10 suggests that 68.33% (82 out of 120) of the total number of legal jurisdictions that require breach reporting to authorities impose a specific timeframe within which to report. The timeframe ranges from 1 to 60 days – for example, Russia and Vietnam require data controllers to report personal data breaches within 24 hours after having become aware of it, Bhutan mandates reporting within 48 hours, the 27 European Union member countries that adopted the GDPR compel reporting within 72 hours, while the US State of Connecticut allows up to 60 days. Meanwhile, 29.17% (35 out of 120) do not provide for an exact period within which to report to the authorities (*see* Figure 4.10). Legal jurisdictions that adopted this approach instead use general terms

such as *immediately* (*e.g.*, China, Israel), *within a reasonable term* (*e.g.*, Brazil), *as soon as feasible* or *practicable* (*e.g.*, Canada - Federal, Ghana), or *without undue delay* (*e.g.*, Angola, Mexico).

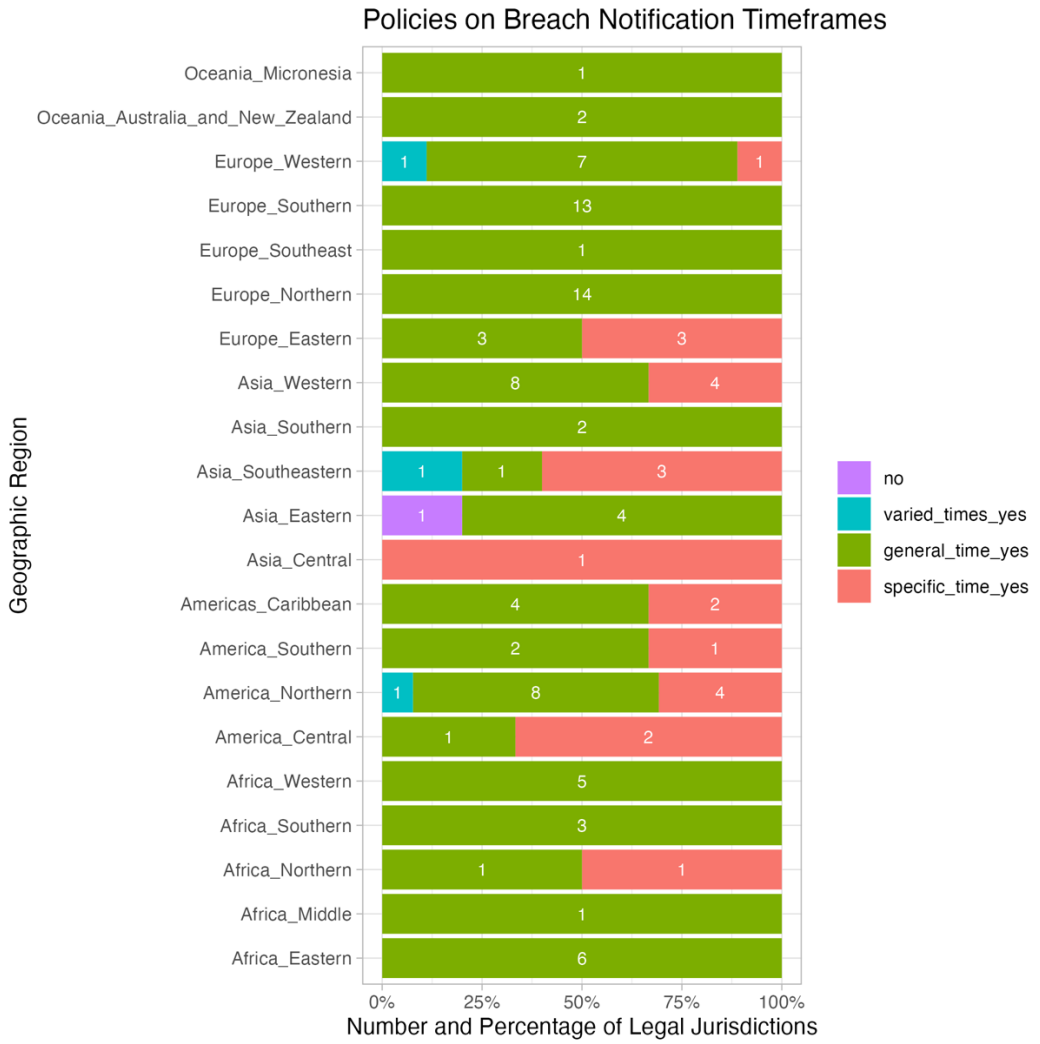

Figure 4.11: A visual representation of how legal jurisdictions impose a timeframe within which to perform breach notification to individuals, grouped by geographic region.

Breach notification. Data suggests that 87 out of 113 or about 76.99% of the total number of examined legal jurisdictions that require breach notification provide a general timeframe within which to notify data subjects (*see* Figure 4.11). Legal jurisdictions that adopted this approach used general terms such as *immediately* (*e.g.*, China, Estonia), *within a reasonable term* (*e.g.*, Brazil), *as soon as feasible* or *practicable* (*e.g.*, Eswatini, Ghana, New Zealand), or *without delay* or *undue delay* (*e.g.*, Austria, Benin). These terms are evidently similar to the language used in breach reporting. Meanwhile, 22 out of 113 or

about 19.47% of these legal jurisdictions impose a specific timeframe (*see* Figure 4.11). For instance, Barbados and Indonesia require notification within 72 hours after having become aware of it, Costa Rica grants 5 working days, Bulgaria allows up to 7 days, and the US State of Connecticut up to 90 days from the time the notification obligation is triggered. Only Taiwan out of 113 or about 0.88% neither provided a general nor a specific timeframe. Taiwanese law merely stated that the data controller has an obligation to notify individuals. Lastly, 3 out of 113 or about 2.65% of these legal jurisdictions set varying timeframes, as in the case of the US Federal Government which is governed by a sectoral approach to breach notification (*see* Figure 4.11).

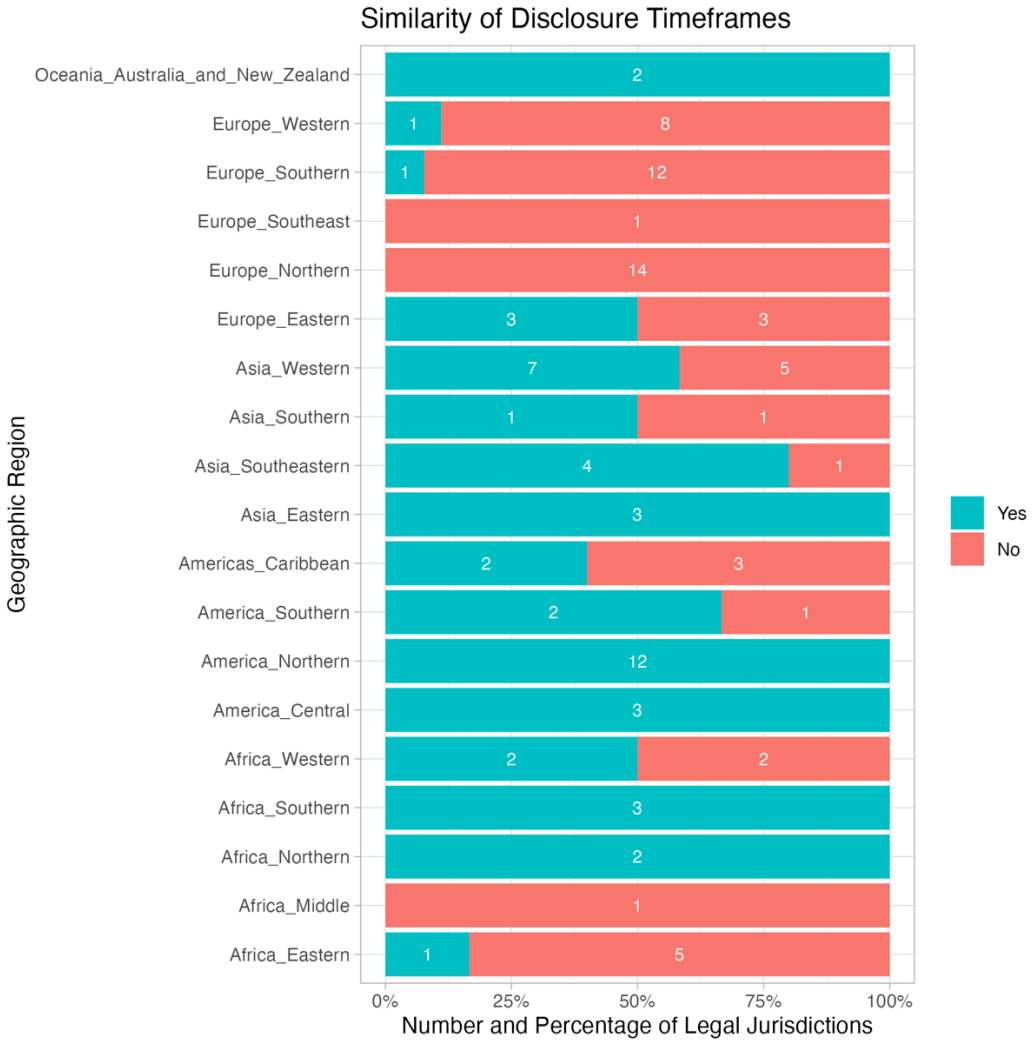

Figure 4.12: A visual representation of legal jurisdictions that require similar timeframes for breach reporting and breach disclosure, grouped by geographic region.

The fact that a legal jurisdiction had adopted a full breach disclosure policy did not appear to influence the *specific-timeframe-for-reporting* and *general-timeframe-for-notification* global trend. For example, of the legal jurisdictions that adopted a full breach disclosure policy, 53.77% (57 out of 106) had different rules on reporting-notification timeframes, while 46.23% (49 out of 106) had similar rules (*see* Figure 4.12).

