DIVIDING TO UNIFY THE INTERNET

Joseph A. Kroon[†]

I. INTRODUCTION

The internet began as a place for the world to connect. A place for information to flow freely. A place for people across the globe to communicate with each other within fractions of a second. The internet was to be "a world that is both everywhere and nowhere."[1] At least, that was what the early internet pioneers wanted it to be.

Today, the internet is separating into geopolitical spheres, mirroring the exact borders the internet pioneers wanted to dismantle.[2] The "Great Firewall of China" has confined Chinese residents into a China-specific internet sphere.[3] Russia requires all cloud and platform data to be stored within Russian borders.[4] India has enacted similar data localization laws.[5] This is the rise of "Internet Balkanization."

The European Union is the latest geopolitical sphere to erect an internet border. On July 16, 2020, the European Union Court of Justice (hereinafter "CJEU") decided *Data Protection Commissioner v. Facebook Ireland, Ltd* (hereinafter "*Schrems II*").[6] Maximillian Schrems, an Austrian privacy activist, brought the case.[7] Schrems requested to suspend data transfers from the European Union to the United States for two reasons. First, he argued that the EU–U.S. Privacy Shield, the EU–U.S. data transfer treaty, did not provide EU citizens with adequate protection mandated by the General Data Protection Regulation (hereinafter "GDPR") and the EU Charter.[8] Second, he argued that Standard

DOI: https://doi.org/10.15779/Z382J6854B

† J.D., University of California, Berkeley School of Law, 2022.

1. John Perry Barlow, *A Declaration of Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.
2. *Id.*
3. *The Great Firewall of China*, BLOOMBERG (Nov. 5, 2018), https://www.bloomberg.com/quicktake/great-firewall-of-china.
4. Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 712–15 (2015).
5. *Id.* at 694–97.
6. Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Ltd., 2020 E.C.R. (hereinafter *Schrems II*).
7. *Id.* ¶ 50.
8. *Id.* ¶ 55.

Contractual Clauses (SCCs), a contract mechanism which allows private entities to transfer data, were incompatible with the Charter.[9] The CJEU ultimately held that the EU–U.S. Privacy Shield was invalid. It also held that the SCCs were still acceptable but reaffirmed their limitations.[10] Therefore, the CJEU *Schrems II* decision limits how data is transferred between the European Union and other countries. Another digital legal border was erected.

This Note argues that *Schrems II* paradoxically promotes Internet Balkanization by maintaining both data users' privacy interests and the open internet ideals. The CJEU rectified high privacy expectations, erected a digital legal border, and fragmented the internet. However, *Schrems II* erects this border by establishing an idea this Note calls "digital autonomy":[11] users' ability to use the open internet free from adverse foreign entities' processing. By establishing digital autonomy, the EU maintained the open internet.

To illustrate, this Note explores the implications of *Schrems II* in a global, digital world. Part II elaborates on the general privacy interest in an increasing global and digital world. It begins with an overview of information privacy, specifically how privacy relates to individual autonomy and how privacy interests have changed in a digital environment. Then it explains what Internet Balkanization is and how it is rising today. Part III of this Note gives an overview of *Schrems II*. It begins with the Snowden revelations and the aftermath of countries adopting more privacy and data localization policies, and then it elaborates on the pertinent GDPR provisions and the *Schrems II* decision. Finally, Part IV argues that *Schrems II* maintains a core open internet ideal—autonomy of individual data users—by promoting Internet Balkanization.

II. PRIVACY INTEREST IN A GLOBAL, DIGITALIZED WORLD

Today, information is one the most valuable pieces of capital,[12] but according to Maximillian Schrems, information is "none of a company's business";[13] and these two forces conflicted with each other in a recent,

9. *Id.*

10. *Id.* ¶ 105.

11. *See infra* pp. 53–55.

12. *The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

13. *See FAQs*, NOYB, https://noyb.eu/en/faqs (referencing how NOYB, Maximillian Schrem's privacy advocacy group, believes that data user's privacy is "none of a company's business").

dominating CJEU case. But what is "information privacy," the central concern Schrems fought for? And what value does information have?

The first Section of this Part reviews information privacy. It discusses what information privacy initially concerned, how it relates to autonomy, and how it is becoming more pertinent due to the greater accessibility of personal information. The second Section examines an open internet—what it is and its societal benefits—and then discusses the open internet's adversary: Internet Balkanization, its rise, and its pros and cons.

A. INFORMATION PRIVACY AND AUTONOMY IN THE DIGITAL AGE

Privacy is the "claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[14] There are different categories of information privacy concerns. Legal scholars have categorized privacy as decisional privacy,[15] physical privacy, proprietary privacy, and information privacy. *Schrems II* and this Note primarily concern information privacy.

This Section discusses information privacy, autonomy, and the relationship between the two. First, this Section summarizes what information privacy is and how the digital era has made information privacy an ever-increasing issue. Then, this Section discusses what autonomy is, how autonomy is a product of information privacy, and how data users' digital experience impacts their autonomy.

1. An Overview of Information Privacy and the Digital Era's Impact on Information Privacy

Information privacy is the right "to control the flow of our personal information."[16] It includes having control over the information that makes up who we are and how society views us.[17] This encompasses information that define individuals objectively (e.g., name, address, age) and information that define individuals subjectively (e.g., political views, sexual preferences, spiritual perspectives).[18]

Society benefits when individuals have control over their information. For instance, privacy promotes different democratic values like freedom of economic choice and freedom of political participation. Privacy allows

14. ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

15. Decisional privacy is the individual's right to make choices about their body and their family.

16. Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J. L. & TECH. 106, 118 (2019).

17. *See id.*

18. *See id.*

individuals to buy what they want or vote for who they want without fear that their choices will be broadcasted publicly, resulting in scrutiny. Also, privacy is fundamental to individual autonomy.[19]

However, information privacy is not a right to control all information at all times. For instance, users cannot assert a privacy right if the information has already been disclosed or if the public has a strong interest in the information.

First, information privacy is limited by whether the information has already been disclosed. Privacy law protects individual's direct control over their information, but it does not limit anyone else from sharing the individual's information unless there is a legal obligation prohibiting disclosure.[20] Individuals no longer have complete control over information after it has been disclosed to someone. Thus, privacy is a limited right, narrowed by who lawfully has access to information.

Second, information privacy is limited by public interests. Legislation should make limitations in order to "meet objectives of [the public's] general interests."[21] Recognized interests include counterintelligence, public security, and contractual performance.[22] These are exceptions legislation decided are more important an individual's privacy.[23] Therefore, people should not have monopoles over their data; their data submits to greater public interests.

In sum, information privacy is control over one's information, but that control only extends as far as one shares their data and what other interests the public is concerned with.

---

19. *See generally* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) ("Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference--a field of operation within which to engage in the conscious construction of self.").

20. *See* Nader v. Gen. Motors Corp., 25 N.Y.2d 560, 569 (1970) (recognizing that interviewing third parties could hardly be an invasion of plaintiff's privacy). Some statutes prohibit third parties from sharing information that individuals have disclosed to them. This includes the GDPR.

21. Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Ltd., 2020 E.C.R. ¶ 174.

22. *See* Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 49, 2016 O.J. (L 119) 1 [hereinafter GDPR] (enumerating some exceptions where data transfers can occur without an adequacy agreement nor Safeguard Agreement).

23. *See id.*

However, the right to privacy was theorized pre-cell phones, pre-social media, pre-globalization,[24] and time has exacerbated information privacy concerns in two ways. An unprecedented amount of data is being collected, and that data discloses more intimate details than ever before.

Today, more data than ever is being collected. At its inception, information privacy concerned the details one normally disclosed while in the confines of their home: information individuals usually shared with their "inner circle," close family and friends.[25] In the digital era, parties in the "inner circle" are now applications we use, websites we visit, or surveillance camera on the streets we walk.[26] For example, a data user's private social media posts are still legally accessible by going through an entity the data user has previously authorized access to. The internet has given companies so much information that they now have a "God's eye" of the market.[27] Facebook knows what people like; Apple knows what apps people download; Amazon knows what people buy. This knowledge gives companies insight into the entire society.

Additionally, data users now disclose more intimate details than before. By using cultivated data, artificial intelligence (AI) can find surprising patterns in data sets that were impossible to discover with previous technology.[28] For example, one study used telephone metadata (e.g., the numbers dialed and length of calls) to infer that a person had cardiac arrhythmia.[29] Indeed, the U.S. Supreme Court has recognized this concern in the context of GPS location.[30] For example, developers used Instagram feeds to create an AI that predicts

24. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

25. *Id.* at 195.

26. *Facial Recognition Technology*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.

27. *See* THE ECONOMIST, *supra* note 12.

28. There is an argument to be had about whether AI conflicts with information privacy because AI can be created with anonymous data. There are two main reasons why anonymized data is not a simple fix for AI. First, some data independently identifies data users (e.g., name, address, phone number, etc.) Because this data is independently identifiable, they are prohibited from AI developers wanting to use the anonymized data exception. Second, a combination of different unidentifiable data together can identify a data user. Although information may originally be anonymized, it can eventually be de-anonymized. For more of this discussion, see Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

29. Bjorn Carey, *Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information*, PHYS ORG (May 17, 2016), https://phys.org/news/2016-05-scientists-metadata-reveal-surprisingly-sensitive.html.

30. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

data users' depression levels.[31] In another example, AI used facial recognition to predict someone's sexual orientation.[32] This is information data users may have disclosed in intimate settings but now unknowingly disclose to the internet.

Information privacy originally concerned the right to control our data. But data, today, is colossal.

