South Dakota Law Review

Volume 68 | Issue 3

2023

Precision Farming and Agricultrual Data Transfers Between the US and the EU

Ana Clara

Mansur Carvalho

PRECISION FARMING AND AGRICULTURAL DATA TRANSFERS BETWEEN THE US AND THE EU

ANA CLARA MANSUR CARVALHO†

This work examines the consequences of the Schrems II *judgment on the transfer of agricultural data between the European Union ("EU") and the United States ("US"). The main objective was to understand the practical implications of the Court of Justice of the European Union ("CJEU") decision on the relations of the EU and the US related to agriculture. For this, a bibliographic review of the laws influencing the understanding of the case was carried to look further at the European legal mechanisms of data protection and the North American approach to the matter. Secondly, it is discussed how data protection is considered a fundamental right in the European Union, while in the US, this value is relativised. Finally, the practical applications of* Schrems II *are discussed, especially concerning agricultural data.*

I. INTRODUCTION

Precision farming is an approach to farm management that can lower expenses and optimise process inputs while increasing agricultural yields and animal performance.[1] Such practice can potentially improve agricultural activities' profitability by using information technology ("IT") systems.[2] Precision farming may also enhance worker safety and lessen the adverse environmental effects of agriculture, which helps ensure ecological sustainability.[3] In the US, larger farms use precision agriculture more frequently and implement strategies despite eventual technological obstacles.[4] However, a tiny percentage of small farms, which account for more than 85% of all American farms, have embraced precision agriculture.[5]

Agricultural technologies are crucial when developing food security and climate change coping mechanisms, so their development requires cooperation on a global scale.[6] Precision farming uses information technology to observe and

† Ana Clara Mansur Carvalho is a Compliance Analyst and a researcher linked to Paris 2 University. Ms. Carvalho has a master's degree in innovation law from the Paris Saclay University and a bachelor's degree from the Federal University of Minas Gerais.

1. Amanda Ashworth & Philip Owens, *Benefits and Evolution of Precision Agriculture*, USDA (Nov. 14, 2022), https://perma.cc/4VEQ-8SUM.

2. *Id.*

3. Marie Hayden et al., *Occupational Safety and Health with Technological Developments in Livestock Farms: A Literature Review*, 19 INT'L J. ENV'T RSCH. PUB. HEALTH 1, 2 (2022).

4. *See* Ashworth & Owens, *supra* note 1.

5. *Id.*

6. Nevin Dembiraş, *Precision Agriculture in Terms of Food Security: Needs for The Future,* X. INT'L BALKAN & NEAR E. SOC. SCI. CONG. SERIES – OHRID/MACEDONIA, Oct. 2018, at 308, 311.

measure the reactions of crops, fields, and animals.[7] In the US, precision agriculture has received much attention due to its potential to sustain food production by improving yields and profits, reducing production's adverse environmental effects, and enhancing food safety and transparency in the food system through the data gathered.[8]

Businesses constantly innovate, and new business processes are now primarily data-driven.[9] Precision farming illustrates this evolution, as digital technology helps farmers increase productivity.[10] The collected data is jam-packed with information about processes, operations, and tools.[11] That data can offer insight into how to increase productivity based on the experience of other agricultural centres.[12] Also, these data are timely benchmark indicators and can help economic development.[13] Consequently, it is essential to establish communication networks between players such as the US and the EU to extract maximum benefit from the data collected.[14]

Although it is not a distinct technical area, the digitisation of agriculture relays technologies that have emerged outside the agricultural industry and have created substantial legal concerns.[15] In the EU, precision farming is vital for ensuring sustainable food production but also raises questions regarding the conditions for collecting and processing farmer-related data as well as the responsibility of the individual farmer.[16] Indeed, the fast technological advancements in this traditional human activity need a review of EU law's capacity to deal with the significant legal difficulties that digitisation and automation of farming operations may offer in the coming years.[17]

Precision farming technology generates massive amounts of data and relies deeply on data interchange.[18] Therefore, actors such as the US and the EU must cooperate in sharing information since agricultural data is crucial for social and scientific progress.[19] The methodology adopted in the present work analyses the legal frameworks and case studies provided by the European Commission and the US Department of Agriculture.[20] Finally, the main objective is to study the need

7. *Id.* at 308-09.