In turn, 51.89% of the full breach disclosure legal jurisdictions (*i.e.*, 55 out of 106) require data controllers to perform breach reporting to authorities within a specified timeframe, while giving them leeway when it comes to when data controllers can perform breach notification to individuals (*i.e.*, either their respective laws provide a general timeframe or no timeframe) (*see* Figure 4.13). It is not immediately clear from the legal texts why there are differences between reporting and notification timeframes.

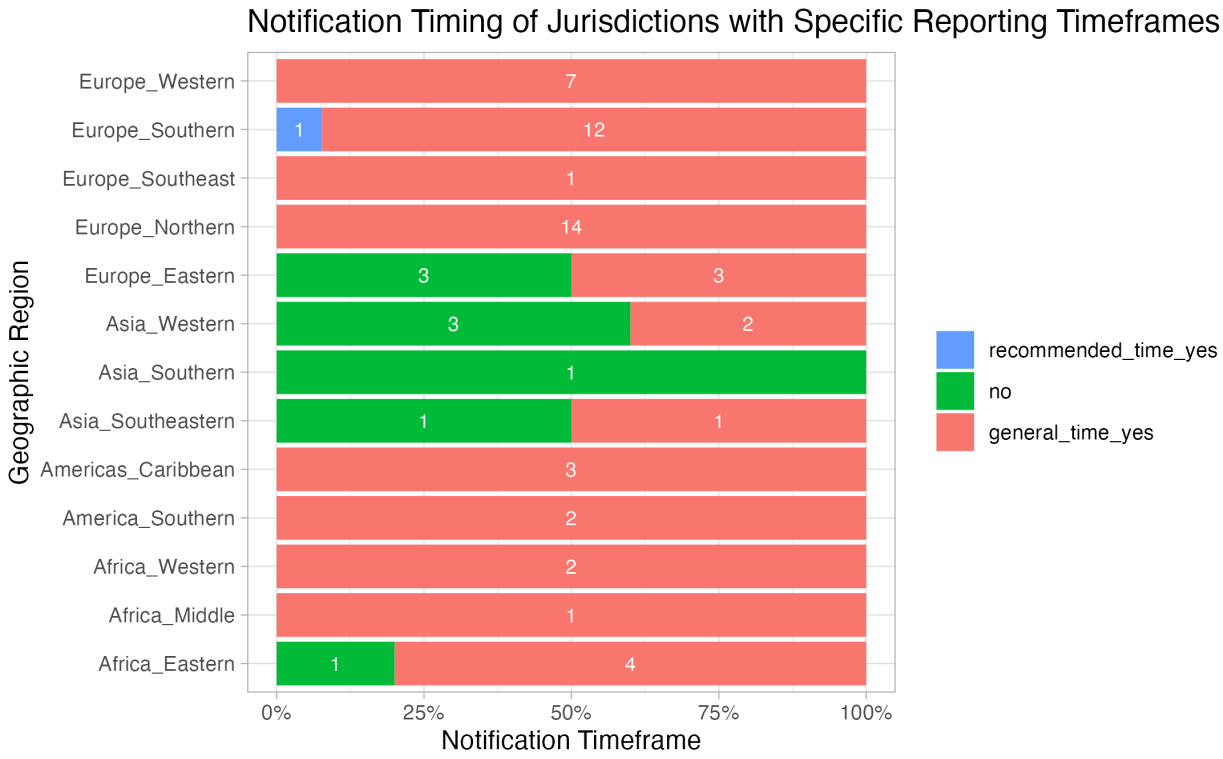

Figure 4.13: A visual representation of the legal jurisdictions that impose a non-specific timeframe for breach notification (even if they impose a specific timeframe for breach reporting), grouped by geographic region.

For legal jurisdictions that have adopted a full breach disclosure policy, I found that they either set (1) both reporting (R) and notification (N) rules with specific (S) timeframes (RS + NS) at 18.87% (20 out of 106); (2) both reporting (R) and notification (N) rules with general (G) timeframes (RG + NG) at 25.47% (27 out of 106); (3) a reporting (R) rule within a specific (S) timeframe and a notification (N) rule within a general (G) timeframe (RS + NG) at 51.89% (55 out of 106); or (4) a reporting (R) rule within a general (G) timeframe and a notification (N) rule within a specific (S) timeframe (RG + NS) at 0.94% (1 out of 106). The other remaining 3 legal jurisdictions (*i.e.*, Malaysia, Switzerland, and the US Federal Government) have varied timeframes. Based on this data, the global trend seems to be for legal jurisdictions to adopt a reporting rule within a specific timeframe and a notification rule within a general timeframe (RS + NG).

D. An overwhelming majority requires the inclusion of specific information when notifying individuals.

As the present study focuses on breach notification to individuals, I will now tackle the following additional questions in this section: (1) whether the law requires the inclusion of specific information when notifying data subjects; and (2) whether the law requires data controllers to communicate that they are performing or offering remedial measures that may benefit data subjects. I asked these questions to make sense of what legal jurisdictions perceive as sufficient to properly inform individuals of a data breach involving their personal data.

Figure 4.14 suggests that 80.53% of legal jurisdictions that mandate breach notification (91 out of 113) require the inclusion of specific information when notifying individuals. Meanwhile, 13.27% of legal jurisdictions (15) do not require specific information to be included; 4.42% (5 legal jurisdictions) have varying notification content requirements; and 1.77% (2 legal jurisdictions) merely recommend what should be included in the breach notification.

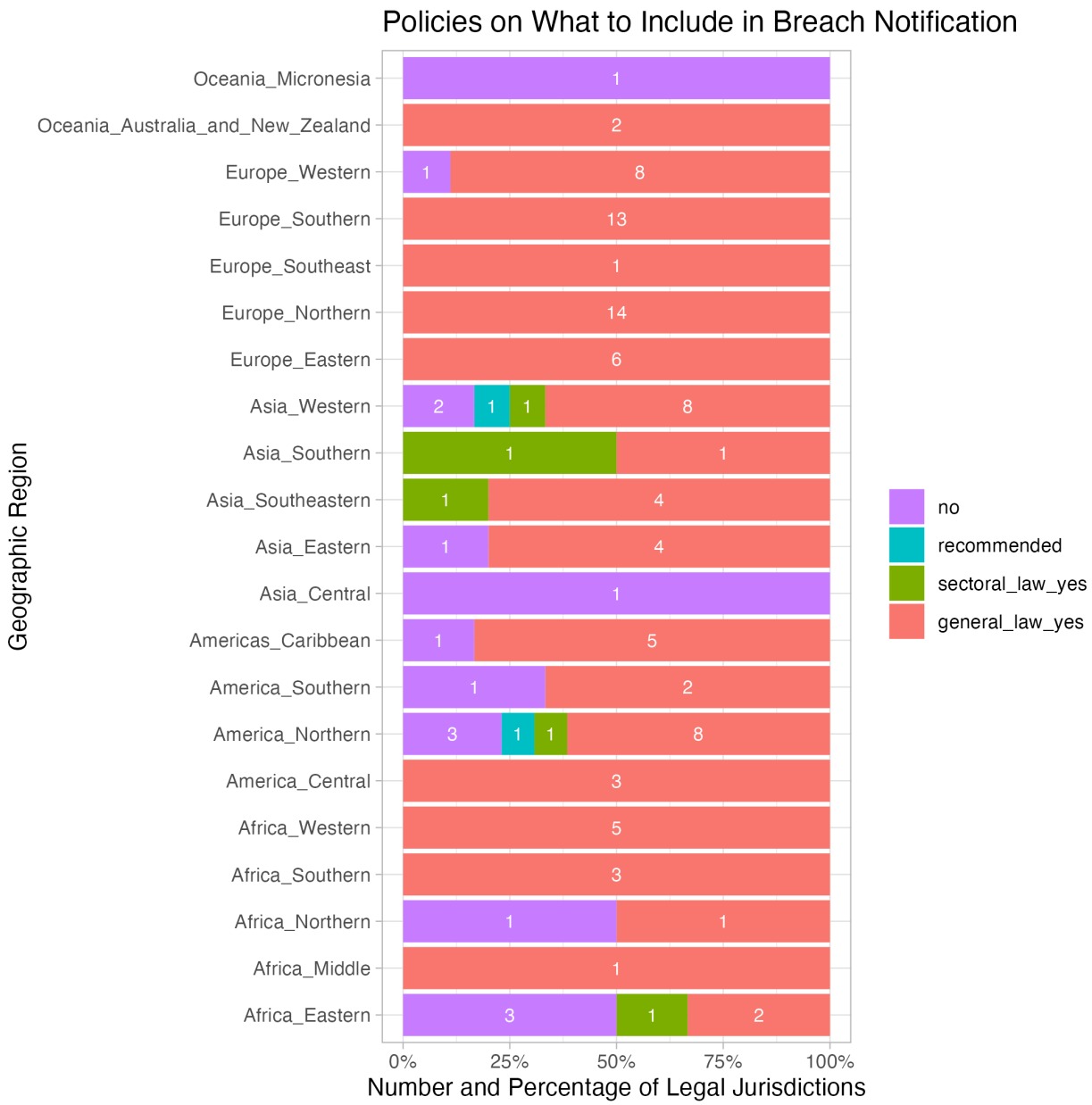

Figure 4.14: A visual representation of the various policies of legal jurisdictions when it comes to the inclusion of specific information in a breach notification, grouped by geographic region.

In Table 4.8 below, I provided examples of what legal jurisdictions require from data controllers to include in a breach notification. One important thing to consider is that the legal jurisdictions' respective laws merely set the minimum information to be included in the breach notification and that data controllers remain free to add further information.