2. *An Overview of Autonomy and How Data Users Have Autonomy in a Digital Environment*

Abstractly, autonomy is the freedom to make one's own decisions, detached from adverse influences. Although individual autonomy is not a modern phenomenon, the digital landscape has altered how autonomy can be impacted. Autonomy is an individual's capacity to make their own decisions, but in the digital landscape, more and more adverse influences impact an individual's autonomy. But maintaining information privacy protects autonomy.

Autonomy is a person's capacity to make their own decisions.[33] It is to be free from external influences that manipulate one's thought process: free form adverse political influences, free form social influences, and free to "engage in the conscious construction of self."[34] The idea that people are free to be oneself, to be autonomous, is a fundamental belief in democratic societies.[35] Autonomy promotes a "vital diversity" of ideas that establish the foundation for democratic debates.[36] However, realistically being completely free from adverse influences is unachievable; it is an aspirational goal.

In the digital landscape, independence from adverse digital influences (i.e., a digital third party) provides users an environment to become autonomous. These adverse digital influences could be other data users (e.g., other data users people communicate with), websites data users visit (e.g., manipulating the data user's experience), or possible surveillance (e.g., the mere knowledge of an adverse user's presence could manipulate a data user's experience). The purest

31. Andrew G. Reece & Christopher M. Danforth, *Instagram Photos Reveal Predictive Markers of Depression*, 6 EPJ DATA SCI. 15, 15–16 (2017).

32. Yilun Wang, Michal Kosinski, *Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images.*, 114 J. PERSONALITY & SOC. PSYCHOL. 246 (2018) (using users' dating app profiles to create an AI system that predicts peoples' sexual orientation).

33. Cohen, *supra* note 19, at 1424 (establishing that autonomy is "how we develop the capacity and facility for choice").

34. *Id.* at 1424.

35. *Id.* at 1426.

36. *Id.* at 1425.

illustration depicting full data user autonomy would be a person surfing through the internet with no surveillance, no tracking, and no incitements manipulating the user's next step. In theory, the data user would visit any website whenever they wanted or do anything they want, without disclosing a hint of their identity. That is not reality, and for good reasons too.[37] But as an illustration, that is closest experience to complete digital autonomy.

Once adverse parties get involved, autonomy erodes. Attaching one's identity in a chat room may incentive them to post less-controversial comments; a search engine operator feeding curated articles may direct the data user to visit different pages than they originally intended.[38] This is the more realistic digital experience. The more third parties manipulate a data user's digital experience, the more a data user risks losing autonomy.[39] A one-off third party may influence a data user to visit an online retail store before they proceed with their intended business. But as more parties become involved, more of the data user's actions become susceptible to the third party's whims.[40] Arguably, the data user chose to visit a different website (a click-bait article perhaps) due to their own interests therefore never losing their autonomy. However, that mistakes the user's independent reaction—independently clicking the click-bait article link—as autonomy. This is an incorrect conclusion because a data user's autonomy comes from their original intentions, what they originally wanted to do. Although the data user may have originally wanted to research the article's topic, they may not have originally gone to that specific click-bait article. The more adverse influences there are, the more a data user's original intentions are manipulated, inevitably losing a portion of their digital autonomy.

To achieve autonomy, digital or otherwise, information privacy is necessary. Arguably, to be truly autonomous, people need to be relatively insulated from external influences, influences that would manipulate a "conscious construction of self."[41] Privacy nurtures this insulated environment and prevents "pervasive monitoring" that would push individuals "toward the bland and the mainstream," stifling individualism.[42] In a democratic society,

37. There are some instances we would want digital monitoring. For example, sometimes we want websites to guide our experience, resulting in a more efficient experience. But also, we want some monitoring to track egregious actions like in sex trafficking or child pornography.

38. *See* Jessica van der Schalk, *The Quest for Autonomy in the Digital Age*, FREEDOM LAB (Aug. 5, 2019), https://freedomlab.org/the-quest-for-autonomy-in-the-digital-age/.

39. *See* Cohen, *supra* note 19, at 1424.

40. *See id.*

41. *Id.*

42. *Id.* at 1426.

individualism is valued because it propagates fundamental democratic values like diverse ideas, diverse voices. Therefore, information privacy is "a constitutive element of a civil society."[43]

B. AN OVERVIEW OF THE OPEN INTERNET, AND ITS ADVERSARY: INTERNET BALKANIZATION

Privacy is not an absolute right.[44] In some instances, access to information counteracts data users' privacy interests. For one, the "[f]lows of personal data . . . [is] necessary for the expansion of international trade and international cooperation," the benefits of an open internet.[45]

This Section begins by summarizing what an "open internet" is and an open internet's economic and social benefits. Then, this Section discusses the rise of an open internet's adversary: Internet Balkanization, what it is, what causes it, and what its debatable pros and cons are.

1. An Overview of the Open Internet

As a preliminary question, what is an open internet? At the beginning of the internet, early pioneers believed the internet to be a place "naturally independent of the tyrannies [governments] seek to impose."[46] That is, governments have no place to confine internet users. This, ideally, would create a "world where anyone, anywhere may express [their] beliefs, no matter how singular, without fear of being coerced into silence or conformity."[47] An open internet is an open frontier of information, free form sovereign confines.

By enabling people to be connected, an open internet generates economic and social benefits.[48] From an economic viewpoint, an open internet minimizes production costs for companies.[49] It also facilitates more international trade, with both business partners and customers.[50] Also, an open

43. *Id.* at 1427.

44. *See* Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Ltd., 2020 E.C.R.. ¶ 172.

45. GDPR, *supra* note 22, recital 101.

46. Barlow, *supra* note 1.

47. *Id.*

48. GDPR, *supra* note 22, recital 6 ("Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.").

49. *See* Dillon Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE (May 22, 2017), https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization (discussing how data localization is expensive work).

50. OECD DIGITAL ECONOMY POLICY PAPER, ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS, at 18 (2016) [hereinafter ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS].

internet stimulates innovation.[51] Much of the digital revolution was enabled by resources being easily communicated via the internet.[52] On the other hand, arguments are being made that an open internet may not be as good for economic growth as some may believe.[53] This is an important debate to be had, but not the focus of this Note.

Also, an open internet has social benefits. With an open internet, people have a forum to communicate with other people regardless of their geographic location. Open communication enables people to connect with close ones, access education, or connect with social services like medical professionals. An open internet "facilitates the exchange of knowledge, ideas, interests, and viewpoints" from news media sources across the globe.[54] Internet users can also express their beliefs to a wider audience. Open internet's accessibility enabled journalists to investigate and widely report about the Uighur "re-education" camps[55] or about the Rohingya genocide.[56] An open internet enables one's voice to be heard, regardless of where they are in the world.

However, data users cannot rely on an open internet. states regularly adopt measures that fragment it. By fragmenting the open internet, data users lose the early cyber pioneers' dream for the internet. Scholars have called this fragmenting phenomenon "Internet Balkanization."

2. The Rise of Internet Balkanization

Opposing the open internet is Internet Balkanization. Internet Balkanization refers to the global internet fragmenting into different geopolitical borders, preventing internet users from accessing each other due to technical, legal, or physical barriers.[57] The internet originated as a universal internet, one spanning across all nations without borders. However, over the

51. *Id.*

52. Flaviu Mircea, *Impacts of the Digital Revolution*, MEDIUM (Nov. 26, 2018), https://medium.com/@flaviu.mirc/impacts-of-the-digital-revolution-e561e1cbc8bd ("Another important aspect of the Digital Revolution is the constant development of the communication technology, the main components being the widespread use of Internet and mobile phones, as well as other mobile communication devices.").

53. Jennifer Daskal, Paul Ohm & Pierre de Vries, *Debate: We Need to Protect Strong National Borders on the Internet*, 17 COLO. TECH. L.J. 13, 26 (2018); *see also* ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS, *supra* note 50, at 22.

54. ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS, *supra* note 50, at 23.

55. *Data Leak Reveals How China 'Brainwashes' Uighurs in Prison Camps*, BBC (Nov. 24, 2019), https://www.bbc.com/news/world-asia-china-50511063.

56. *Myanmar's Genocide Against Rohingya Not over, Says Rights Group*, THE GUARDIAN (Nov. 23, 2020), https://www.theguardian.com/world/2020/nov/23/myanmar-is-still-committing-genocide-against-rohingya-says-rights-group.

57. Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 373–74 (2008).

past decade states have started adopting more legal barriers, creating "internet borders."[58] Thus, the open internet is fragmenting into geopolitical internet spheres.[59]

These internet borders, unlike geographic borders, are not defined by one line. They change based on the type of data and what entities can do with the data. For example, some states prohibit a certain type of data from crossing its internet border, but more pervious for other types of data.[60] Or on the other hand, some states' internet borders are due to the lack of internet cables, a mechanical border.[61] These are all ways nations created internet borders, fragmenting the global internet.

Originally, more authoritarian states had internet barriers, but today more democratic states are also adopting internet borders. China has the "Great Chinese Firewall,"[62] which uses filters to block certain IP addresses, keywords, internet addresses, and so on.[63] As another example, Iran wants to make its own internet: an "isolated domestic intranet that can be used to promote Islamic content."[64] In recent years, however, imposing internet borders has spread beyond authoritarian states. Post-Snowden, more democratic states have also adopted internet barriers.[65] Germany proposed to build an EU internet network, intending to keep data user information within the EU.[66] Australia adopted the Personally Controlled Electronic Health Records Act, which prohibits health data from leaving Australia's internet borders.[67] These states' willingness to adopt internet borders, and the active steps they've taken to do so, makes Internet Balkanization an inevitability.

Although Internet Balkanization is the open internet's adversary, Internet Balkanization does not necessarily counteract the open internet's benefits. It is

58. Sally Adee, *The Global Internet Is Disintegrating. What Comes Next?*, BBC (May 14, 2019), https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next (discussing how North Korea is secluded because it lacks internet cables connecting it to the rest of the world).