8. *Id.*

9. Tim Punt et al., *Exploring Precision Farming Data: A Valuable New Data Source? A First Exploration*, STATS. NETH. 1, 1 (Oct. 9, 2019).

10. Dembiraş, *supra* note 6, at 308-09.

11. Punt et al., *supra* note 9, at 1.

12. Dembiraş, *supra* note 6, at 311.

13. Punt et al., *supra* note 9, at 1.

14. *Id.* at 7-8.

15. *See generally* Mihalis Kritikos et al., *Precision Agriculture in Europe: Legal, Social, and Ethical Considerations*, SCI. FORESIGHT UNIT, Oct. 2017, https://perma.cc/6PUY-KK3T (discussing the legal implications of precision agriculture in Europe).

16. *Id.* at 4.

17. *Id.* at 5, 14-15.

18. *Id.* at 5.

19. *See* Punt et al., *supra* note 9, at 8 (highlighting the importance of data harmonisation).

20. *See infra* Part II (surveying United States and European Union privacy laws and cooperation).

to regulate an agricultural communication network binding the EU and US to ensure progress in precision farming.[21]

II. NORTH AMERICAN PROCESSING OF EUROPEAN DATA

The United States, as a federation, does not have a legal framework for data protection.[22] Unlike the EU's General Data Protection Regulation ("GDPR"), no federal legislation protects the transfer of personal data.[23] However, in the US, several vertically established laws focus on privacy protection that applies to different sectors of the economy, including agriculture.[24] Many personal data processing laws concentrate on respecting the data subject's will.[25] More particularly, three states in the United States—California, Colorado, and Virginia—have enacted significant privacy laws.[26]

Out of these states, the California Privacy Rights Act of 2020 ("CPRA") is the initiative that comes closest to GDPR as it addresses the lawfulness of processing personal data for California residents.[27] The comparison between the CPRA and GDPR is quite interesting. These two legal instruments give consumers the right to access, delete, and object to processing their data at any time.[28] Previously, the California Code did not grant consumers the right to correct or rectify interpersonal date, but due to legislative updates in 2020, both the GDPR and CPRA grant such rights.[29] Also, it is essential to point out that the laws are similar in the process of obtaining consent, but the kind of processing that requires consent differs.[30] The CPRA is crucial in understanding Americans' reasoning for protecting personal data.[31] Given the lack of a comprehensive federal privacy law in the US, the CPRA is considered one of the country's most important pieces of privacy legislation in the US.[32] However, its scope is limited

21. *See infra* Part V (concluding that international cooperation must have a basis in privacy rights and the rule of law).

22. *See* CHARLES D. LINEBAUGH & EDWARD C. LIU, CONG. RSCH. SERV., R46724, EU DATA TRANSFER REQUIREMENTS AND U.S. INTELLIGENCE LAWS: UNDERSTANDING SCHREMS II AND ITS IMPACT ON THE EU–U.S. PRIVACY SHIELD 12-13 (2021) (recommending US actions to resolve data privacy concerns of the EU).

23. *Id.*

24. Jody L. Ferris, *Data Privacy and Protection in the Agricultural Industry: Is Federal Regulation Necessary?* 18 MINN. J.L. SCI. & TECH. 309, 326-29 (2017).

25. *Id.*

26. *Data Privacy Laws by State: Comparison Charts*, BLOOMBERG LAW (Feb. 2, 2022), https://perma.cc/FT4U-4WDB [hereinafter *Privacy Laws by State*].

27. 2020 Cal. Legis. Serv. Prop. 24 (West).

28. *See id.*; Commission Regulation 2016/679, 2016 O.J. (L 119) (EU).

29. *Compare* 2018 Cal. Legis. Serv. Ch. 55 (West), *with* 2020 Cal. Legis. Serv. Prop. 24 (West), *and* Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (illustrating that the CPRA and the GDPR give more rights to consumers than the California Consumer Protection Act did).