	Australia	Bahrain	Brazil	California	Canada (F)	China	Croatia	France	Indonesia	Kenya	Mexico	New Zealand	Philippines	South Africa	Turkey
1. Information about Data Controller	✓			✓	✓	✓	✓	✓		✓		✓	✓		✓
2. Description of the circumstances surrounding the personal data Breach	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓		✓
3. Description of the personal data involved	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓		✓
4. Description of the security measures used to protect personal data			✓												
5. Risks or consequences associated with the personal data breach			✓			✓	✓	✓						✓	✓
6. Recommended defensive action by Data Subjects	✓	✓			✓	✓				✓	✓	✓		✓	
7. Measures to be taken by the Data Controller to reverse or mitigate the effects of the personal data breach			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8. Identity of the unauthorized actor involved in the personal data Breach										✓				✓	
9. Contact information of credit reporting agency				✓											
10. Offer to provide assistance or services to Data Subjects				✓									✓		

Table 4.8: Examples of what legal jurisdictions require in terms of what should be included in a breach notification.

Meanwhile, Figure 4.15 below suggests that 81.42% of legal jurisdictions that mandate breach notification (92 out of 113) require data controllers to perform or offer general remedial measures that may benefit individuals. In contrast, 13.27% (15 legal jurisdictions) did not expressly require performance or offer remedial measures; 2.65% (3 legal jurisdictions) merely recommend general measures; and another 2.65% (3 legal jurisdictions) require specific measures.

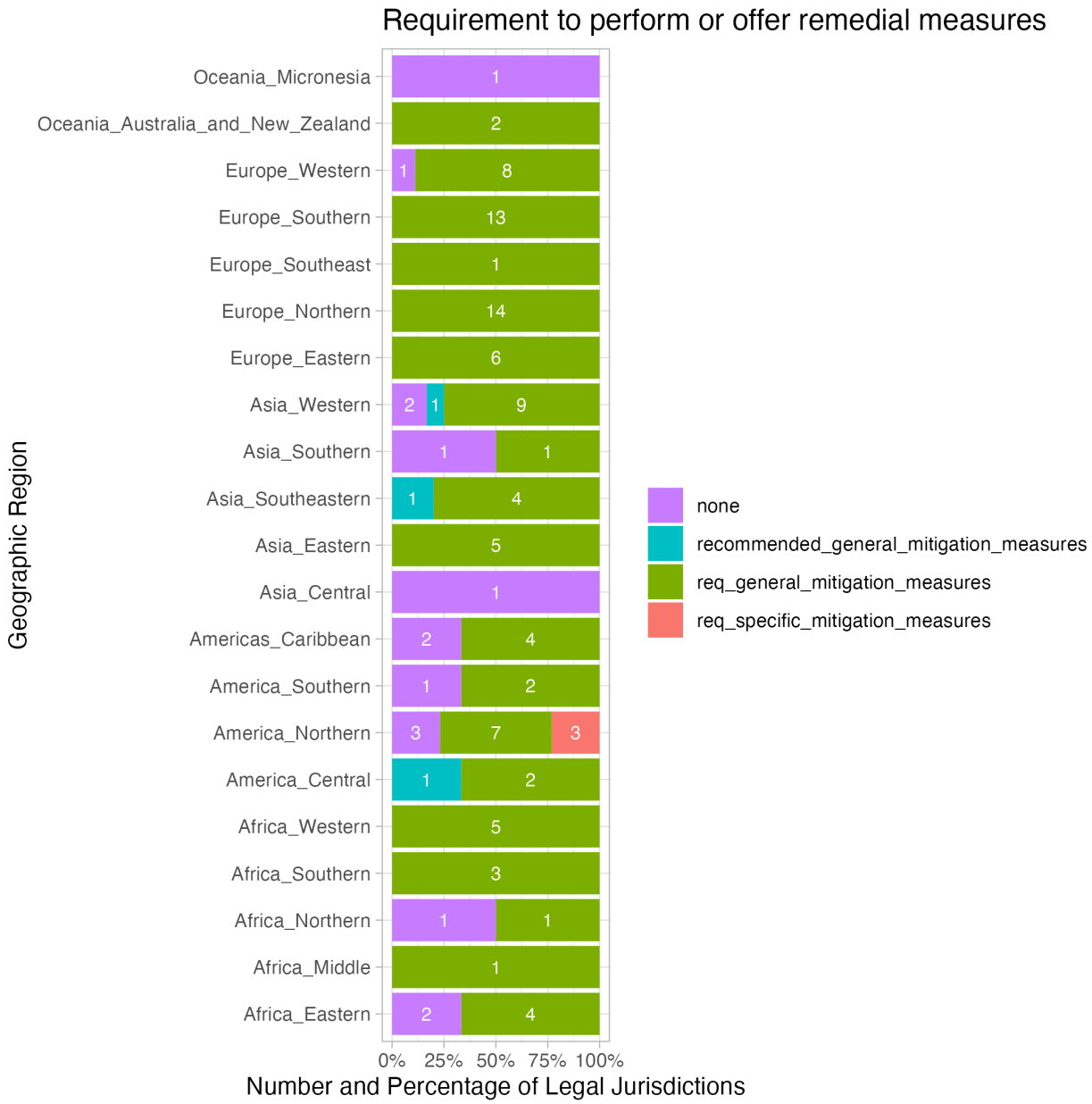

Figure 4.15: A visual representation of the various policies of legal jurisdictions when it comes requiring the performance or offer remedial measures, grouped by geographical region.

Legal jurisdictions do not substantially vary in terms of communicating the nature of remedial measures that data controllers are performing or offering to perform. As the data in Table 4.9 suggests, data controllers are given the leeway in ascertaining the measures to adopt in order to reverse or mitigate the effects of a data breach. What is notable is that both California and the Philippines require mention of any assistance to be provided to individuals. California goes a step further by legally

mandating data controllers to mention an "offer to provide appropriate identity theft prevention and mitigation services" at no cost to individuals. This legal requirement appears unique to California and a few other US legal jurisdictions such as Connecticut and the District of Columbia.

Legal Jurisdictions	Legal Provision
1. Brazil[100]	The controller must communicate to the national authority and to the data subject the occurrence of a security incident that may create risk or relevant damage to the data subjects. §1 The communication … shall contain, at the very least: … VI – the measures that were or will be adopted to reverse or mitigate the effects of the damage.
2. California (United States)[101]	A person or business that is required to issue a security breach notification ... (2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information: (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h). (3) At the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached. ...
3. Canada (Federal Government)[102]	A notification provided by an organization … to an affected individual with respect to a breach of security safeguards must contain … (d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach ….
4. China[103]	Where the breach, tampering, or loss of personal information occurs or may occur, a personal information processor shall immediately take remedial measures and notify the departments with personal information protection duties and the relevant individuals. The notice shall include the following items: … (2) the remedial measures adopted by the personal information processor and the measures the individuals may take to mitigate the harm ….
5. Croatia[104]	The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and ... describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

[100] Brazil's Data Protection Law, Art. 48, https://www.dataguidance.com/sites/default/files/lgpd_translation.pdf.
[101] California's Civil Code, Sec. 1798.82(d), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.
[102] Canada's Breach of Security Safeguards Regulations: SOR/2018-64, Art. 3, https://canadagazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html.
[103] Personal Information Protection Law of the People's Republic of China, Art. 57, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.
[104] EU's General Data Protection Regulation, Art. 34 in relation to Art. 33(3), https://gdpr.eu/article-33-notification-of-a-personal-data-breach/; Croatia's General Data Protection Regulation Implementation Act 2018, https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html.

6. France[105]	The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and ... describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
7. Indonesia[106]	In the event of failure of personal data Protection, the personal data Controller must give written notification … to: a. personal data Subject … (2) The written notification … shall contain at least: … c. efforts to handle and recover the disclosure of personal data by the personal data Controller.
8. Kenya[107]	The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including — … (b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach; (c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise ….
9. Mexico[108]	The person in charge must inform the owner of at least the following: … III. Recommendations to the owner about the measures he can adopt to protect his interests; IV. Corrective actions taken immediately, and ….
10. New Zealand[109]	A notification to an affected individual under section 115 or a representative under section 116(3) must— (b) explain the steps taken or intended to be taken by the agency in response to the privacy breach; and (c) where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any) ….
11. Philippines[110]	The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures: ... The notification shall include, but not be limited to: ... measures taken to address the breach; measures taken to reduce the harm or negative consequences of the breach; ... and any assistance to be provided to the affected data subjects.
12. South Africa[111]	The notification of a data subject referred to in subsection (1) must provide sufficient information to allow the data subject to take proactive measures against the potential consequences of the compromise, including-- (b) a description of the measures that the responsible party intends to take or has taken to address the security compromise; (c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise ….

[105] EU's General Data Protection Regulation, Art. 34 in relation to Art. 33(3), https://gdpr.eu/article-33-notification-of-a-personal-data-breach/; France's General Data Protection Regulation Implementation Act 2018, https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html.

[106] Indonesia's Law No. 27 of 2022 regarding Personal Data Protection, Art. 46, https://peraturan.bpk.go.id/Home/Download/224884/UU%20Nomor%2027%20Tahun%202022.pdf.

[107] Kenya's Data Protection Act of 2019, Sec. 43(5), https://www.odpc.go.ke/dpa-act/.

[108] Mexico's General Law on the Protection of personal data in Possession of Obliged Subjects (Ley General de Proteccion de Datos Personales en Possesion de Sujetos Obligados), Art. 41. Text (in Spanish), https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[109] New Zealand's Privacy Act of 2020, Sec. 117(2), https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html.

[110] Philippine's National Privacy Commission Circular 2016-03 – Personal Data Breach Management, Sec. 18, https://www.privacy.gov.ph/memorandum-circulars/npc-circular-16-03-personal-data-breach-management/.