59. This Note uses the term "internet spheres" to describe the different geopolitical fragments the global internet is separating into.

60. *See* Chadner & Lê, *supra* note 4, at 683. Australia has the Personally Controlled Electronic Health Records (PCEHR) Act which prohibits the transfer of healthcare data outside of Australia, with some exceptions.

61. Adee, *supra* note 58.

62. *Id.*

63. *Id.*

64. Matt Vasilogambros, *Iran's Own Internet*, THE ATLANTIC (Aug. 29, 2016), https://www.theatlantic.com/news/archive/2016/08/irans-own-internet/497894/; *Iran Rolls out Domestic Internet*, BBC (Aug. 29, 2016), https://www.bbc.com/news/technology-37212456.

65. For a more extensive discussion about the rise of data localization, see *infra* p. 15.

66. Chander & Lê, *supra* note 4, at 694.

67. *Id.* at 683.

important to understand Internet Balkanization's pros and cons before resolving its potential adverse effects.

3. The Pros and Cons of Internet Balkanization

Recognizing that Internet Balkanization is happening, the pros and cons should be assessed. This Section begins by discussing Internet Balkanization's three main benefits: it rebalances internet control, adds beneficial friction to innovation, and possibly supports economic development by providing space for smaller companies. This Section also discusses Internet Balkanization's two main detriments: the downsides of centralizing data and possibly deterring economic development.

First, one possible benefit is that Internet Balkanization rebalances governmental control over local communication, speech, and commerce. Internet Balkanization creates internet "borders," like geographic borders. Parallel to how a state controls what goes through geographic borders, Internet Balkanization shifts more power to states.[68] This shift gives states more control over what goes in and out of states' internet, which can be beneficial. For example, in the Cambridge Analytical scandal,[69] the American government could have had more control over how Cambridge Analytica used American data for campaign ads. However, countries can use internet borders problematically, like geographic borders. These issues will be discussed later in this Section.[70] Overall, creating these internet borders gives countries the opportunity to properly protect data users' internet experience.

Second, another possible benefit is that Internet Balkanization adds friction to innovation so that engineers can incorporate human values into the systems.[71] Without any friction, the internet is uncontrolled, a digital Wild West. This makes the internet extremely efficient, but it also makes the internet susceptible to malicious manipulation or adverse consequences. For example, adding friction—coined as "desirable inefficiency"—creates a space for corrective human intervention. There is time to assess the technology before

68. *See* Daskal et al., *supra* note 53, at 21; *see also* David R. Johnson & David Post, *Law and Borders - the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996) ("The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules.").

69. Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

70. *Infra* p. 20.

71. Note that this can also be a con because it would disrupt innovation, which harms everyone. This point will be discussed below.

engineers implement it. This is a "design strategy for building systems that are fairer and more trustworthy."[72]

The third possible benefit is that Internet Balkanization supports economic development by providing a space for fair competition. Internet Balkanization uncontestably increases the barriers to entry for companies.[73] Countries set requirements about how the tech companies can use the internet. For instance, South Korea has a law that makes it difficult to build location services on foreign APIs (application programming interfaces).[74] Australia prohibits transferring any personally identifiable health data outside of Australia.[75] Thus companies need to build data centers within Australia or outsource to local services.[76] All of this results in companies allocating resources to comply with the requirements.

Restrictions also make it more difficult for companies to utilize the internet by creating legislative hurdles, thus making it harder for mid-size and smaller companies to enter markers. Arguably, only the Tech Titans (e.g., Amazon, Google, Facebook) have the resources to comply with different requirements across borders.[77] However, even the largest companies do not have enough resources to comply with every country's restriction.[78] Companies must choose which markets to enter and which ones to leave alone. In the left-alone markets, smaller, competitive companies can grow, ideally to a size that would compete with the large tech companies. Therefore, Internet Balkanization potentially promotes economic development by leaving a space for smaller companies to grow to a competitive size.

There are two main cons to Internet Balkanization: (1) the cautions of centralizing data and (2) the economic concerns.

First, centralizing data within geopolitical spheres risks violating human rights. Internet Balkanization makes it hard for outside parties to access information by adding more barriers to the data and by centralizing the data.[79] Information is opaque, and this opaqueness risks violating human rights. Countries can more easily censor information, stifling dissenting speech.[80] In

72. Paul Ohm & Jonathan Frankle, *Desirable Inefficiencies*, 70 FLA. L.R. 777, 785 (2018).
73. *See* Daskal et al., *supra* note 53, at 22, 26.
74. Chander & Lê, *supra* note 4, at 704.
75. *Id.* at 683.
76. *Id.*
77. *See* Daskal et al., *supra* note 53, at 26.
78. *Id.* at 22.
79. ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS, *supra* note 50, at 23.
80. *See* Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES (Nov. 28, 2008), https://www.nytimes.com/2008/11/30/magazine/30google-t.html; Clifford J. Levy, *Russia Uses*

2022, Russia suppressed online dissenters of the Ukrainian invasion.[81] Saudi Arabia has imprisoned several journalist who "stray away from the pro-government narrative."[82] The Electronic Frontier Foundation, ACLU, and public interest organizations have expressed that Internet Balkanization "undermines [the] rights [to Freedom of Expression and association] and threatens the potential of the Internet as a powerful tool for advancing human rights and democracy."[83]

Second, Internet Balkanization arguably deters economic development by increasing barriers to entry. Although it may promote economic development because it leaves a space for small to mid-size companies to grow.[84] The flip side argues that Internet Balkanization stifles tech developments by ossifying large tech companies. Arguably, only the Tech Titans (e.g., Amazon, Google, Facebook) have the resources to comply with different border requirements.[85] Therefore, they are the only ones with the resources to span across multiple internet spheres. Only large tech companies can penetrate the large markets because of the barriers to entry.[86] The result is that Internet Balkanization ossifies large tech companies' power in major markets, chilling the market.

Because of the inevitable development of Internet Balkanization, states should guide Internet Balkanization in a way that protects the original open internet benefits while maintaining data users' information privacy rights, particularly if countries want to continue benefiting from the global, open internet. And one way to maintain the ideals of the open internet is to provide individuals more autonomy over their data. *Schrems II* accomplishes this.

Microsoft to Suppress Dissent, N.Y. TIMES (Sept. 11, 2010), http://www.nytimes.com/2010/09/12/world/europe/12raids.html.

81. Robert McMahon, *Russia Is Censoring News on the Ware in Ukraine. Foreign Media Are Trying to Get Around That*, COUNCIL ON FOREIGN RELS. (Mar. 18, 2020), https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around.

82. *Ten Most Censored Countries*, COMM. TO PROTECT JOURNALISTS (Sept. 10, 2019), https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/.

83. Letter from ACLU et al., to Senator and Chairman Patrick J. Leahy and Senator and Ranking Member Jeff Sessions (Oct. 26, 2010).

84. *See* Daskal et al., *supra* note 53, at 22.

85. *See id.* at 26.

86. *See id.*

III. *SCHREMS II* OVERVIEW

On July 16, 2020, the CJEU decided *Schrems II*. However, like all cases, that decision did not occur in a vacuum. The environment was one of increasing globalization and increasing privacy concerns.[87]

This Section begins by illustrating *Schrems II*'s landscape. This includes a discussion about the Snowden revelations and the GDPR. Then, this Section discusses the two Safeguard Agreements at issue in *Schrems II*: the EU–U.S. Privacy Shield, and the Standard Contractual Clauses (SCCs). Finally, this Section explains the *Schrems II* decision.

A. SNOWDEN, THE GDPR, AND THE DEVELOPMENT BEFORE *SCHREMS II*

Schrems II's journey to the CJEU began at least seven years prior, starting with an American: Edward Snowden. This Section begins by summarizing the Snowden revelations and Snowden's impact on privacy laws. Then, this Section further explores those privacy laws, specifically data localization laws and the GDPR.

In June 2013, Edward Snowden, a former U.S. National Security Agency (NSA) agent leaked classified materials that revealed NSA wiretapping and data collection activities.[88] The materials revealed how the United States covertly wiretapped prominent international leaders, including Brazil's former president Dilma Rouseff and Germany's Chancellor Angela Merkel.[89] Snowden's revelation incited uproar, with some calling him a "hero" and others calling him a "grandiose narcissist."[90] The revelations, more importantly, impacted international privacy laws.

Following Snowden's revelations, governments began reevaluating their privacy laws. One type of law governments began implementing was "data localization" laws.[91] Data localization is a process where governments "limit the storage, movement, and/or processing of digital data to specific

87. Chander & Lê, *supra* note 4, at 679.

88. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY 455 (Rachel E. Barkow et al. eds., 6th ed. 2018).

89. *Id.*; Brian Winter, *Brazil's Rousseff Wants U.S. Apology for NSA Spying*, REUTERS (Sept. 4, 2013), https://www.reuters.com/article/us-usa-security-snowden-brazil/exclusive-brazils-rousseff-wants-u-s-apology-for-nsa-spying-idUSBRE98314N20130904.

90. SOLOVE & SCHWARTZ, *supra* note 88, at 477.

91. *See generally* Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policy Makers and Business Leaders*, LAWFARE RES. PAP. SER. (2014) (analyzing the rise of data localization laws post-Snowden); *see also* Chander & Lê, *supra* note 4, at 694 ("In February 2014, Chancellor Angela Merkel proposed that Europe build out its own internet infrastructure designed to keep data within Europe.").

geographies, jurisdictions, and companies."[92] Although data localization has been around since the 1990s, primarily in more authoritarian states, since then more democratic countries have also introduced data localization laws.[93] Most notoriously, Russia began implementing a plan, requiring all of Russia's information to be stored on servers physically located in Russia.[94] This secludes any Russian information within its borders. However, following Snowden, more democratic countries also began adopting data localization laws, including Australia, Canada, and others.[95] Australia requires all health data to confined within Australia.[96] Canadian provinces require public institutions to store data user's personal information within Canada.[97] In sum, data localization has become a common practice.