30. *Compare* 2018 Cal. Legis. Serv. Ch. 55 (West), *with* 2020 Cal. Legis. Serv. Prop. 24 (West), *and* Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (describing when consent is required).

31. Sam Pfeifle, *California Privacy Law: CCPA, CPRA, and Beyond*, OSANO (Aug. 24, 2022), https://perma.cc/8YM6-2CR3.

32. *See id.*

and confined to the southwestern US (although the expected impacts are global given California's status as a significant player in the global economy).[33]

To study large-scale transfers with critical implications for both the US and the EU, it is necessary to consider the frameworks and regulations of the US as a whole. Also, since it is crucial to consider the concerns of the data subjects, this study will need to focus on the points related to the agricultural industry. In the US, farmers' worries about how their farm data is used in some ways are like general consumer worries "about the security and privacy of data in the cloud."[34] While the risk of identity theft associated with some consumer data may not apply to farm production data, agricultural service providers may utilize production data to discriminate on price in addition to helping producers by supporting managerial decisions.[35] There are also worries that the regulations governing data sharing may hurt development of agricultural activities or the economic blossom of farming activities.[36]

A. THE PRIVACY SHIELD ISSUE

Following the cancellation of the Safe Harbour agreement system, by way of decision 2016/1250, the EU and the US government had concluded a new similar agreement.[37] This time it was the Privacy Shield.[38] On July 16, 2020, the CJEU issued a new decision in the case between Maximilian Schrems, the US social network Facebook, and the Data Protection Commission.[39] Popularly known as "*Schrems II*," this new judicial event invalidated the EU–US Privacy Shield with immediate effect, and validated, under certain conditions, the standard contractual clauses ("SCCs").[40] *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*[41] (the *Schrems II* case) comes into play to challenge the scope of US surveillance laws.[42] In four years, this is the second decision finding that US digital surveillance practices fail to respect the privacy and data integrity of foreign citizens, such as Europeans.[43]

The regulatory framework currently in force in the territory of the EU has a standard of data protection that is contrary to the reasoning seen in the surveillance

33. *Id.*; *Privacy Laws by State*, *supra* note 26.

34. Michael E. Sykuta, *Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data Services*, 19 INT'L FOOD & AGRIBUSINESS MGMT. REV. 57, 62 (2016).

35. *Id.*

36. *Id.* at 62-66.

37. DICKINSON, MACKAMAN, TYLER & HAGEN, P.C., *Schrems II Decision and its Inevitable Impact on US Companies Processing Data in EU*, JDSUPRA (July 20, 2020), https://perma.cc/5A7A-MTXT.

38. *Id.*

39. *Id.*

40. *Id.*

41. Case C-311/18, Data Prot. Comm'r v. Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020).

42. *Id.*

43. *Id.* ¶¶ 191-202; *Commission Implementing Decision (EU) 2016/1250*, COM (2016) 1250 final (July 12, 2016).

laws of the US.[44] That said, the CJEU's position pushes the US government to enter into a new agreement with the EU to replace the Privacy Shield and seek to balance digital surveillance practices and privacy rights.[45] Until such an agreement is reached, the decision will limit and potentially disable the mechanisms that US companies have relied on to transfer personal data from the EU to the US.[46]

One of the most critical points of *Schrems II* is that the CJEU invalidated the Privacy Shield legal framework.[47] The Privacy Shield was an agreement negotiated between the EU and the US with the objective of easing the transfers of personal data with commercial purposes.[48] It required companies and organizations participating in the program to comply with various data protection requirements and, in turn, assured participants that the transfer complied with EU requirements.[49] The Privacy Shield replaced Safe Harbour legislation from the 2000s, designed to regulate the transfer of personal data from the EU and the European Economic Area ("EEA") and mitigate their vulnerability in the wake of the Patriot Act.[50] It should be mentioned that such a US law offered the US government and its representatives the right to access all data stored on US shores, without a warrant, after September 11, 2001.[51]

The Safe Harbour and Privacy Shield were designed to address the fundamental difference between the US and EU views on data sovereignty, i.e., who has rights regarding personal data from Europe.[52] In addition, European law grants ownership of data to the individual under the "right to privacy" established by the European Convention on Human Rights so that personal communications are considered private, and an individual's data belongs to him.[53] In the US, on the other hand, private data belongs to the state because the nation's protection is much more important than that of the individual.[54]