[111] South Africa's Protection of Personal Information Act, Art. 22(5), https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

13. Turkey[112]	The breach notification to be made by the data controller to the relevant person is made in a clear and plain language, and as a minimum; … Measures taken or proposed to be taken to reduce the negative effects of data breach ….

Table 4.9: Excerpts from the legal texts of various legal jurisdictions, providing examples of how they frame breach notification requirements, especially in terms of communicating the nature of remedial measures to be performed or offered.

4.2 Analysis

In section 4.1, I sifted through hundreds of legal texts to answer the survey questions in Annex 1. In so doing, I was able to synthesize my findings on various aspects of the global breach disclosure rules. In this section, I will go full circle and answer my five main research questions.

A. Research Question 1: What are the global trends on whether there is a legal requirement for data controllers to disclose personal data breaches?

I described in section 4.1(A) that out of the 187 legal jurisdictions studied, I discovered that an overwhelming number of legal jurisdictions (67.91%) adopted a breach disclosure rule. This indicates a global trend: the world is moving towards legally mandating data controllers to reveal the occurrence of a personal data breach. From a single US State (California) passing a unique and innovative law in 2003,[113] the obligation to disclose has spread to 127 legal jurisdictions, becoming a worldwide requirement. Organizations can no longer conceal a failure in their data security.[114] If we espouse the idea that law mirrors societal values, then it is reasonable to say that the world now expects data controllers to issue an alert that the individuals' personal data have been compromised.

Moreover, through systematic content analysis, I identified and categorized three breach disclosure policies – full breach disclosure policy, government-centered reporting policy, and data subject-centered notification policy. Significantly, out of the 127 legal jurisdictions that adopted a breach disclosure rule, an overwhelming 83.46% (106) adopted a full breach disclosure policy, while

[112] Turkey's Law on Protection of personal data No. 6698, Art. 12(5), https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law; Board Decision 2019/10 (24 January 2019) regarding the notification procedures and principles related to personal data breach. Text (in Turkish), https://www.kvkk.gov.tr/Icerik/5547/2019-271.
[113] SOLOVE & HARTZOG, *supra*, note 16; Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; Ablon, *et. al.*, *supra*, note 19; Bisogni, *supra*, note 19.
[114] *See* SOLOVE & HARTZOG, *supra*, note 16 at 37.

only 11.02% (14) adopted a government-centered reporting policy, and 5.51% (7) adopted a data subject-centered notification policy. That the world is moving towards full breach disclosure is a significant development in the light of the twin goals of breach disclosure rules that Bisogni identified, the achievement of which can be best done through a full breach disclosure policy. According to Bisogni, breach disclosure rules typically have two main goals: first, to alert individuals so that they can employ mitigation measures against risks of harms arising from the personal data breach; and second, to introduce a market-based incentive so that data controllers can improve security measures that protect personal data.[115] A full breach disclosure policy is most consistent with these twin goals, since – for good measure – it provides two avenues for achieving them. This in contrast to a government-centered reporting only policy or a data subject-centered notification only policy, which gives only one avenue.

I then identified the 14 legal jurisdictions[116] that adopted a breach disclosure policy, which does not center on directly warning individuals to protect themselves from harm (*i.e.*, government-centered reporting policy). Categorizing these legal jurisdictions may prove useful for future research, especially when investigating the underlying reasons for preferring reporting to data protection authorities over notifying individuals. Going back to Bisogni's twin goals of breach disclosure, it is unclear whether such a policy can achieve the aims of the first goal – further research is thus necessary to understand the underlying reasons why the 14 legal jurisdictions preferred reporting to data protection authorities over notifying individuals. It is possible that individuals would eventually be informed of personal data breaches once the data protection authority determines that it is in their best interest to know. In fact, this approach had been adopted by Israel and Sri Lanka. For Israel, the data controller may be ordered to notify individuals about the security incident if they may suffer damage from such an event.[117] In the case of Sri Lanka, its data protection authority will determine the circumstances in which individuals would be notified.[118] While one can argue that a government-

[115] Bisogni, *supra*, note 19, *citing* Paul Schwartz and Edward Janger, *Notification of Data Security Breaches*, 105(5) MICH. L. REV. 913 (2007); and Steve Ranger, *Data Breach Laws Make Companies Serious about Security*, SILICON.COM (3 Sep 2007), http://management.silicon.com/itdirector/0,39024673,39168303,00.htm?r=1. *See also* SOLOVE & HARTZOG, *supra*, note 16; Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; Ablon, *et. al.*, *supra*, note 19.

[116] These legal jurisdictions are the following: Albania, Angola, Belarus, Botswana, Colombia, Guatemala, India, Kazakhstan, Macau, Moldova, Russia, Saudi Arabia, Uzbekistan, and Vietnam.

[117] Israel's Protection of Privacy Regulations (Data Security) Sec. 11(d)(1) (2017), https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf.

[118] Sri Lanka's Personal Data Protection Act of 2022, Article 23(2), https://www.dataguidance.com/sites/default/files/personal_data_protection_act_no._6_of_2022.pdf.

centered policy can be adopted as a way to address breach notification fatigue or as a way to avoid impeding criminal investigation or jeopardizing national security,[119] the value of such arguments requires further research and consideration.

B. Research Question 2: What are the global trends in trigger requirements for when data controllers are legally required to notify individuals?

The prevailing global breach notification policy seems to be that individuals should be informed of a breach if it involves their personal data (with broad scope) and if there is a risk of harm to them. I explained in section 4.1(B) that an overwhelming number of legal jurisdictions with breach notification obligation (87.61% or 99 out of 113) adopted a broad scope of personal data types. In addition to the materiality of the personal data type, an overwhelming number of legal jurisdictions (70.80% or 80 out of 113 that require breach notification) also require a risk of harm threshold before individuals are notified of a personal data breach.

The significance of this finding is that, globally speaking, individuals are more likely to be informed of a personal data breach. Especially in view of the rapidly increasing rate of cyber fraud and identity theft,[120] this finding is great news for individuals – one of the avowed purposes of breach notification rules is to make sure that they can timely employ mitigation measures to protect themselves against possible harm. The alternative approach posited by the Australian Attorney-General, however, deserves thorough consideration. According to him, one of the reasons Australia adopted a comparatively higher notification threshold was to address the risk of breach notification fatigue. This reasoning is particularly interesting, especially in the light of the rising views that we may have already reached a point of experiencing a "data breach fatigue."[121] They claim that individuals

---

[119] *See, e.g.*, Bisogni, *supra*, note 19 at 164, in which he recognized that "notifications may in fact be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security"

[120] *New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020*, 4 February 2021, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers (hereinafter "FTC, *New Data Shows*").

[121] Sasha Jones, *What Is Breach Fatigue and Does It Contribute to Rise in Data Compromises*, NBC (24 Jan 2022), https://www.nbcmiami.com/responds/what-is-breach-fatigue-and-does-it-contribute-to-rise-in-data-compromises/2668964/; Bethan Moorcraft, *Are US consumers suffering from data breach notification fatigue?*, INSURANCE BUSINESS AMERICA (19 Jun 2019), https://www.insurancebusinessmag.com/us/news/cyber/are-us-consumers-suffering-from-data-breach-notification-fatigue-170386.aspx; Michael Bruemmer, *The misconceptions of data breach fatigue*, IAPP (22 Feb 2016), https://iapp.org/news/a/the-misconceptions-of-data-breach-fatigue/.

have now started tuning out of these notifications given how prevalent they are, as if personal data breaches have now been accepted as an unfortunate fact of life.[122] Further research is necessary to see if the Australian approach can strike a good balance between the need to be alerted and the need to address breach notification fatigue. The nine legal jurisdictions that currently have a higher breach notification threshold compared to the global trend might be fertile ground for such a research.

C. Research Question 3: What are the global trends on the legally mandated timeframes within which individuals should be notified?

Global breach disclosure policies vary in terms of the timeframes given to data controllers to report to data protection authorities and notify individuals about a personal data breach. The global trend is that majority of legal jurisdictions (68.33% or 82 out of 120) require a specific timeframe within which to report a breach, ranging from 1 to 60 days. Meanwhile, majority of legal jurisdictions (76.99% or 87 out or 113) require data controllers to notify individuals about the breach, typically using general terms such as immediately, within a reasonable term, as soon as feasible or practicable, or without delay or undue delay. These suggest that data controllers are given the discretion to ascertain when to inform individuals about breaches, while no exercise of discretion is necessary to report to data protection authorities. This does not bode well for individuals, because general timeframes make it more difficult to determine the reckoning period for negligent delays in notifying them and to exact accountability for that. In contrast, specific measurable timeframes facilitate determination whether there has been a delay and make it easy for individuals to demand accountability. This will, in turn, force data controllers to act fast, thereby halting potential further harms.

I did not find any reasoning in the legal texts why there was a divergence in the disclosure timeframes. In fact, it is curious that the government is likelier to know about the incident even before individuals who own the personal data that was breached. If one of the reasonings behind breach disclosure laws is to immediately inform individuals so that they can perform protective measures, it is interesting to know why legal jurisdictions decided that breach notifications need not have a more

[122] *Id.*

stringent timeframe. Further research is needed to understand whether setting a general timeframe is more beneficial to individuals.

D. Research Question 4: What are the global trends on legally requiring data controllers to communicate certain information when notifying individuals?

Worldwide trend shows that it is global policy to regulate the content of breach notices. Simply communicating to individuals that their personal data were compromised is not enough. An overwhelming 80.53% of legal jurisdictions (91 out of 113) require the inclusion of specific information when notifying individuals. Equally overwhelming is the percentage of legal jurisdictions (81.42% or 92 out of 113) that require data controllers to communicate the nature of remedial measures they are performing or offering to perform.