In addition to data localization, governments reevaluated their general privacy laws, particularly the European Union. The European Union reevaluated their Proposed Data Protection Regulation and their Safe Harbor Agreement with the United States.[98] In 2018, the European Union passed the GDPR, the state's primary privacy legislation. The GDPR regulates how entities collect, transfer, process, and disclose data subjects'[99] personal data,[100] and it has become the standard privacy law for EU citizens.

In particular, the GDPR's Articles 44, 45, and 46 were pertinent to *Schrems II*. Article 44 sets the foundation for international data transfers.[101] If a company plans to transfer EU data internationally, they need to ensure EU data users have the same level of protection provided by the GDPR.[102]

Article 45 elaborates when a party can transfer data under an EU Commission Adequacy Decision, such as data transfer treaties. The European

92. Hill, *supra* note 91, at 1.

93. STEPHEN J. EZELL, ROBERT D. ATKINSON & MICHELLE A. WEIN, LOCALIZATION AS BARRIERS TO TRADE: THREAT TO THE GLOBAL INNOVATION ECONOMY 20 (2013).

94. Adee, *supra* note 58.

95. Hill, *supra* note 91, at 4 n.3.

96. Chander & Lê, *supra* note 4, at 683.

97. *See id.* at 685 ("British Columbia and Nova Scotia have enacted laws requiring that personal information held by public institutions--schools, universities, hospitals, government-owned utilities, and public agencies--be stored and accessed only in Canada unless one of a few limited exceptions applies.").

98. SOLOVE & SCHWARTZ, *supra* note 88.

99. "Data subjects" is defined as the person(s) whose data is collected and processed. GDPR, *supra* note 22, art. 4.

100. *Id.* arts. 2, 4.

101. *Id.* art. 44.

102. GDPR art. 44 specifies that "[a]ny transfer of personal data . . . to a third country . . . shall take place only if . . . conditions . . . are compiled with by controller . . . including for onward transfers." Further, Article 44 mandates that all provisions shall be applied the same level of protection to EU citizens so that "this Regulation is not undermined."

Union Commission, the EU's executive branch, can evaluate a third-party country's data protection standards. If the third-party's country "ensures an adequate level of protection," then the third party does not need a special authorization before they transfer data to an entity in that third-party country.[103]

Article 45(2) elaborates on elements the Commission should consider when determine a country's data protection standards. These elements include "respect for human rights and fundamental freedoms . . . national security and criminal law and access of the public authorities to personal data," and additional elements.[104] After assessing the country's level of protection, the Commission can implement an act ensuring "an adequate level of protection."[105] Implementation allows parties to transfer data to that country without needing specific authorization.

Article 46 provides other viable agreements that would enable transnational data transfers absent an Article 45 Adequacy Agreement.[106] A controller can transfer data internationally "only if the controller or processor has provided appropriate safeguards."[107] Some do not require authorization. These include "a legally binding and enforceable instrument between public authorities," "binding corporate rules," and others.[108] Some safeguards do require authorization before data is transferred. These include "contractual clauses."[109] If a company, in a country not recognized under Article 44, wants to transfer EU data internationally, an Article 46 agreement (hereinafter "Safeguard Agreement") is the next viable option.

The GDPR also contains recitals, providing additional context to the GDPR Articles. They recognize the balance between technology's need for data and the importance of protecting personal data.[110] That is, for instance, it

103. *Id.* art. 45(1).

104. *Id.* art. 45(2).

105. *Id.* art. 45(3).

106. "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." *Id.* art. 46(1).

107. A "controller" is defined as any entity that "determines the purposes and means of the processing of personal data." A "processor" is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.* art. 4.

108. *Id.* art. 46(2).

109. *Id.* art. 46(3).

110. GDPR, *supra* note 22, recital 6 ("[S]haring of personal data has increased significantly . . . and should further facilitate the free flow of personal data within the Union

acknowledges the importance of international collaboration in data transfers but also guards against "undermin[ing]" the "level of protection of natural persons in the [European] Union."[111] Additionally, the recitals recommend what factors the Commission should take into account when assessing transnational data transfers.[112] If foreign government's privacy laws do not protect EU consumer data adequately, then foreign data controllers "should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject."[113] Controllers should fill the gap in the absence of an EU Adequacy Decision. In addition to the Articles, the recitals illustrate the GDPR's expectations.

Following the Snowden revelations, governments recalibrated their privacy policies, whether that meant enacting data localization laws or adopting standardized privacy policies. Although the Snowden revelations occurred almost a decade ago, governments are still grappling with its implications, leading to *Schrems II*.

B. THE EU–U.S. PRIVACY SHIELD & SCCS, THE TWO SAFEGUARD PROVISIONS THE CJEU REVIEWED IN *SCHREMS II*

Under the GDPR, non-EU entities (also called third-country entities) can transfer EU data user information under an Article 45 Adequacy Decision or an Article 46 Safeguard Agreement. In *Schrems II*, the EU–U.S. Privacy Shield Adequacy Decision was the Article 45 Adequacy Decision at issue, and Standard Contractual Clauses were the Article 46 Safeguard Agreements at issue.[114] Before reviewing *Schrems II*, this Section provides background regarding both the EU–U.S. Privacy Shield and SCCs.

After collaborating with U.S. authority, the EU Commission adopted the EU–U.S. Privacy Shield to transfer data between the two unions. The Privacy Shield contained new protocols in addition to existing ones, but the EU Commission was particularly concerned with three of them.[115] First was the Ombudsperson Clause. Second was the U.S. Executive Branch's foreign surveillance authority. Finally, the EU Commission reviewed the Foreign

and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data.").

111. GDPR, *supra* note 22, recital 101.

112. GDPR, *supra* note 22, recital 104 specifies that when judging data transfers to foreign countries, the GDPR recommended that "the Commission should . . . take into account how a particular third country respects the rule of law . . . including legislation concerning public security."

113. GDPR, *supra* note 22, recital 108.

114. *Schrems II*, ¶ 1.

115. Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Ltd., 2020 E.C.R., ¶ 42.

Intelligence Surveillance Act (FISA). These three protocols are addressed in turn.

To supply sufficient remedies to EU data subjects,[116] as mandated by the GDPR,[117] the United States created a new Ombudsperson Mechanism.[118] The Ombudsperson Mechanism created a Senior Coordinator (or "Ombudsperson") in the State Department. This Ombudsperson was foreign governments' point of contact to raise concerns about U.S. intelligence activities.[119] In response to these concerns, the Ombudsperson can rely on existing U.S. review mechanisms to remedy intelligence agency's non-compliance.[120] This system created a reactive response to non-compliance.

The second component the EU Commission assessed was the U.S. Executive's foreign surveillance authority. Under the Constitution, the Executive branch has authority over national security.[121] Congress can limit that authority, but the President can still govern intelligence agencies within those limitations. The EU Commission reviewed two key Presidential tools, Executive Order 12333 (E.O. 12333) and Presidential Policy Directive 28 (PPD-28). E.O. 12333, when enacted in 1981, established new surveillance authorities for U.S. intelligence agencies.[122] E.O. 12333 allows intelligence agencies to collect and retain EU data users' information that is travelling to the United States. Furthermore, E.O. 12333 is not governed by statute and does not give EU data users redress.[123]

The EU Commission also considered PPD-28, an executive order. PPD-28 imposed limitations on "signals intelligence operations," binding U.S. intelligence authorities.[124] The purpose of PPD-28 was to clarify what the

116. Under FISA, the U.S. provided some remedies to EU Data Subjects. This included bringing a civil cause of action against U.S. government officials and the Freedom of Information Act (FOIA).

117. *See* GDPR, *supra* note 22, art. 44 ("All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."); *Schrems II*, ¶ 92 (discussing how adequate remedies is implicitly required in Article 45 Adequacy Agreements, even though Article 45 does not explicitly require it).

118. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016 [hereinafter EU–U.S. Privacy Shield].

119. EU–U.S. Privacy Shield recital 116.

120. EU–U.S. Privacy Shield recital 120.

121. EU–U.S. Privacy Shield recital 68.

122. Executive Order 12333, EPIC (accessed Oct. 26, 2020), https://epic.org/privacy/surveillance/12333/.

123. *See* EU–U.S. Privacy Shield recital 115.

124. EU–U.S. Privacy Shield recital 69.

United States does and does not do during foreign surveillance.[125] The EU Commission found that PPD-28 "capture[d] the essence of the principles of necessity and proportionality."[126] Together, E.O. 12333 and PPD-28 authorizes American intelligence agencies foreign surveillance power.

The third component the EU Commission was concerned with was FISA, an American law establishing foreign surveillance procedures. FISA was originally enacted in 1978 as a response to "abuses of U.S. persons' privacy rights" by the U.S. government.[127] The U.S. government claimed those abuses occurred during national security investigations.[128] Therefore, Congress passed FISA to establish foreign surveillance procedures, specifically to collect information about "agents of foreign powers."[129] Rather than authorizing individual surveillance activities on a case-by-case situation, FISA authorizes authorized surveillance programs (e.g., PRISM[130] and UPSTREAM[131]).[132]

In light of the Ombudsperson Clause, U.S. Executive's power (i.e., E.O. 12333 and PPD-28), and FISA, the EU Commission assessed the EU–U.S. Privacy Shield's safeguards and limitations.[133] Ultimately, the EU Commission adopted the EU–U.S. Privacy Shield, finding that the "United States ensures an adequate level of protection for personal data transferred from the Union" to the United States.[134] Therefore, any entity that accepts the Privacy Shield's provisions can transfer data, relying on an Article 45 Adequacy Agreement.