The objective of the Privacy Shield was to promote transatlantic trade by offering data controllers and data subjects a level of protection for their private information and the possibility of appealing to the legal system in the event of a violation of their rights.[55] Legislation such as the Privacy Shield has been used to

44. DICKINSON, MACKAMAN, TYLER & HAGEN, P.C., *supra* note 37.

45. LINEBAUGH & LIU, *supra* note 22, at 12-13.

46. DICKINSON, MACKAMAN, TYLER & HAGEN, P.C., *supra* note 37.

47. LINEBAUGH & LIU, *supra* note 22, at 6.

48. *Id.* at 1.

49. *Id.* at 3.

50. *Id.* at 3, 5.

51. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001) (allowing the US government to access data of US citizens but subsequently amended to limit access by requiring investigation and application prior to ordering the production of information).

52. LINEBAUGH & LIU, *supra* note 22, at 3.

53. 2007 O.J. (C 303) 20.

54. *See generally* LINEBAUGH & LIU, *supra* note 22 (describing inadequacies of US data protection as it relates to EU regulations).

55. Case C-311/18, Data Prot. Comm'r v. Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 45 (July 16, 2020).

bridge the gaps between Europe and the US and has served to provide legal protection to companies that have joined it, enabling them to justify their transatlantic transfers of personal data from the US to the EU and vice versa.[56]

Schrems II invalidated the US–European Privacy Shield program that many US companies used to demonstrate compliance with EU data laws.[57] It left few options for US companies if they wanted to serve European customers.[58] The decision also affected agricultural goods' exportation and farming methods' research and development.[59] With *Schrems II*, the CJEU raised questions about legally permitted transfer methods.[60] The applicability of the remaining options is impractical and a problem on both sides of the Atlantic.

Finally, the CJEU invalidated the suitability of the Privacy Shield for data transfer security due to US surveillance laws.[61] Foreign Intelligence Surveillance Act ("FISA") section 702 and Executive Order 12333, even limited by Presidential Policy Directive-28, are too permissive to meet GDPR requirements and do not provide EU data subjects with an effective judicial remedy to appeal and safeguard their rights.[62] It should also be noted that the CJEU invalidated the Privacy Shield, but the Privacy Shield was not dissolved.[63] In a post-*Schrems II* context, companies can still display their compliance with the Privacy Shield to show their attention to protecting personal data.[64] This is especially true for the precision farming industry, where data is the core of this trade and technology.[65]

Digital technologies gather, store, integrate, and analyse copious amounts of agricultural data to foresee an occurrence, offer a solution, assist farmers in making better decisions, or develop automated systems to make strategic decisions or carry out tasks automatically.[66] Due to the sensitive nature of their operations, farmers might be personally recognized either directly, by name, email address, and location, or indirectly, by PII data on farming activities, for example.[67] As a result, when added to the data flow between the EU and US, the data related to precision farming must be treated cautiously since it falls under the purview of the data protection legislation.[68] Also, large amounts of data are necessary for the

56. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 770, 793-803 (2019).

57. *Data Prot. Comm'r*, ECLI:EU:C:2020:559, ¶ 201.

58. LINEBAUGH & LIU, *supra* note 22, at 6-7.

59. *See* DIGITAL EUROPE, SCHREMS II IMPACT SURVEY REPORT 3, 4, 8 (2020), https://perma.cc/RK5K-H3JP (describing Schrems II impact on research and development and listing the agricultural sector as an effected industry).

60. *Data Prot. Comm'r*, ECLI:EU:C:2020:559, ¶ 203.

61. Angelo A. Stio III et al., *The Impact of Schrems II on EU and US Cloud-Based Services*, EUR. AM. CHAMBER OF COM. (Aug. 13, 2021), https://perma.cc/3P8T-7XL6.

62. LINEBAUGH & LIU, *supra* note 22, at 8-12.

63. PRIVACY SHIELD FRAMEWORK, *Privacy Shield Program Overview*, https://perma.cc/2HET-BXM5 (last visited Jan. 24, 2023).