Considering that the rate of cyber fraud and identity theft has been rapidly increasing,[123] giving data controllers the leeway to ascertain the measures to adopt in order to reverse or mitigate the effects of a data breach may not be enough. It may be necessary for breach disclosure policies to consider including specific measures. For example, California goes a step further by legally mandating data controllers to mention an "offer to provide appropriate identity theft prevention and mitigation services" at no cost to individuals. This policy requiring specific notification content as well as the communication of remedial measures – and not just leave these to data controllers – could be viewed as reassuring to individuals and as a movement toward better protecting their emergent right to be alerted.

[123] FTC, *New Data Shows*, *supra*, note, at 120.

Chapter 5
Conclusion

In 2003, California passed the first breach disclosure law – a unique and innovative law that required data controllers to notify individuals when a personal data breach occurs.[124] Twenty years later, the policy compelling organizations to reveal the fact that they suffered from a personal data breach had spread like wildfire. Now, at least 127 legal jurisdictions have adopted breach disclosure rules, suggesting that data controllers around the world have practically lost their ability to conceal a failure in their security. Such failures can no longer be kept as ugly company secrets, swept under the rug, and whispered only within company corridors.[125]

As Bisogni predicted,[126] governments indeed could play a pivotal role in setting the policy on breach disclosures. The current global trend shows that data controllers worldwide are now legally required to inform data protection authorities and individuals about a data breach. Insofar as protection of individuals is concerned, it is encouraging to see that the right to be alerted has now been recognized worldwide.

Bisogni also highlighted the importance of when breach notices are sent out. In this regard, global trend dictates that legal jurisdictions have coalesced insofar as when breach disclosure rules would be triggered. The breach must have affected personal data and created a risk of harm to individuals. If these *type-of-data* and *risk-of-harm* trigger requirements are not present, data controllers are not obligated to reveal the failure in their data security (unless required by a different law). In turn, global trend shows that data controllers must report the personal data breach within a specific timeframe, typically not more than 60 days; and then notify individuals within a general timeframe, usually within a reasonable time that would enable them to employ protective countermeasures. The variance between the reporting and the notification timeframes seems problematic, especially considering the alleged purpose of breach disclosure rules: to alert individuals. Policymakers must thus reassess the underlying reason behind such variance and ascertain whether the policy is in the interest of individuals.

---

[124] SOLOVE & HARTZOG, *supra*, note 16 at 39.
[125] *Id.*
[126] Bisogni, *supra*, note 19.

Finally, Bisogni proposed the need to strictly regulate the content of these notices to ensure that data controllers do not downplay the actual risks to individuals. On this front, the global trend is rather encouraging: worldwide practice indicates that legal jurisdictions have indeed regulated the content of breach notices, and so data controllers must ensure that their breach notifications contain the necessary minimum information. Data controllers must also communicate the measures they have implemented to mitigate the impact of the breach. Policymakers, however, need to consider taking the next step if the main goal is to alert individuals so that they can employ protective countermeasures. For example, legal jurisdictions can strengthen responses to personal data breaches by addressing Zou *et al.*'s[127] findings on the readability of breach notices, as well as their structure, risk communication, and presentation of potential actions as I discussed in Chapter 2. Legal jurisdictions might also want to tackle the "prohibitively difficult" countermeasures that individuals might employ to protect themselves. An example would be how California legally mandates data controllers to mention an "offer to provide appropriate identity theft prevention and mitigation services" at no cost to individuals.

Towards a global model on breach disclosure?

In Chapter 1, I argued that a study on global breach disclosure rules can provide evidence of global values and societal expectations when it comes to alerting individuals about data breaches. Indeed, data shows that the global community recognizes an individual's right to be alerted. What is more, it has been the practice of legal jurisdictions around the world to regulate the content of breach notifications, which only serves to highlight the importance of effectively informing individuals about the breach and the nature of remedial measures that data controllers are performing or offering to perform. Given these, what then could be the components of a global model approach to breach disclosure?

1. The starting point is to frame breach disclosure as being akin to an individual right and a subset of one's right to privacy and right to human dignity, rather than being seen as a mere regulatory compliance issue. The value of reframing how we view breach disclosure rules – *i.e.*, a right to be alerted – is that we effectively elevate it to an individual rights-level status. Corollary to such

[127] Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19.

status is the ability of individuals to make demands in relation to such right, that is, an actionable right to be informed. This is only natural, especially in this digital age when everything about us has been reduced to digital dossiers, making privacy harms more insidious and devastating when accessed by bad actors. In particular, the right to be alerted can be treated as akin to the other global rights recognized under various international human rights instruments (*e.g.*, the Covenant on Civil and Political Rights with 174 state parties[128] and the Covenant on Economic, Social, and Cultural Rights with 171 state parties[129]) such as the right to privacy; right to choose one's residence; right to the protection against interference or attacks on one's honor and reputation; right to freedom of thought, conscience and religion; right to hold opinions without interference; right to freedom of association with others, including the right to form and join trade unions; right of everyone to the enjoyment of the highest attainable standard of physical and mental health; right of everyone to education; right of everyone to take part in cultural life; and others. I argue that the global model approach to breach disclosure should be seen through an individual rights angle, especially considering that the subject of all these global rights I have just identified are now typically represented in digital format.

2. Viewed from the lens of an individual right, a global model approach to breach disclosure should, at minimum, contain the twin requirements of reporting to authorities and notification to individuals. As regards the first requirement (breach reporting), government can play a crucial role in keeping individuals informed about data breaches as well as the protective actions they can take against privacy harms. An example of what the government can do would be what the US Federal Trade Commission ("FTC") did when it took a proactive stance during the Equifax data breach saga[130] when they launched a nationwide information campaign on how the victims can protect themselves.[131] A similar approach has been done by the Australian

---

[128] Status of the Covenant on Civil and Political Rights as of 02 May 2023, UNITED NATIONS, https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND.
[129] Status of the Covenant on Economic, Social, and Cultural Rights as of 02 May 2023, UNITED NATIONS, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-3&chapter=4.
[130] *See:* FTC, *Equifax Data Breach Settlement*, *supra*, note 28; *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FEDERAL TRADE COMMISSION (22 Jul 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach (hereinafter "FTC, *Equifax to Pay $575 Million*").
[131] *See: FTC Encourages Consumers to Opt for Free Credit Monitoring, as part of Equifax Settlement*, FEDERAL TRADE COMMISSION (31 Jul 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-encourages-consumers-opt-free-

Information Commissioner during the Optus data breach.[132] With respect to the second requirement (breach notification), the perspective should be to give individuals a genuine opportunity to decide for themselves whether, how, and when they should employ protective measures. This means that they should be directly notified of a data breach. We have seen from the incidents in Singapore and India how serious and life-threatening data breaches can be, and so individuals should be deemed to know what the best course of action could be depending on their personal circumstances. A global model approach to breach disclosure that provides less than these twin requirements can only serve to minimize the effectiveness of the right to be alerted.

3. In line with the overall goal of giving individuals every opportunity to protect themselves, breach disclosure rules should consider limiting, if not outrightly eliminating, the data controllers' exercise of discretion when disclosing breaches. For example, rules should carefully delineate when an incident surpasses the risk-of-harm threshold in a way that what qualifies as a risk of harm should not be subject to the data controllers' interpretation and individual evaluation. Borrowing from the time-honored legal principle of *in dubio pro reo* (when in doubt, in favor of the accused), rules can consider a parallel principle of *in dubio pro victima* such that all doubts as to whether to inform, or whether there is risk of harm, should be decided in favor of the victim. Another example of when data controllers exercise discretion is the timeframe within which breach reporting and notification should be performed. From the standpoint of a right to be alerted, it does not make much sense that governments are alerted first before individuals when it is the latter who are the ultimate victims of the data breach. Disclosure timeframes should be as short as possible, given the speed with which bad actors can release data and the potentially devastating impact of such releases. This means that breach disclosure rules should set specific timeframes for both breach reporting and breach notification. Further, specific measurable timeframes facilitate determination whether there has been a delay in informing individuals and make it easy for them to demand accountability. This will, in turn, force data controllers to act fast, thereby halting potential further harms.

---

credit-monitoring-part-equifax-settlement (hereinafter "FTC, *Encourages Consumers to Opt for Free Credit Monitoring*".); Alvaro Puig, *Equifax Data Breach Settlement: What You Should Know*, FEDERAL TRADE COMMISSION (22 Jul 2019), https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know.

[132] *See: Advice on Optus data breach*, Office of the Australian Information Commissioner (14 Oct 2022), *https://www.oaic.gov.au/newsroom/advice-on-optus-data-breach*.

4. A full recognition of the right to be alerted should entail the effective communication of the potential impact of the data breach, so that individuals can truly make informed decisions as to the defensive countermeasures that they need to perform. Following research,[133] rules should mandate breach notifications to be readable and in plain language, without downplaying the consequences and risks of data breach. Following global trends and innovations, breach notifications should include the following components at minimum:

   a. clear and concise description of the circumstances surrounding the personal data breach, so that individuals understand whether there were lapses on the part of the data controller;
   b. clear and concise description of the personal data involved, so that individuals can get a better picture of the seriousness and severity of the breach;
   c. clear and concise description of the security measures used to protect personal data as well as any improvements implemented to remedy gaps in them, so that individuals are informed of how data controllers protect their data;
   d. clear and concise description of the risks or consequences associated with the personal data breach, so that individuals are informed of how they can be affected by the breach;
   e. clear and concise description of the specific measures undertaken or to be taken by the data controller to reverse or mitigate the effects of the personal data breach together with their proposed timelines, so that individuals know whether the measures are enough to protect themselves given their individual circumstances;
   f. clear and concrete recommended defensive actions that individuals can take in addition to the measures to be taken by the data controller, so that individuals know what else they can do to protect themselves given their individual circumstances;
   g. general description of the unauthorized actor involved in the personal data breach, so that individuals can get a better picture of the seriousness and severity of the breach and the gravity of the damage they may suffer;
   h. contact information of the relevant agencies, so that individuals know who to reach out to when the need arises; and

[133] Zou, *et. al., You 'Might' Be Affected*, (2019), *supra*, note 19; Ponemon Institute, The Aftermath of a Data Breach: Consumer Sentiment (Technical Report) (2014) ; Zou, *et. al.*, *Beyond Mandatory*, (2019), *supra*, note 23; Bisogni, *supra*, note 19.

i. clear and concise statement on the presence or absence of assistance or services, which would be offered or provided to individuals, so that they know the kind of protective services available to them.