---

125. *President Obama's Remarks on NSA Program (Transcript)*, POLITICO (Jan. 17, 2014), https://www.politico.com/story/2014/01/barack-obama-nsa-speech-transcript-102315 ("[T]he new presidential directive that I have issued today will clearly prescribe what we do, and do not do, when it comes to our overseas surveillance.").

126. EU–U.S. Privacy Shield recital 76.

127. James G. McAdams III, *Foreign Intelligence Surveillance Act (FISA): An Overview*, FED. L. ENF'T TRAINING CTRS., https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

128. *See id.*

129. *Id.*; *The Foreign Intelligence Surveillance Act - News and Resources*, ACLU, https://www.aclu.org/other/foreign-intelligence-surveillance-act-news-and-resources.

130. "PRISM is a tool used by the US National Security Agency (NSA) to collect private electronic data belonging to users of major internet services like Gmail, Facebook, Outlook, and others." T.C. Sotteck & Janus Kopfstein, *Everything You Need to Know About PRISM*, THE VERGE (July 17, 2013), https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

131. "Upstream Surveillance is a term used by the National Security Agency (NSA) of the United States for intercepting telephone and Internet data from the Internet backbone, i.e., major Internet cables and switches, both domestic and foreign." *Upstream Surveillance*, LDAP WIKI, (last updated Oct. 8, 2018), https://ldapwiki.com/wiki/Upstream%20Surveillance.

132. EU–U.S. Privacy Shield recital 109.

133. EU–U.S. Privacy Shield recital 65.

134. EU–U.S. Privacy Shield art. 1.

Absent an Article 45 Adequacy Agreement (e.g., the Privacy Shield), private entities can transfer data if protected by an Article 46 Safeguard Agreement, the second safeguard provision the GDPR authorizes.[135] One type of Safeguard Agreement is SCCs. SCCs are pre-authorized contracts that can be an EU entity and a non-EU entity can adopt, notably not directly including governments as parties to the SCCs. In the SCCs, the non-EU entity would agree to appropriate safeguards to ensure adequate protection and remedies for EU data users. Once the entities agreed to an SCC, the SCC is subject to review by the EU entity's supervisory authority, an independent public authority that is responsible for monitoring GDPR compliance.[136] Unless the supervisory authority finds that the SCC does not provide an adequate protection, the two entities can transfer the data transnationally, and this protocol applies to all Safeguard Agreements under Article 46.

Together, non-EU entities can legally transfer data under an Article 45 Adequacy Agreement or an Article 46 Safeguard Agreement (e.g., an SCC). If the non-EU entity is in a country with a valid Adequacy Agreement, then the entity only must subscribe to their respective Adequacy Agreement's provisions before transferring data. If the entity is not in a country with an Adequacy Agreement, then the entity can still transfer data with an Article 46 Safeguard Agreement. That is, the non-EU entity does not have to rely on their own government to provide adequate protections. A non-EU entity can provide adequate protections on their own. Together, Adequacy Agreements and Safeguard Agreements provide non-EU entities options to transfer data in compliance with the GDPR.

C. THE CJEU DECISION IN *SCHREMS II*

In *Schrems II*, the CJEU scrutinized the EU–U.S. Privacy Shield Adequacy Agreement and SCC Safeguard Agreements. Essentially, the CJEU addressed whether the EU–U.S. Privacy Shield provided enough protection to EU data users to be a valid Adequacy Agreement, and whether SCCs could ever provide an adequate level of protection mandated by the GDPR. The CJEU concluded negatively to the former but affirmatively to the latter.

135. "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." GDPR, *supra* note 22, art. 46.

136. *Id.* arts. 4, 51.

This Section begins by discussing why the CJEU invalidated the EU–U.S. Privacy Shield. Then this Section discusses why the CJEU affirmed SCCs' validity.

1. The CJEU Privacy Shield Invalidation

The first question the CJEU evaluated was whether the EU–U.S. Privacy Shield was a valid treaty under Article 45.[137] The CJEU invalidated the EU–U.S. Privacy Shield because of its unproportionate limitations and lack of remedies.[138]

The CJEU found the Privacy Shield's inadequacies invalid for two reasons. First, the U.S. foreign surveillance programs were not proportional to what is strictly necessary. The CJEU recognized that data user's privacy rights are not absolute, but considered in connection to personal data's function in society.[139] This includes data transfers necessary for important public interest reasons, like public security.[140] But, that limitation must be proportional to the interest and applied only as strictly necessary.[141] In the Privacy Shield, FISA authorized U.S. surveillance programs in general, not on a case-by-case basis.[142] That means there was no limitation on FISA's powers. Therefore, because FISA lacked proportionality, the Privacy Shield's failure to address those inadequacy rendered it invalid.

Second, the CJEU determined that the Privacy Shield did not provide EU data users adequate remedies. The GDPR requires that those whose rights have been violated shall have the right to an effective tribunal remedy.[143] When deciding an Adequacy Decision, the Commission must consider "effective administrative and judicial redress for the data subjects whose personal data are being transferred."[144]

Furthermore, although some data users can be susceptible to U.S. surveillance, they do not necessarily have legal redress[145] under E.O. 12333 and

137. The fourth, fifth, ninth, and tenth questions concerned whether the Privacy Shield Decision ensures an adequate level of protection and whether data transfers, pursuant to the SCC and Privacy Shield's ombudsperson clause, is compatible with the GDPR and the Charter. In essence, whether the Privacy Shield is valid under EU law.

138. *See* Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Ltd., 2020 E.C.R., ¶ 201.

139. *Id.* ¶ 172.

140. *See* GDPR, *supra* note 22, art. 49.

141. *Schrems II*, ¶¶ 174–76.

142. *Id.* ¶ 179. For a discussion on FISA, see *supra* pp. 1588–1591.

143. GDPR, *supra* note 22, art. 78.

144. *Id.* art. 45.

145. *Schrems II*, ¶ 191.

PPD-28,[146] leaving a gap in EU data users' legal remedies. The Commission relied on the Privacy Shield's Ombudsperson to fill this gap. The Ombudsperson[147] allegedly ensured the required remedial rights.[148] Contrary, the CJEU found that the Ombudsperson did not have binding power over the U.S. intelligence agencies.[149] Furthermore, the Ombudsperson mechanism did not provide any legal safeguards that EU data users could rely on.[150] These two issues made the Ombudsperson mechanism an insufficient remedy.[151] The CJEU found that this gap in legal remedies, and the fact that the Ombudsperson did not fill this gap, the Privacy Shield did not ensure an adequate level of protection. Therefore, the Privacy Shield was invalid.

2. The CJEU SCC Validation

The second question the CJEU evaluated was whether SCCs were valid means to internationally transfer data. The CJEU affirmed their validity because SCCs, ostensibly, provide adequate safeguards.

Preliminarily, the CJEU defined what level of protection the GDPR requires to transfer data via an SCC. Addressing Article 46's required level of protection, the CJEU clarified that an adequate level is enough protection to be "essentially equivalent to that guaranteed within the European Union."[152] In order to transfer EU data, non-EU entities must provide an adequate level of protection. To determine whether a non-EU entity is providing an adequate level of protection, an EU member state's supervisory authority assesses both the contractual clauses and the non-EU entity's legal system.[153] Notably, the non-EU government does not have to provide the adequate level of protection; instead, a non-EU entity itself can "compensate for the lack of data protection in a third country."[154] Considering all the above, if a supervisory authority determines there is an adequate level of protection, then the non-EU entity can transfer EU data.

However, if the EU supervisory authority determines that an adequate level of protection is not ensured by the SCC, then the supervisory authority

146. *Id.* ¶ 182–83.

147. This is the "Senior Coordinator for International Technology Diplomacy," or the EU's point of contact.

148. *Schrems II*, ¶ 193.

149. *Id.* ¶ 196.

150. *Id.*

151. *Id.* ¶ 197.

152. *Id.* ¶ 94.

153. *Id.* ¶ 104. When assessing a third-country entity, the CJEU directed Supervisory Authorities to Article 45(2) which enumerates a non-exclusive set of factors to consider.

154. GDPR, *supra* note 22, recital 108.

must take remedial action to ensure EU data user's privacy rights.[155] This includes "impos[ing] a temporary or definitive limitation including a ban on processing . . . to order the suspension of data flows to a recipient in a third country."[156] In addition, supervisory authorities can suspend international data transfers if the supervisory authority determines that "the standard data protection clauses are not or cannot be complied with" and adequate protection cannot be ensured.[157] That is, EU supervisory authorities have some discretion as to which corrective power is necessary. But if a supervisory committee determines that the SCC does not provide an adequate level of protection, then the private parties must suspend data transfers.

In addition to the supervisory authorities, EU private parties also have responsibility to ensure an adequate level of protection before transferring data outside of the EU. Transfers with EU data inevitably involve an EU party before they transfer the data out of the EU. If the EU party cannot guarantee an adequate level of protection, they must suspend data transfers.[158] That is, EU parties have responsibility to ensure EU data-users protection before internationally transferring the data.

In conclusion, the CJEU determined the Privacy Shield was invalid because the U.S. access to EU data was not proportional to what was strictly necessary and failed to provide EU citizens adequate remedies. Nonetheless, the CJEU determined SCCs were still valid because SCCs have backstops to protect data users' privacy rights, so the CJEU determined that SCCs were still a valid means to transfer data.