64. *Id.*; LINEBAUGH & LIU, *supra* note 22, at 3.

65. Jasmin Kaur et al., *Protecting Farmers' Data Privacy and Confidentiality: Recommendations and Considerations*, FRONTIER SUSTAINABLE FOOD SYS.: POL'Y & PRAC. REV. 1, 1-2 (Oct. 19, 2022), https://perma.cc/TG7S-X5SH (describing the importance of data collection to precision agriculture).

66. *Id.* at 2.

67. *Id.*

68. *Id.*

accuracy and dependability of many of the agricultural systems that make usage of information technology.[69] However, extensive data collection puts farmers at risk for privacy issues.[70] "[I]dentification, reputation loss, misuse of data, [lack of or limited control], social engineering, and unauthorized access to data" are some examples of privacy hazards.[71] When applied to civil data subjects such as farmers, information privacy is defined in various ways that address both technological and administrative facets of data processing.[72]

III. DATA PROTECTION IN EUROPE AS A FUNDAMENTAL RIGHT

In the case of Europe, data protection is a fundamental right enshrined in all the EU legal orders of founding treaties.[73] Indeed, Article 8 of the EU Charter of Fundamental Rights protects personal data and assures privacy by all means possible.[74] The right is extended to everyone within the scope of a said legal instrument, and the consent of the person concerned becomes one of the fundamental elements to ensure the legality of personal data processing.[75] Even in cases where individual consent can be waived, as in the case of a second legal provision, everyone has the right to access the data collected concerning them and to obtain rectification.[76]

Nonetheless, the current legislation regarding privacy security is more centred around personal data, with data subjects being private citizens in their daily lives. Sectors of the economy that are more specific industry sectors, such as agriculture, should be more directly concerned with meeting their needs. Consequently, farmers' privacy concerns have increased due to the lack of specific legislation or standards on farm data.[77] This is especially true for sectors highly dependent on gathering and handling data, such as precision farming.[78] Agricultural data is deserving of attention on the part of the legislator, no matter what side of the Atlantic, once its security has heavy implications for the data subject. In other words, the identification of farmers is one of the most significant privacy hazards since it could reveal private information without their knowledge, causing identity theft or reputation damage.[79]

The fact that personal data protection is a basic right recognized in the EU Treaties has significant ramifications for data transfers and, more broadly, for

69. *Id.*

70. *Id.*

71. *Id.*

72. *See id.* (citing Sebastian Linsner et al., The Role of Privacy in Digitalization—Analyzing Perspectives of German Farmers, PROCS. ON PRIV. ENHANCING TECHS. 334, 335-37 (July 2021)).

73. 2007 O.J. (C 303) 20 (describing a number of bases for Article 8's data protection provision).

74. *Id.*

75. 2000 O.J. (C 364) 10 (stating that "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned").

76. *Id.*

77. Kaur, *supra* note 65, at 2.

78. *Id.*

79. *Id.*

extraterritorial monitoring that extends outside of the EEA.[80] Therefore, this makes it feasible to use the universality of the soft law principle in the present case.[81] This means that, before European law, "the privacy or data protection laws of any state should apply to all processing of all personal data of all individuals whose rights [those related to personal data and privacy] are affected by actions of (private or public sector) entities under the jurisdiction of the relevant state, irrespective the individuals' nationality or status."[82]

The principle of universality in the application of remedies to protect against unlawful surveillance based on an alleged pretext of the fight against terrorism by the US was discussed in *Schrems II*.[83] This is because the US does not accept this principle of extraterritorial application of international human rights law or international human rights treaties on which it depends.[84] This point was proven by the Snowden case, which exposed the extent of the violations committed by the US under the guise of its surveillance laws.[85]

Under the GDPR, personal data can only be freely transferred from EU member states to countries capable of providing substantially equivalent protection to that provided on European soil.[86] Furthermore, the EU data exporter must adopt appropriate safeguards in line with GDPR principles.[87] It should be emphasised that this requirement does not apply as much as an imposition of legal obligations on private sector organizations or third countries.[88] It is up to the mission controller to secure and guarantee the processes for which he is responsible; it is also expected to meet communication obligations, which the GDPR has enforced.[89] The responsibility rests above all on the exporter since a duty of collaboration rests on the importer.[90]