5. Finally, from the standpoint of an individual right, alerts should not only serve as a mechanism for transparency, but also accountability. In this regard, a global model approach to breach disclosure should use breach notification to exact meaningful accountability insofar as individuals are concerned. For example, part of the data controllers' mandatory notification could be to communicate how they intend on improving their information security program to remedy any gaps in their security measures.[134] They may also be mandated to specify how they plan on reversing or mitigating the effects of the breach, such as offering free credit monitoring or cash payment, reimbursement for time and other cash payments, and free identity restoration services.[135] As another form of accountability, they may also be mandated to inform individuals if the company has experienced a data breach before and what has been done to address the past breach. Just like how the FTC conducted a nationwide information campaign during the Equifax breach saga, data controllers can also be mandated to conduct similar campaigns to educate individuals. Building on Ablon *et al.*'s study,[136] the whole breach notification regime should also seek the reduction of costs associated with the prohibitively difficult and high costs of consumer-initiated protective action to encourage individual response.

Viewed from the perspective of an individual right to be alerted, I argue that a global model approach to breach disclosure should be to consider the best interest of individuals as the primary goal. Reputational risks of data breaches to data controllers should not override this goal, especially if legal jurisdictions were to maintain the risk-of-harm requirement. Seen from this standpoint, governments and data controllers should not be given much discretion in ascertaining when individuals should be informed about data breaches concerning their personal data. Individuals should be given the opportunity to ultimately decide what the best course of action would be to protect themselves.

---

134 *See, e.g.:* FTC, *Equifax Data Breach Settlement*, *supra*, note 28; FTC, *Equifax to Pay $575 Million*, *supra*, note 130; FTC, *Encourages Consumers to Opt for Free Credit Monitoring*, *supra*, note 131; Puig, *supra*, note 131.
135 *See, e.g.: id.*; Puig, *supra*, note 131.
136 Ablon, *et. al.*, *supra*, note 19.

Future Work

We can consider this study as laying the groundwork for future research on many areas. For example, now that we have gathered and analyzed the breach disclosure rules of 187 legal jurisdictions, future research can explore how these global trends compare with existing best practices recommended by research for breach notice design. Further research may also be necessary to consider how legal jurisdictions can address breach notification fatigue, and whether Australia's approach in increasing the notification threshold might be a viable solution amidst the rising rate of cyber fraud and identity theft.[137] For this, I have identified a total of 9 legal jurisdictions that may serve as starting points for this future research. An even deeper analysis may also require understanding the severity of harm thresholds, particularly what constitutes as "severe" or "substantial" harm in the context of privacy violations. Finally, a subsequent study may need to be undertaken in order to understand and test the underlying reason/s why data controllers are given more leeway when it comes to when a breach notification to individuals should be sent out, as opposed to the more stringent temporal requirement of breach reporting to authorities.

[137] FTC, *New Data Shows*, *supra*, note, at 120.

Annex 1: Survey Questions

Questions	Reasons for Adding / Modifying
1. What is the relevant definition of personal data in the breach notification law? (new)	It is possible for a jurisdiction to adopt different definitions for the same legal term (*e.g.*, "personal information" or "personal data"). For example, California adopted a restrictive definition for "personal information" insofar as notifying consumers of data breaches is concerned, *i.e.*, the law lists the particular types of data that must be involved in the incident before the legal requirement to notify consumers arises. In contrast, California adopted an expansive definition of "personal information" insofar as consumer privacy and data protection is concerned. Since this research focuses on breach notification laws, the restrictive definition was examined. This question is meant to help answer research question 2. *Note: the terms "personal information," "personal data," and "personally identifiable information" have been considered interchangeable.*
2. Was the definition of personal data for the purpose of breach notification open-ended or closed-ended? (new)	The response for this would signal whether the jurisdiction has an open-ended (*i.e.*, subject to factual determination) or close-ended (*i.e.*, enumerated) definition of personal data. This is relevant to determine whether the breach disclosure obligation would be triggered. This question is meant to help answer research question 2.
3. Did the law distinguish the types of personal data subject to breach notification? (new)	The response for this would signal whether the jurisdiction identifies the types of data that must have been subject of a data breach before the legal obligation to notify arises. This question is meant to help answer research question 2.
4. Did the law require reporting to authorities in case of a personal data breach?	This question was adopted from Thomson Reuters's chart. This question is meant to help answer research question 1.
5. What are the events and factors that would trigger reporting to authorities? (new)	This aims to be an overarching question meant to discover all possible events and factors that would trigger reporting to governmental authorities. This question is meant to help answer research question 2.
6. Did the law provide a timeframe within which to report to authorities?	This question was adopted from Thomson Reuters's chart. It will give a sense of when disclosure must be performed and whether there is urgency to the disclosure. This question is meant to help answer research question 3.
7. Did the law require notification of data subjects in case of a personal data breach?	This question was adopted from Thomson Reuters's chart. This question is meant to help answer research question 1.
8. What are the events and factors that would trigger notification to data subjects? (new)	This aims to be an overarching question meant to discover all possible events and factors that would trigger notification to consumers. This question is meant to help answer research question 2.

9. Did the law clearly require the existence of the possibility of harm before notifying data subjects?	This question was adopted from Thomson Reuters's chart. This is relevant to determine whether the breach disclosure obligation would be triggered. This question is meant to help answer research question 2.
10. Did the law provide a timeframe within which to notify data subjects?	This question was adopted from Thomson Reuters's chart. It will give a sense of when disclosure must be performed and whether there is urgency to the disclosure. This question is meant to help answer research question 3.
11. Did the law require the inclusion of specific information when notifying data subjects? (new)	This question is meant to help answer research question 4.
12. Did the law require the entity to communicate that they are performing or offering remedial measures that may benefit Data Subjects?	This question is meant to help answer research question 4.

Table A-1.1: Survey questions used during systematic content analysis with reasons for the questions.

Annex 2: Codebook

Question	Standard Response	Description (if applicable)
1. What is the relevant definition of personal data in the breach notification law?	Text of the actual provision	did not adopt standard response
2. Was the definition of personal data for the purpose of breach notification open-ended or closed-ended?	open_ended	law classifies data as personal data if it satisfies a criteria / subject to factual determination
	closed_ended	law classifies data as personal data if it falls under one of the enumerated data types
	not_applicable	law either did not provide a definition for breach notification purposes, or has no breach notification rule
3. Did the law distinguish the types of personal data subject to breach notification?	distinguished	law expressly specifies the categories of personal data that must have been subject of a data breach before the legal obligation to notify arises (*i.e.*, internal, external, historical, financial, social, and tracking)
	not_distinguished	law does not specify the categories of personal data that must have been subject of a data breach before the legal obligation to notify arises (i.e., internal, external, historical, financial, social, and tracking)
	not_applicable	jurisdiction does not have a law, regulation, or express and clear legal provision on personal data breach notification
4. Did the law require reporting to authorities in case of a personal data breach?	general_law_required	jurisdiction has an overarching law that regulates breach notification consistently across all industries this response covers the obligation to consider reporting
	sectoral_law_required	jurisdiction has a breach notification law that is industry or sector-specific
	not_required	no legal requirement and/or data protection agency does not make any recommendations
	recommended	law does not provide for mandatory reporting, though the jurisdiction's data protection authority recommends it
5. What are the events and factors that would trigger reporting to authorities?	Text of the actual provision	did not adopt standard response

6. Did the law provide a timeframe to report to authorities in case of a personal data breach?	specific_time_yes	law mentions a specific timeframe or deadline to report the breach (*e.g.*, within 48 hours)
	general_ time_yes	either law mentions a general timeframe or deadline to report the breach (*e.g.*, "immediately"), or law does not provide a timeframe or deadline
	varied_ times_yes	industry or sector-specific breach notification law mentions different timeframes or deadlines
	none	there is no breach notification law
7. Did the law require notification of data subjects in case of a personal data breach?	general_law_required	jurisdiction has an overarching law that regulates breach notification consistently across all industries this response covers the obligation to consider reporting
	sectoral_law_required	jurisdiction has a breach notification law that is industry or sector-specific
	not_required	no legal requirement and/or data protection agency does not make any recommendations
	recommended	law does not provide for mandatory notification, though the jurisdiction's data protection authority recommends it
8. What are the events and factors that would trigger notification to data subjects?	Text of the actual provision	did not adopt standard response
9. Did the law clearly require the existence of the possibility of harm before notifying data subjects?	yes_with_severity_of_harm	law requires notification only if there is a possibility of harm to data subjects (*e.g.*, risk of harm, right infringed, *etc.*) **and** that the harm that might be caused can reach a certain degree of severity / seriousness (*e.g.*, minor harm, serious harm, critical harm, *etc.*)
	yes_absent_severity_ of_harm	law requires notification only if there is a possibility of harm to data subjects, **regardless** of the degree of severity / seriousness of the harm that might be caused
	no_harm_element	law does not require the possibility or existence of harm before notifying data subjects (*e.g.*, mere unlawful destruction, loss, alteration, unauthorized disclosure of or, access without any further reference to infringement, damage, or harm to individuals or their rights)
	no_breach_provision	no legal requirement and/or data protection agency does not make any recommendations
	recommended	law does not provide for mandatory notification, though the jurisdiction's data protection authority recommends it