IV. PARODOXICALLY, *SCHREMS II* PROMOTES INTERNET BALKANIZATION WHILE MAINTAINING AN OPEN INTERNET

By invalidating the EU–U.S. Privacy Shield and upholding SCCs, *Schrems II* requires non-EU entities to adopt the EU's stringent privacy standard (i.e., the GDPR) if they want to participate in the EU market. That leaves some non-EU entities (e.g., American entities, likely, and other close economic allies) to adopt the EU standard. However, the EU standard may fundamentally preclude some non-EU entities because of their own home country regulations.[159] This dichotomy fragments the internet, resulting in Internet

155. *Schrems II*, ¶ 111.
156. GDPR, *supra* note 22, art. 58(2).
157. *Schrems II*, ¶ 113.
158. *Id.* ¶ 135.
159. Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security*, BROOKINGS INST. (Aug. 5, 2020), https://

Balkanization. But, by refusing access to EU data from non-compliant entities, EU data users' information privacy rights are upheld; EU data users have more control over their data without fear that non-compliant parties will inappropriately use their data. Moreover, as a result of having more control over their information, EU data users have more freedom to choose how they present themselves on the internet, how they interact with the internet, and how others interact with them on the internet. That is, they have more autonomy—independence from adverse influence. Having internet autonomy is one of the foundational tenets of the open internet. Thus, in effect, *Schrems II* maintains open internet ideals by promoting Internet Balkanization.

This Part begins by discussing how *Schrems II* promotes Internet Balkanization, the global internet's fragmentation. Next, this Part discusses how the "digital border" the European Union erected in *Schrems II*, the border fragmenting the internet, protects EU data users' information privacy. From that, EU data users maintain digital autonomy, which the third Section of this Part discusses. Finally, this Part concludes by discussing how maintaining digital autonomy maintains one of the open internet's core tenets: the free flow of information.

A. *SCHREMS II* PROMOTES INTERNET BALKANIZATION

Following *Schrems II*, there are three legal remedies entities can adopt to continue transnational data transfers and be compliant with the GDPR. Entities residing in a country with an Article 45 Adequacy Decision can rely on the Adequacy Decision, entities can adopt an Article 46 Safeguard Agreement (e.g., SCC), or entities can localize their data in the European Union. However, limiting entities to these three options promotes Internet Balkanization.

This Section begins by analyzing each option independently. Then, it discusses how limiting non-EU entities to these three options promotes Internet Balkanization.

1. The three options non-EU entities have post-Schrems II

Following the CJEU's decision, there are three option non-EU entities can take to legally transfer EU data.

First, non-EU states can adopt a new Article 45 Adequacy Decision treaty, allowing economic entities to transfer data. For American entities, it is very possible that the European Union and United States will agree to a new EU–

www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/; *see infra* pp. 45–48.

U.S. treaty, but this is the second EU–U.S. treaty the CJEU has invalidated.[160] Repeated invalidation insinuates that Article 45 Adequacy Decisions to be less reliable long term. Also, until the EU Commission accepts another Article 45 Adequacy Decision, companies must rely on other lawful means to transfer data.[161] Therefore, because of the lack of reliability and lack of time frame, this remedy is not a viable option in the meantime.

Second, companies could comply with other Safeguard Agreements under Article 46: a more stable choice. Prior to the *Schrems II* decision, some companies, like Microsoft, already adopted standard contractual clauses.[162] Also, "89% of non-government EU firms transfer personal data from the Union to the United States using the SCCs, making it the most relied upon mechanism for such transfers."[163] However, post *Schrems II*, the Commission will have to approve SCCs on a case-by-case basis.[164]

Third, companies can localize EU data users' information in the European Union, a strategy rising in recent years.[165] Data localization is when data controllers or processors move their facilities into the respective jurisdiction, here the European Union, to avoid transnational data transfers laws. This is a way for companies to avoid the transatlantic data transfer issue. However, data localization is not a perfect remedy. For instance, keeping all European data in Europe could be expensive because it impairs the economies of scale and reduces efficiency.[166] Another downside of data localization is the existence of technical problems with data localization.[167] For example, data may need to be

160. *See generally* Case C-362/14, Data Protection Commissioner v. Facebook Ireland, Ltd., 2015 E.C.R. (invalidating the EU-U.S. International Safe Harbor Privacy Principles).

161. The California Consumer Protection Act (CCPA) is the State of California's general statute for privacy rights. It can be argued that since Article 45 only applies to federal statutes, the CCPA fall under Article 45's Adequacy Decision. If so, this would allow California companies to transfer EU data user information without needing to develop their own safeguards.

162. Natasha Lomas, *Europe's Top Court Strikes down Flagship EU-US Data Transfer Mechanism*, TECH CRUNCH (July 16, 2020), https://techcrunch.com/2020/07/16/europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/?guccounter=1#:~:text=A%20highly%20anticipated%20ruling%20by,wrote%20in%20a%20press%20release [https://perma.cc/EYA7-Z39G].

163. Brief for BSA The Software Alliance as Amici Curiae Supporting Respondents Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Ltd., 2020 E.C.R.

164. *Shcrems II*, ¶ 134.

165. Chander & Lê, *supra* note 4 (reviewing recent data localization laws of Australia, Brazil, Canada, China, European Union, France, Germany, India, Indonesia, Malaysia, Nigeria, Russia, South Korea, Vietnam, and others).

166. Reisman, *supra* note 49; Cody Ankeny, *The Costs of Data Localization*, ITI (Aug. 16, 2017), https://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization.

167. Reisman, *supra* note 49.

accessed by engineers in other countries for maintenance.[168] Furthermore, data localization restricts what companies can do with data. Restricting the flow of information "raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances."[169] Because of these issues, data localization is not an ideal plan, but it is one that would prevent transnational data transfer issues.

2. These options require entities to adopt an EU-centric internet standard.

Limiting non-EU entities to these options leaves non-EU entities two options to transfer EU data. Non-EU entities can adopt an EU-centric privacy standard, by adopting an Adequacy or Safeguard Agreement, and be included in the EU-centric internet sphere. Or non-EU entities can reject these remedies and exclude themselves from the EU-centric internet sphere. Choosing either agreement results in the entity adopting an EU-centric internet standard and making themselves more EU-centric.

Non-EU countries adopting an Article 45 Adequacy Decision must ensure "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order."[170] This includes both private entities and the non-EU state. In other words, if a foreign entity wants to have an Adequacy Decision, they will have to adopt and comply with GDPR equivalent standards. By adopting GDPR equivalent standards, non-EU entities adopt an EU-centric internet standard. A handful of countries have an EU Adequacy Decision.[171] These countries can openly flow data between themselves and the European Union, allowing them to be included in the EU-centric internet sphere.

Similarly, if an entity adopts a Safeguard Agreement, that entity is inevitably adopting an EU-centric internet standard. If a non-EU entity resides in a country that does not have a valid Article 45 Adequacy Agreement, then that entity can adopt an Article 46 Safeguard Agreement.[172] When adopting a

168. *Id.*

169. Chander & Lê, *supra* note 4, at 721.

170. *Schrems II*, ¶ 162.

171. *Adequacy Decisions*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,are%20ongoing%20with%20South%20Korea [https://perma.cc/JM5D-XWZK], (accessed November 3, 2020) (listing Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay all have Adequacy Decisions).

172. GDPR, *supra* note 22, art. 46 ("In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards.").

Safeguard Agreement, entities are required to ensure a level of protection "essentially equivalent" to that guaranteed in the European Union.[173] However, this is not an "identical level of protection," as the CJEU made clear, but it is difficult to distinguish the difference between "essentially equivalent" and "identical."[174] Furthermore, by adopting a Safeguard Agreement, entities ensure protection whether the data will be processed immediately or in the future.[175] This requires entities to ensure an equivalent level of protection perpetually. By adopting an Article 46 Safeguard Agreement, entities adopt the EU-centric internet standard, similar to when third countries adopt an Article 45 Adequacy Agreement.

Entities without Article 45 and Article 46 Agreements can still participate in the EU market if they localize EU user data in the European Union, completely avoiding international data transfers. Under this option, EU data user's information would be collected, processed, and stored in the European Union. Localization creates a confined EU internet sphere.[176] As discussed earlier,[177] data localization is not an ideal solution for several reasons,[178] but it is an option available.

In sum, whether an entity adopts an Article 45, Article 46, or a data localization remedy, the entity is adopting an EU-centric internet standard.

3. The EU-centric internet border divides entities that can adopt an EU internet standard and those that cannot.

Requiring non-EU entities to adopt an EU internet standard creates an internet border around the EU. If a non-EU entity wants to participate, they must adopt one of the three options above. The option is their "passport" to transfer data between different states freely. If an entity fails to adopt one of the three options, they do not have a passport, and they are unable to transfer data. Therefore, there is a dichotomy between entities that adopt the EU

173. *Schrems II*, ¶ 94.

174. Also, supervisory authorities can suspend data transfers, which would disrupt business. This incentivizes entities to ensure compliance. *See Schrems II*, ¶ 113.

175. *Schrems II*, ¶ 89.

176. However, GDPR art. 49 includes exceptions that allow transfer of data if the transfer is necessary for important reasons of public interest," if "the transfer is necessary for the establishment, exercise, or defense of legal claims," "the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject," and other reasons. But those instances are rare. Council of Bars and Law Societies of Europe, *CCBE Assessment of the U.S. CLOUD Act* 7 (Feb. 28, 2019).

177. *See supra* pp. 40–41.

178. *See* Meltzer, *supra* note 159 ("Yet for small companies, the impacts are most pronounced. For many, setting up in the EU is not an option.").

internet standard and those that don't. There are some organizations that fundamentally cannot adopt an EU model.