Regarding *Schrems II*, the crux is whether the US offers personal data protection equivalent to the GDPR.[91] However, this is a separate but related issue. First, it is necessary to know if a US law, such as the Safe Harbour or the Privacy Shield, can provide such protection and if this legislation allows the authorities to

80. *See* 2007 O.J. (C 303) 20 (describing data protection and the free movement of data as a fundamental right); IAN BROWN & DOUWE KORFF, POL'Y DEP'T FOR CITIZENS' RTS. & CONST. AFFS., EXCHANGES OF PERSONAL DATA AFTER THE SCHREMS II JUDGEMENT 18 (2021), https://perma.cc/5RDD-4YT8.

81. BROWN & KORFF, *supra* note 80, at 18.

82. *Id.*

83. Case C-311/18, Data Prot. Comm'r v. Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 112 (July 16, 2020).

84. BROWN & KORFF, *supra* note 80, at 21.

85. United States v. Moalin, 973 F.3d 977 (9th Cir. 2020); *see also* LINEBAUGH & LIU, *supra* note 22, at 11 (describing the aftermath of the Snowden allegations).

86. 2016 O.J. (L 119) 19.

87. *Id.*

88. *Id.*

89. *Id.* at 20.

90. BROWN & KORFF, *supra* note 80, at 58.

91. *See* Case C-311/18, Data Prot. Comm'r v. Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 203 (July 16, 2020) (holding that third countries must afford essentially equivalent data protection as the GDPR).

access the personal data of EU persons only in the circumstances and under conditions that meet the standards of the European Data Protection.[92]

Although the countries of Europe have undertaken to ensure that the organizations which process the personal data of European citizens ensure an adequate level of data protection, the legal framework for this protection is limited by the requirements relating to national security, public interest, and compliance with applicable law.[93] It is also subject to the scope of national constitutions and the European Convention on Human Rights.[94] Further, the national security grievance exemption does not apply to the imposition of legal obligations on private sector organizations or third countries.[95]

A. GDPR AND INTERNATIONAL DATA TRANSFER

The GDPR, which came into force on May 25, 2018, and is current at this publication, is one of the world's most comprehensive personal data protection laws.[96] It coordinates the legal regime for protecting personal data, applicable to all EU nationals, companies, and subcontractors who reside within the perimeter of the EEA.[97] The GDPR also applies to all companies that offer services to EU nationals.[98] This legal instrument has an extraterritorial application and concerns data transfers to the US.[99]

Given the features of, and issues with, big data in agriculture described above, it is clear that both sides of the data equation are interested in establishing explicit property rights over agricultural production data and its use.[100] On following guiding principles for utilising and distributing data, several agricultural producers have reached an understanding on how to handle personal data.[101] The guiding principles established a shared approach to dealing with privacy issues and a dedication to continued communication as new technology and inherent difficulties emerge.[102] However, those principles are a source of soft law, and in the rule of law, they lack force when compared to hard law, such as the GDPR.

Moreover, in addition to the GDPR, which sets the general data protection framework, the EU has also adopted the directive of 27 April 2016, also known as the Police-Justice Directive, which addresses the processing of personal data in

92. LINEBAUGH & LIU, *supra* note 22, at 8.
93. BROWN & KORFF, *supra* note 80, at 30.
94. *Id.* at 8.
95. *Id.*
96. *See generally* 2016 O.J. (L 119) (protecting data privacy rights in the European Union and setting forth compliance requirements).
97. *Id.*
98. *Id.*
99. 2016 O.J. (L 119) 101.
100. Sykuta, *supra* note 34, at 66.
101. *Id.*
102. *Id.*

the criminal sphere.[103] These two texts are complementary and together constitute the "European personal data protection package" adopted as part of the strategy for a digital single market in Europe.[104]