10. Did the law provide a timeframe within which to notify data subjects?	specific_time_yes	law mentions a specific timeframe or deadline to report the breach (*e.g.*, within 48 hours)
	general_time_yes	either law mentions a general timeframe or deadline to report the breach (*e.g.*, "immediately"), or law does not provide a timeframe or deadline
	varied_times_yes	industry or sector-specific breach notification law mentions different timeframes or deadlines
	no	there is no breach notification law
11. Did the law require the inclusion of specific information when notifying data subjects?	general_law_yes	jurisdiction has an overarching law that regulates the contents of breach notification consistently across all industries this response covers the obligation to consider reporting
	sectoral_law_yes	jurisdiction has an industry or sector-specific breach notification law that regulates the contents of breach notification
	recommended	law does not provide for specific information to be included, though the jurisdiction's data protection authority recommends it
	no	no legal requirement and/or data protection agency does not make any recommendations
12. Did the law require the entity to perform or offer remedial measures that may benefit data subjects?	req_specific_mitigation_measures	law mandates offering or performance of specific mitigation measures
	req_general_mitigation_measures	law mandates offering or performance of general mitigation measures
	recommended_specific_mitigation_measures	law merely recommends offering or performance of specific mitigation measures
	recommended_general_mitigation_measures	law merely recommends offering or performance of general mitigation measures
	none	no legal requirement and/or data protection agency does not make any recommendations

Table A-2.1: Codebook containing description of standard responses.

Annex 3: Data

[Please proceed to the next page]

[Also available here]

No.	Area	Region	Legal_Jurisdiction	q1_personal_data_definition	q2_personal_data_definition_distinguished	q3_report_reqt	q4_report_time	q5_notify_reqt	q6_notify_harm_reqt	q7_notify_time	q8_notify_content	q9_breach_mitigation	report_notif_compare	breach_disclosure_policy
1	Asia	Asia_Southern	Afghanistan	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
2	Europe	Europe_Southern	Albania	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	recommended	recommended	recommended_time_yes	no	none	No	breach_reporting_only
3	Africa	Africa_Northern	Algeria	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	no	none	Yes	full_breach_disclosure
4	Europe	Europe_Southern	Andorra	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
5	Africa	Africa_Middle	Angola	open_ended_definition	not_distinguished	general_law_required	general_time_yes	not_required	no_breach_provision	no	no	none	No	breach_reporting_only
6	Americas	Americas_Caribbean	Antigua_and_Barbuda	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
7	Americas	America_Southern	Argentina	open_ended_definition	not_distinguished	recommended	no	not_required	no_breach_provision	no	sectoral_law_yes	req_general_mitigation_measures	Not_Applicable	no_breach_disclosure_policy
8	Asia	Asia_Western	Armenia	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	specific_time_yes	no	none	Yes	full_breach_disclosure
9	Americas	Americas_Caribbean	Aruba	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
10	Oceania	Oceania_Australia_and_New_Zealand	Australia	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_with_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
11	Europe	Europe_Western	Austria	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
12	Asia	Asia_Western	Azerbaijan	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
13	Americas	Americas_Caribbean	Bahamas	open_ended_definition	not_distinguished	recommended	no	recommended	recommended	no	recommended	recommended_general_mitigation_measures	Yes	breach_disclosure_nonmandatory
14	Asia	Asia_Western	Bahrain	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	no	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
15	Asia	Asia_Southern	Bangladesh	open_ended_definition	not_distinguished	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
16	Americas	Americas_Caribbean	Barbados	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
17	Europe	Europe_Eastern	Belarus	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	not_required	no_breach_provision	no	no	req_general_mitigation_measures	No	breach_reporting_only
18	Europe	Europe_Western	Belgium	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
19	Africa	Africa_Western	Benin	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
20	Americas	America_Northern	Bermuda	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	no	req_general_mitigation_measures	Yes	full_breach_disclosure
21	Americas	Americas_Caribbean	BES_Islands	open_ended_definition	not_distinguished	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
22	Asia	Asia_Southern	Bhutan	open_ended_definition	not_distinguished	sectoral_law_required	specific_time_yes	sectoral_law_required	no_harm_element	no	sectoral_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
23	Americas	America_Southern	Bolivia	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
24	Europe	Europe_Southern	Bosnia_Herzegovina	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
25	Africa	Africa_Southern	Botswana	open_ended_definition	not_distinguished	general_law_required	general_time_yes	not_required	no_breach_provision	no	no	none	No	breach_reporting_only
26	Americas	America_Southern	Brazil	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
27	Europe	Europe_Eastern	Bulgaria	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
28	Africa	Africa_Western	Burkina_Faso	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
29	Asia	Asia_Southeastern	Cambodia	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
30	Africa	Africa_Middle	Cameroon	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
31	Americas	America_Northern	Canada_Alberta	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_with_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
32	Americas	America_Northern	Canada_Federal	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_with_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
33	Africa	Africa_Western	Cape_Verde	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
34	Americas	Americas_Caribbean	Cayman_Islands	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
35	Africa	Africa_Middle	Chad	open_ended_definition	not_distinguished	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
36	Americas	America_Southern	Chile	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
37	Asia	Asia_Eastern	China	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
38	Americas	America_Southern	Colombia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	not_required	no_breach_provision	general_time_yes	general_law_yes	req_general_mitigation_measures	No	breach_reporting_only
39	Americas	America_Central	Costa_Rica	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
40	Africa	Africa_Western	Cote_d'_Ivoire	open_ended_definition	not_distinguished	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
41	Europe	Europe_Southern	Croatia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
42	Americas	Americas_Caribbean	Curaçao	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
43	Asia	Asia_Western	Cyprus	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
44	Europe	Europe_Eastern	Czech_Republic	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure

45	Africa	Africa_Middle	Democratic_Republic_of_Congo	open_ended_definition	not_distinguished	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
46	Europe	Europe_Northern	Denmark	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
47	Americas	Americas_Caribbean	Dominican_Republic	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
48	Asia	Asia_Southeastern	East_Timor	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
49	Americas	America_Southern	Ecuador	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	specific_time_yes	no	none	Yes	full_breach_disclosure
50	Africa	Africa_Northern	Egypt	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
51	Americas	America_Central	El_Salvador	open_ended_definition	not_distinguished	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
52	Europe	Europe_Northern	Estonia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
53	Africa	Africa_Southern	Eswatini	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
54	Africa	Africa_Eastern	Ethiopia	open_ended_definition	not_distinguished	sectoral_law_required	specific_time_yes	sectoral_law_required	no_harm_element	general_time_yes	sectoral_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
55	Europe	Europe_Northern	Faroe_Islands	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
56	Oceania	Oceania_Melanesia	Fiji	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
57	Europe	Europe_Northern	Finland	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
58	Europe	Europe_Western	France	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
59	Africa	Africa_Middle	Gabon	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
60	Africa	Africa_Western	Gambia	open_ended_definition	not_applicable	not_required	no	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	No	breach_notification_only
61	Asia	Asia_Western	Georgia	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
62	Europe	Europe_Western	Germany	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
63	Africa	Africa_Western	Ghana	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
64	Europe	Europe_Southern	Gibraltar	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
65	Europe	Europe_Southern	Greece	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
66	Americas	America_Northern	Greenland	open_ended_definition	not_distinguished	not_required	no	not_required	no_harm_element	no	no	none	Not_Applicable	no_breach_disclosure_policy
67	Americas	America_Central	Guatamela	open_ended_definition	not_applicable	general_law_required	general_time_yes	not_required	no_breach_provision	no	no	none	No	breach_reporting_only
68	Europe	Europe_Northern	Guernsey	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
69	Americas	America_Southern	Guyana	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
70	Americas	America_Central	Honduras	open_ended_definition	not_applicable	not_required	no	not_required	no_harm_element	no	no	none	Not_Applicable	no_breach_disclosure_policy
71	Asia	Asia_Eastern	Hong_Kong	open_ended_definition	not_distinguished	recommended	recommended_time_yes	recommended	yes_absent_severity_of_harm	recommended_time_yes	recommended	recommended_general_mitigation_measures	Yes	breach_disclosure_nonmandatory
72	Europe	Europe_Eastern	Hungary	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
73	Europe	Europe_Northern	Iceland	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
74	Asia	Asia_Southern	India	open_ended_definition	not_distinguished	general_law_required	general_time_yes	not_required	no_harm_element	no	no	none	No	breach_reporting_only
75	Asia	Asia_Southeastern	Indonesia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
76	Asia	Asia_Southern	Iran	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
77	Asia	Asia_Western	Iraq	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
78	Europe	Europe_Northern	Ireland	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
79	Europe	Europe_Northern	Isle_of_Man	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
80	Asia	Asia_Western	Israel	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	recommended	recommended_general_mitigation_measures	Yes	full_breach_disclosure
81	Europe	Europe_Southern	Italy	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
82	Americas	Americas_Caribbean	Jamaica	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
83	Asia	Asia_Eastern	Japan	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	no	req_general_mitigation_measures	Yes	full_breach_disclosure
84	Europe	Europe_Northern	Jersey	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
85	Asia	Asia_Central	Kazakhstan	open_ended_definition	not_distinguished	general_law_required	general_time_yes	not_required	no_breach_provision	no	no	none	No	breach_reporting_only
86	Africa	Africa_Eastern	Kenya	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
87	Europe	Europe_Southeast	Kosovo	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
88	Asia	Asia_Western	Kuwait	open_ended_definition	not_distinguished	sectoral_law_required	specific_time_yes	sectoral_law_required	no_harm_element	specific_time_yes	sectoral_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
89	Asia	Asia_Central	Kyrgzstan	open_ended_definition	not_applicable	not_required	no	general_law_required	no_harm_element	specific_time_yes	no	none	No	breach_notification_only