Beginning with Article 45 Adequacy Agreements, there are only a handful of non-EU states that have valid Adequacy Agreements with the EU.[179] The states that have adopted an Adequacy Agreement are culturally and politically similar to the European Union. The fact that the United States did not have a valid Adequacy Agreement, a country with strong ties and political consistencies with the European Union, highlights how unfeasible an Article 45 Adequacy Agreement can be. There are some states that are very unlikely to adopt an Adequacy Agreement,[180] and not many countries may want to adopt an Adequacy Agreement. Entities outside of these enumerated states have to have an Article 46 Safeguard Agreement or localize their data.

Even though entities can adopt an Article 46 Safeguard Agreement to authorize data transfers, this is not a simple remedy. First, some home state policies fundamentally prevent entities from adopting an adequate Article 46 Safeguard Agreement, especially in more authoritarian states with different privacy rights.[181] Some states *want* private entities to collect information; that way, the state can use the collected behavioral data for their own use.[182] If an EU Supervisory Authority does not find an adequate level of protect, data transfers would be suspended.[183]

Furthermore, companies may be dissuaded from adopting an Article 46 Safeguard Agreement regardless of the home country's policies.[184] This is particularly true for smaller companies. Safeguard Agreements create difficulties for smaller companies by imposing additional costs which smaller companies may feel are not possible or worthwhile to bear.[185] Therefore,

179. Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay all have Adequacy Decisions.

180. Meltzer, *supra* note 159 ("If the U.S. is still not adequate, then it must be the case that other countries, including China will never be adequate and not only that, but it is hard to see how any Chinese company collecting EU personal data can transfer it back to China consistently with GDPR.").

181. *Id.*

182. Mariano-Florentino Cuéllar & Aziz Z. Huq, *Privacy's Political Economy And The State Of Machine Learning*, 76 NYU ANNUAL SURVEY OF AMERICAN LAW 317, 342 (2021).

183. *Schrems II*, ¶ 113.

184. *See Facebook Will Move UK Users to US Terms, Avoiding EU Privacy Laws*, THE GUARDIAN (Dec. 16, 2020), https://amp.theguardian.com/technology/2020/dec/15/facebook-move-uk-users-california-eu-privacy-laws (discussing how Facebook will move UK data users to U.S. terms because the EU privacy regime is the strictest privacy regime).

185. *See* Meltzer, *supra* note 159 ("The difficulties with SCCs also create additional costs and disincentives for EU companies to develop digital supply chains with SMEs in third countries.").

smaller companies' limited resources may hinder them from adopting the EU-centric internet sphere.

Finally, there is the data localization option. This is the option of last resort for entities that cannot rely on an Article 45 Adequacy Agreement nor comply with an Article 46 Safeguard Agreement. Those entities are left with only localizing their data in the European Union. That data would remain exclusively in the European Union, exclusively in the EU-centric internet sphere.

In order to use EU data at all, non-EU entities must adopt EU privacy standards. However, some non-EU entities are prohibited—fundamentally or functionally—from adopting EU privacy standards. The barriers to entry are too inaccessible. Therefore, a robust legal border confines the EU-centric internet sphere, fragmenting the open internet.

B. FROM THE REGULATIONS THAT WILL FRAGMENT THE INTERNET, EU DATA USERS' INFORMATION PRIVACY RIGHTS REMAIN INTACT

Information privacy is the control a data user has over their information,[186] the "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[187] In an increasing digital, globally connected world, people relinquish greater volumes of data and more private information.[188] Collecting information has turned into an industrial complex.[189] Increasingly, more and more entities want access to data user's information.[190]

However, in *Schrems II* the CJEU's objective was to uphold EU data users' information privacy rights. It succeeded; from the regulations that will inevitably fragment the internet come procedures that will uphold information privacy. *Schrems II* prioritized data users' privacy rights in two ways. First, *Schrems II* limited non-EU state actors' access to EU data users' information by holding states accountable for using private entities data. Second, *Schrems II* limited private third parties' access to data users' information. By separating both non-EU states and private third parties from EU data users, the fragment, *Schrems II* bestowed enforceable privacy right to EU citizens.

186. Manheim & Kaplan, *supra* note 16, at 118.

187. GDPR, *supra* note 22, art. 1.

188. *See supra* pp. 5–9; *see also* GDPR, *supra* note 22, recital 6 (illustrating data collection's increasing prominence in society and discussing how "[t]echnology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally.").

189. THE ECONOMIST, *supra* note 12.

190. *See id.*

1. Schrems II limits state actors' access to data users' information, prioritizing data users' privacy rights over non-EU states' interests.

Schrems II recognized that, even when states use private party's data for security reasons, states remain susceptible to the GDPR. However, the CJEU also recognized that private entities themselves can adopt adequate privacy standards regardless of their home state's standards; just because a state does not provide adequate safeguards does not necessarily mean that the private entities themselves cannot provide the required safeguards.[191] Therefore, the CJEU recognized a separation between private entities and their states. But, whether private entities are capable of providing adequate protection depends on whether their home state's policies infringe on the private entities' safeguard measures.[192] If the state infringes on an EU data users' privacy rights (e.g., conducting general surveillance), then the private entity risks having all data transfers suspended.[193] Therefore, states do not get to take advantage of their domiciled companies with EU data, even when they are processing the data for national security concerns.[194] The states' actions have consequences.

Using the EU–U.S. Privacy Shield as an example, the CJEU ensured data users' privacy rights when another party transfers their data out of the European Union via an Adequacy Agreement. The CJEU did that in two ways.

First, when states process data for national security, processing must be proportional to what is strictly necessary.[195] In other words, supervisory authorities do not enjoy carte-blanche access to data and get to claim "security" as its valid reason. Otherwise, this would lead to an indefinite loss of control over one's data.[196] For example, by invalidating the Privacy Shield because of this carte-blanche surveillance power, the CJEU set precedent for data users' privacy in all Adequacy Agreements. Data users can use the web without indefinite surveillance threats. Of course, the supervisory authority can monitor data users when necessary, but that is only in narrow situations, prompted by justified reasons.

Second, the CJEU required Article 45 Adequacy Agreement states to arrange data users with more remedial agency. Providing adequate remedies is

191. *Schrems II*, ¶ 136 ("[T]he mere fact that standard data protection clauses . . . do not bind the authorities . . . cannot affect the validity of that decision.").

192. *See id.* ¶ 129.

193. This is another reason why some private entities may not be able to ensure an adequate level of protection. Governments take advantage of tech companies data collection.

194. *See Schrems II*, ¶ 88.

195. *Id.* ¶ 176.

196. Although the supervisory authority may not constantly monitor data users' activities, the threat alone may adversely impact data users' experience.

essential to information privacy. Otherwise, privacy would be toothless. Adverse third parties would be able to interfere with data users without repercussions. Therefore, to practically have privacy rights, adequate remedies are essential. *Schrems II* reinforces the right to adequate remedies.[197] The CJEU recognized how some American surveillance programs do not provide legal redress,[198] which the U.S. government also recognized,[199] and the Ombudsperson did not remedy those gaps.[200] Therefore, the Privacy Shield's lack of adequate remedies left EU data users with toothless privacy rights, privacy rights EU data users could not enforce.

2. Schrems II limits private third parties' access to data users' information.

By recognizing that private entities are not confined by their home state's regulations, the CJEU tasked private entities with the responsibility to ensure an adequate level of protection. This specifically concerns Article 46 Safeguard Agreements. The CJEU recognized that Article 46 Safeguard Agreements are based on private entities, both EU and non-EU private entities, to ensure adequate levels of protection.[201] On a case-by-case basis, the EU entity decides whether Safeguard Agreements provide an adequate level of protection.[202] Also, if the non-EU recipient cannot comply with their Safeguard Agreement, then they are required to suspend data transfers.[203] Therefore, the CJEU delegated responsibility to private entities.[204]

At first impression, giving power to private entities may not seem to give data users more privacy rights, but the way *Schrems II* gives private entities more responsibility indirectly ensures more data user privacy rights. *Schrems II* mandated that economic entities must ensure an adequate level of protection. If not, they risk suspending data transfers. This incentivizes economic entities to ensure adequate protection. Otherwise, data transfer suspensions could drastically harm the company because a suspension of data transfers would disrupt their business operations.

In addition to the original party to whom an EU data user relinquishes their data, the GDPR and EU Charter also require third parties (e.g., economic partners or companies that buy their data) to ensure an adequate level of

197. *Id.* ¶ 197; GDPR, *supra* note 22, art. 45.
198. *Schrems II*, ¶ 191.
199. *Id.* ¶ 181.
200. *Id.* ¶ 196.
201. *Id.* ¶ 134.
202. *Id.*
203. *Id.* ¶ 143 (additionally requiring entities to return or destroy any data that has already been transferred).
204. *Id.* ¶ 137.

protection.[205] If an economic entity transfers user data to a third party, and that party does not provide an adequate level of protection, then the original party risks having their data transfers suspended.[206] In other words, parties are accountable for where they transfer data to. Therefore, EU privacy standards transfer with EU data.

In sum, the CJEU requires third-party entities to comply with the GDPR before the third-party transfers the EU data user's information.

C. FROM INFORMATION PRIVACY, EU DATA USERS WILL HAVE MORE DIGITAL AUTONOMY

When data users have more control over their data, they have more autonomy. As discussed above, *Schrems II* protected data user's control over their information. Now, EU data user's rights transfer along with their data,[207] extending protection past the original recipient. Since data users still have rights when a third party has possession over that data, data users have more control. When data users have more control, they have more influence on who impacts their digital experience. If a data user wants to share their location with friends, an action that may potentially impact where someone goes on a given day, they can. If a data user wants to have curated advertisements, they can. But they are the ones who decide, not an adverse party. In other words, data users control who has what information, information that may influence a data users' actions depending on who has it.

Schrems II embodies digital autonomy. An EU data user may consensually disclose information to a foreign entity. Take, for instance, Facebook U.S. as an extension of Facebook Ireland. An EU citizen discloses information to Facebook U.S. via the Facebook app. However, that data user may not want to disclose that information to the U.S. government via FISA.[208] *Schrems II* prevents that. Even if the foreign entity (Facebook U.S.) shares that information to a third party (e.g., a business partner), that party also has to ensure GDPR compliance.[209] And part of the GDPR grants data users the right

205. *See id.* ¶ 137 (requiring standard data protection clauses to ensure effective measures to provide an adequate level of protection, this can be implicitly read to ensure an adequate level of protection for wherever the data goes).

206. *See id.*

207. *See* Case C-311/18, Data Protection Commissioner v. Facebook Ireland, Ltd., 2020 E.C.R., ¶ 137 (requiring standard data protection clauses to ensure effective measures to provide an adequate level of protection, this can be implicitly read to ensure an adequate level of protection for wherever the data goes).

208. *See supra* p. 34 (discussing how FISA was too over encompassing, allowing U.S. intelligence agencies general surveillance rights over EU citizens).

209. *See Schrems II*, ¶ 137.

to know where their personal information has been transferred,[210] what safeguards that foreign entity has implemented,[211] and the right to "erasure."[212] All these rights aggregate to EU data users having independent control over their information. From this control, data users have more autonomy.

By having digital autonomy, EU citizens can freely express themselves as their individual selves, free from adverse users, manipulation, or political influence. Using the Cambridge Analytica scandal as an example, data users would have had the ability to track where Facebook shared data users' information and how they were using that data. Ideally, this would have preempted Cambridge Analytica from manipulating political opinions by sending targeted propaganda. Therefore, data users' political intentions would have remained unadulterated. They would have remained individualistic.

D. HAVING DIGITAL AUTONOMY MAINTAINS ONE OF THE OPEN INTERNET'S CORE TENETS

By providing more individual autonomy, *Schrems II* promotes the free flow of information an open internet sought to achieve. There are two main reasons why greater accessibility is desirable: the open internet enables information to flow freely, and the open internet stimulates economic advancement.[213]

1. Digital autonomy facilitates the free flow of information.

The open internet has social benefits, arising from the free flow of information, ideas, knowledge, and viewpoints.[214] The free flow of information is beneficial to society because it prevents suppression, and digital autonomy upholds those interest. At the end of this Section, there is a discussion about how the free flow of information could inadvertently harm data users by allowing too much transparency, but this Section resolves those concerns.

As explained above, the open internet is beneficial because it cultivates open communication.[215] It is a vehicle to share information with people,

210. GDPR, *supra* note 22, art. 15(1). ("The data subject shall have the right to obtain from the controller confirmation as to whether . . . [their information is] processed, and, . . . access to the personal data and the following information: (c) the recipients . . . to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.").

211. *Id.* art. 15(2) ("Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.").

212. *Id.* art. 17.

213. Daskal et al., *supra* note 53, at 26.

214. ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS, *supra* note 50, at 22–23.

215. *See supra* p. 13.

regardless of distance. Two people, physically present at two different parts of the world, could still connect with each other. From that connection, they can share ideas or information with each other. Or this connection could involve an individual reading the daily news in a different continent. In general, the internet provides open, uncomplicated mediums to communicate globally.

Digital autonomy protects the ability for data users to have this open communication by preventing information suppression. As discussed earlier, digital autonomy provides data users more control over their data.[216] Data users, at least EU data users, will be able to choose whether to communicate and whom to communicate with. At a minimum, EU journalists would be able to communicate what is happening across the world, especially when more traditional methods of communication, like print media, are easier to restrict and censor.[217] In theory, they would be able to disseminate information via social media, news websites, or other mass media vectors.[218] Therefore, suppressive laws would silence their information. A government would not be able to suppress EU data user's right to disclose. EU data users can still publish information about local political movements, human rights crises, or general cultural experiences.

At the same time, free flow of information could have adverse consequences. An entity may have more access to data users' information than intended. As more information becomes accessible, and sophisticated technology can find patterns in seemingly insignificant data, data users could disclose more information than they intended. Furthermore, data users may vary on what kind and how they disclose information.[219] That is, cultural differences may impact what information a data user discloses and who has access to that information.

---

216. *See supra* pp. 56–57.

217. MIKAL HEM, REUTERS INST. FOR THE STUDY OF JOURNALISM, EVADING THE CENSORS: CRITICAL JOURNALISM IN AUTHORITARIAN STATES 20 (2014), https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Evading_the_Censors_Critical_journalism_in_authoritarian_states_0.pdf ("Some journalists use social media and other internet outlets to publish material that is not possible to publish in traditional media, and online newspapers are generally confined by less strict censorship laws. But increasingly, governments in authoritarian countries try to restrict online content.").

218. Of course, if the internet sphere is fragmented due to mechanical barriers, then the internet would be preliminarily inaccessible. However, there are few places with such strict internet barriers (e.g., North Korea).

219. *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004) (exploring how Europeans and Americans have two different cultures of privacy, which exemplifies how different cultures have different definitions of "privacy").

States upholding EU users' autonomy will respect EU data users' different cultural values. Data users may value different information more than others, thus making data users more inclined to disclose certain information. For example, Americans privacy stems from the belief that Americans should be free from intrusions of the state.[220] But Europeans privacy stems from the belief that people have the right to dignity and honor.[221] The different implicit beliefs may result in data users being more willing to disclose certain information than other information. Americans may be more willing to disclose information to companies (i.e., not the state) while Europeans may be more willing to disclose innocuous information to the state.[222]

As a more practical example, data users may vary how much they disclose intimate details depending on which state they are in. For example, queer data users may readily disclose their sexual identity to an American entity to find community. But in countries where it is illegal to be queer,[223] queer data users would be more reluctant to disclose their sexual orientation. In a completely open internet, queer data users may not have that liberty to differentiate which entities have that information. But with digital autonomy, data users get to choose which foreign entities have that information and which do not. Having digital autonomy enables the open internet to respect different data users' cultural differences while still maintaining an open internet.

An increasing digital environment only exacerbates the cultural difference concerns. As discussed earlier, as more information becomes accessible, data processers can discover more intimate details.[224] Data users' digital presence discloses intimate details that they may not want to readily disclose. Therefore, it is pertinent that data users have autonomy in an increasing digital and global environment.

220. *Id.* at 1161.

221. *Id.*

222. *Id.*

223. OUTLIFE, https://www.outlife.org.uk/which-countries-criminalise-homosexuality?gclid=CjwKCAiAq8f- BRBtEiwAGr3Dgfod5qF7Y3j0e2sm14QUEj7T2TkFY6bBisoaZmJDZKMTz4xh9xIIuxoCWj0QAvD_BwE [https://perma.cc/8APQ-LN97].

224. Cuéllar & Huq, *supra* note 182, at 328–30 (discussing how AI can also expand privacy intrusions based on making inferences, predicting behavior, drawing on information once unanalyzable (e.g., genetics)).

2. Arguably, digital autonomy will facilitate an open market.

An open internet favors economic advancements for two main reasons.[225] First, the open internet, as an open market, facilitates global trade efficiently.[226] Second, the open market facilitates innovation. Internet Balkanization arguably counteracts them both.[227]

But this Note is not focused on remedying Internet Balkanization's economic maladies. In the first place, how Internet Balkanization harms the economy is debatable.[228] Also, empirical research would better address this issue. However, this Note briefly discusses whether digital autonomy will be better or not for the global economy.

One of the major criticisms against Internet Balkanization is that it will ossify large companies.[229] The heightened barriers to entry will prohibit emerging companies from entering various internet spheres. Therefore, since large companies are the only ones capable of handing the various barriers to entry, they will be the only companies with a global reach. However, if states adopt digital autonomy in general, then data users should have more market agency.[230] They would be able to actively choose which companies to solicit. This would create a more pervious market.[231] On the contrary, even if data users have autonomy, the heightened barriers of entry could prevent companies from connecting to data users in the first place, making data users susceptible to market forces. Therefore, without facilitated connection, digital autonomy could be an ill-fated remedy for market access.

In sum, Internet Balkanization has some economic implications. However, how and to what extent they impact the global economy is out of this Note's scope, but future scholars should conduct empirical research on how Internet Balkanization impacts the global economy.

---

225. ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS, *supra* note 50, at 18–19.

226. *See* U.S. DEP'T OF COM., U.S. SECRETARY OF COMMERCE WILBUR ROSS STATEMENT ON SCHREMS II RULING AND THE IMPORTANCE OF EU–U.S. DATA FLOWS (July 16, 2020). U.S. Secretary of Commerce, Wilbur Ross, expressed his dissatisfaction with the decision because of the vast number of American and European companies that relied on the EU–U.S. Privacy Shield.

227. *See* Daskal et al., *supra* note 53, at 25–26.

228. *Id.*

229. *Id.*

230. *See* Cohen, *supra* note 19, at 1426 (discussing how autonomy results in people having more independent, diverse choice which can occur in the market).

231. ECONOMIC AND SOCIAL BENEFITS OF INTERNET OPENNESS, *supra* note 50, at 35–36 (discussing how the open internet increases trade).

V. CONCLUSION

"Governments of the Industrial World . . . I come from Cyberspace, the new home of Mind. . . . You are not welcome among us. You have no sovereignty where we gather."[232] Here, early internet pioneers declared cyber freedom.

When Maximillian Schrems brought his case against Facebook to the European Court of Justice, his goal was to protect EU data users' information privacy. He succeeded. But to do so, the CJEU adopted principles that would fragment the EU internet away from the global, open internet. Although Internet Balkanization would normally suppress open communication, paradoxically that may not be the case here. Instead, there may be more communication because data users have more autonomy. So, in the end, the governments of the Industrial World still are not welcomed.

232. Barlow, *supra* note 1.