90	Europe	Europe_Northern	Latvia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
91	Asia	Asia_Western	Lebanon	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
92	Africa	Africa_Southern	Lesotho	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
93	Europe	Europe_Western	Liechtenstein	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
94	Europe	Europe_Northern	Lithuania	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
95	Europe	Europe_Western	Luxembourg	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
96	Asia	Asia_Eastern	Macau	open_ended_definition	not_distinguished	sectoral_law_required	varied_times_yes	not_required	no_breach_provision	no	no	none	No	breach_reporting_only
97	Africa	Africa_Eastern	Madagascar	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
98	Africa	Africa_Eastern	Malawi	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
99	Asia	Asia_Southeastern	Malaysia	open_ended_definition	distinguished	sectoral_law_required	varied_times_yes	sectoral_law_required	yes_absent_severity_of_harm	varied_times_yes	sectoral_law_yes	recommended_general_mitigation_measures	Yes	full_breach_disclosure
100	Asia	Asia_Southern	Maldives	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
101	Africa	Africa_Western	Mali	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
102	Europe	Europe_Southern	Malta	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
103	Africa	Africa_Western	Mauritania	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
104	Africa	Africa_Eastern	Mauritius	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
105	Americas	America_Central	Mexico	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_with_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
106	Europe	Europe_Western	Monaco	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	specific_time_yes	no	none	Yes	full_breach_disclosure
107	Asia	Asia_Eastern	Mongolia	open_ended_definition	not_distinguished	not_required	no	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	No	breach_notification_only
108	Europe	Europe_Southern	Montenegro	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
109	Africa	Africa_Northern	Morocco	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
110	Africa	Africa_Eastern	Mozambique	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
111	Asia	Asia_Southeastern	Myanmar	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
112	Asia	Asia_Southern	Nepal	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
113	Oceania	Oceania_Australia_and_New_Zealand	New_Zealand	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_with_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
114	Americas	America_Central	Nicaragua	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
115	Africa	Africa_Western	Niger	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
116	Africa	Africa_Western	Nigeria	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
117	Europe	Europe_Southern	North_Macedonia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
118	Europe	Europe_Northern	Norway	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
119	Asia	Asia_Western	Oman	open_ended_definition	not_distinguished	general_law_required	no	general_law_required	yes_absent_severity_of_harm	no	no	none	Yes	full_breach_disclosure
120	Asia	Asia_Southern	Pakistan	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
121	Americas	America_Central	Panama	open_ended_definition	not_applicable	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	general_law_yes	recommended_general_mitigation_measures	Yes	full_breach_disclosure
122	Americas	America_Southern	Paraguay	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
123	Americas	America_Southern	Peru	open_ended_definition	not_distinguished	not_required	no	recommended	recommended	general_time_yes	general_law_yes	req_general_mitigation_measures	Not_Applicable	no_breach_disclosure_policy
124	Asia	Asia_Southeastern	Philippines	open_ended_definition	distinguished	general_law_required	specific_time_yes	general_law_required	yes_with_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
125	Europe	Europe_Eastern	Poland	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
126	Europe	Europe_Southern	Portugal	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
127	Asia	Asia_Western	Qatar	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_with_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
128	Asia	Asia_Western	Qatar_Financial_Centre	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	no	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
129	Africa	Africa_Western	Republic_of_Guinea	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
130	Europe	Europe_Eastern	Republic_of_Moldova	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	not_required	no_harm_element	no	no	none	No	breach_reporting_only
131	Africa	Africa_Middle	Republic_of_the_Congo	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
132	Europe	Europe_Eastern	Romania	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
133	Europe	Europe_Eastern	Russian_Federation	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	not_required	no_breach_provision	no	no	req_general_mitigation_measures	No	breach_reporting_only
134	Americas	Americas_Caribbean	Saint_Lucia	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy

135	Americas	Americas_Caribbean	Saint_Vincent_and_the_Grenadines	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
136	Europe	Europe_Southern	San_Marino	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
137	Africa	Africa_Middle	Sao_Tome_and_Principe	open_ended_definition	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
138	Asia	Asia_Western	Saudi_Arabia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	not_required	no_breach_provision	no	no	none	No	breach_reporting_only
139	Africa	Africa_Western	Senegal	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
140	Europe	Europe_Southern	Serbia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
141	Africa	Africa_Eastern	Seychelles	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
142	Asia	Asia_Southeastern	Singapore	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_with_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
143	Europe	Europe_Eastern	Slovakia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
144	Europe	Europe_Southern	Slovenia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
145	Africa	Africa_Eastern	Somalia	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
146	Africa	Africa_Southern	South_Africa	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
147	Asia	Asia_Eastern	South_Korea	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
148	Europe	Europe_Southern	Spain	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
149	Asia	Asia_Southern	Sri_Lanka	not_applicable	not_applicable	general_law_required	no	general_law_required	no_harm_element	no	general_law_yes	none	Yes	full_breach_disclosure
150	Europe	Europe_Northern	Sweden	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
151	Europe	Europe_Western	Switzerland	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	varied_times_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
152	Asia	Asia_Eastern	Taiwan	open_ended_definition	not_distinguished	sectoral_law_required	varied_times_yes	general_law_required	no_harm_element	no	general_law_yes	req_general_mitigation_measures	No	breach_notification_only
153	Asia	Asia_Central	Tajikistan	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
154	Africa	Africa_Eastern	Tanzania	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
155	Asia	Asia_Southeastern	Thailand	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
156	Europe	Europe_Western	The_Netherlands	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
157	Africa	Africa_Western	Togo	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
158	Americas	Americas_Caribbean	Trinidad_and_Tobago	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
159	Africa	Africa_Northern	Tunisia	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
160	Asia	Asia_Western	Turkey	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
161	Asia	Asia_Central	Turkmenistan	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
162	Africa	Africa_Eastern	Uganda	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	no	none	Yes	full_breach_disclosure
163	Europe	Europe_Eastern	Ukraine	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
164	Asia	Asia_Western	United_Arab_Emirates	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
165	Asia	Asia_Western	United_Arab_Emirates_Abu_Dhabi_Global_Market_(ADGM)	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
166	Asia	Asia_Western	United_Arab_Emirates_Dubai_International_Finance_Centre_(DIFC)	open_ended_definition	not_distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
167	Europe	Europe_Northern	United_Kingdom	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
168	Americas	America_Northern	United_States_Alabama	closed_ended_definition	distinguished	general_law_required	specific_time_yes	general_law_required	yes_with_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
169	Americas	America_Northern	United_States_Alaska	closed_ended_definition	distinguished	general_law_required	general_time_yes	general_law_required	yes_absent_severity_of_harm	general_time_yes	no	none	Yes	full_breach_disclosure
170	Americas	America_Northern	United_States_California	closed_ended_definition	distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_specific_mitigation_measures	Yes	full_breach_disclosure
171	Americas	America_Northern	United_States_Colorado	closed_ended_definition	distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	general_law_yes	none	Yes	full_breach_disclosure
172	Americas	America_Northern	United_States_Connecticut	closed_ended_definition	distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	specific_time_yes	recommended	req_specific_mitigation_measures	Yes	full_breach_disclosure
173	Americas	America_Northern	United_States_District_of_Columbia	closed_ended_definition	distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_specific_mitigation_measures	Yes	full_breach_disclosure
174	Americas	America_Northern	United_States_Federal	closed_ended_definition	distinguished	sectoral_law_required	varied_times_yes	sectoral_law_required	yes_varied	varied_times_yes	sectoral_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
175	Oceania	Oceania_Micronesia	United_States_Guam	closed_ended_definition	distinguished	not_required	no	general_law_required	yes_absent_severity_of_harm	general_time_yes	no	none	No	breach_notification_only
176	Americas	America_Northern	United_States_Oregon	closed_ended_definition	distinguished	general_law_required	specific_time_yes	general_law_required	yes_absent_severity_of_harm	specific_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
177	Americas	Americas_Caribbean	United_States_Puerto_Rico	closed_ended_definition	distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	none	Yes	full_breach_disclosure
178	Americas	America_Northern	United_States_Utah	closed_ended_definition	distinguished	not_required	no	general_law_required	no_harm_element	general_time_yes	no	none	No	breach_notification_only
179	Americas	Americas_Caribbean	United_States_Virgin_Islands	closed_ended_definition	distinguished	not_required	no	general_law_required	no_harm_element	general_time_yes	no	none	No	breach_notification_only

180	Americas	America_Northern	United_States_Virginia	closed_ended_definition	distinguished	general_law_required	general_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
181	Americas	America_Southern	Uruguay	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	general_time_yes	general_law_yes	req_general_mitigation_measures	Yes	full_breach_disclosure
182	Asia	Asia_Central	Uzbekistan	open_ended_definition	not_distinguished	sectoral_law_required	general_time_yes	not_required	no_breach_provision	no	no	req_general_mitigation_measures	No	breach_reporting_only
183	Americas	America_Southern	Venezuela	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
184	Asia	Asia_Southeastern	Vietnam	not_applicable	not_applicable	general_law_required	specific_time_yes	not_required	no_harm_element	no	no	none	No	breach_reporting_only
185	Asia	Asia_Western	Yemen	not_applicable	not_applicable	not_required	no	not_required	no_breach_provision	no	no	none	Not_Applicable	no_breach_disclosure_policy
186	Africa	Africa_Eastern	Zambia	open_ended_definition	not_distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	general_time_yes	no	none	Yes	full_breach_disclosure
187	Africa	Africa_Eastern	Zimbabwe	closed_ended_definition	distinguished	general_law_required	specific_time_yes	general_law_required	no_harm_element	no	no	req_general_mitigation_measures	Yes	full_breach_disclosure