When thinking about a unified market for Europe, it is also necessary to address its implications for the data subjects. Farmers' concerns about the handling of their data go beyond the ones of ordinary consumers, who are more concerned about their privacy, the risk that online merchants may charge them differently for the things they want to buy, and how those stores would utilize their data to develop new items and commercial strategies.[105] In addition to issues with personal privacy and worries that farm input suppliers might practice price discrimination for seeds and chemicals, farmers are worried about data aggregators using the data to gain an unfair advantage in the commodity and real estate markets, which has significant implications for the value of agricultural operations.[106] Although those are not specifically personal risks, they nevertheless illustrate concerns about the privacy of data that is collected in bulk and put to use.[107]

IV. THE *SCHREMS II* CASE

Following the cancellation of the Safe Harbour Agreement system, by Decision 2016/1250, the EU and the US government concluded a similar new agreement.[108] This time it was the Privacy Shield.[109] What followed suit was a legal debacle that began in 2013 with activist Maximilian Schrems's request that the Irish Data Protection Commissioner invalidate the SCC because Facebook was using it to send users' data to its US headquarters. Schrems argued that the law and practices within the US did not warrant adequate protection of the personal data held within its borders against the surveillance activities engaged by local public authorities such as the National Security Administration ("NSA").[110] Popularly known as "*Schrems II*," this new legal action invalidated the EU–US Privacy Shield with immediate effect and validated, under certain conditions, the SCCs.[111] The SCCs became crucial in regulating data transfers between the EU and US. In the following graphic,[112] it is possible to see that three percent of the

103. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, LE CADRE EUROPEEN (2022), https://perma.cc/Y9FC-SK3B.

104. *Id.*

105. Sykuta, *supra* note 34, at 64-65.

106. *Id.*

107. *Id.* at 65.

108. LINEBAUGH & LIU, *supra* note 22, at 3.

109. *Id.*

110. Case C-311/18, Data Prot. Comm'r v. Maximillian Schrems, ECLI:EU:C:2020:559, ¶¶ 1-2 (July 16, 2020).

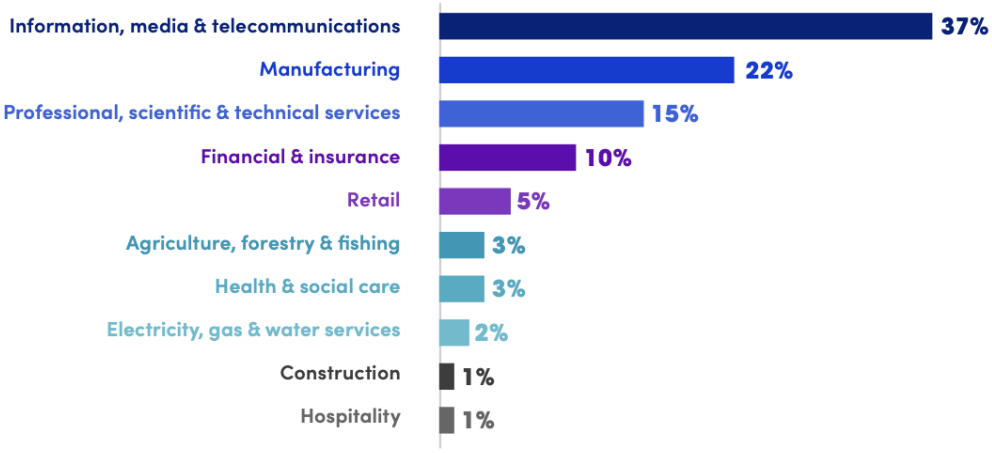
111. LINEBAUGH & LIU, *supra* note 22, at 1.

112. DIGITAL EUROPE, SCHREMS II IMPACT SURVEY REPORT 3, 8 (Nov. 26, 2020), https://perma.cc/RK5K-H3JP.

agricultural industry relies on SCCs for their data transfers and, consequently, was deeply affected by the *Schrems II* judicial case:

JUST ABOUT ALL INDUSTRY SECTORS RELY ON SCCs FOR THEIR TRANSFERS OF PERSONAL DATA

Figure 3: % of respondents by sector, amongst SCC users



Source: DIGITALEUROPE I Base: estimated SCC users (n = 249)[7]

After *Schrems II*, the Data Protection Commission ("DPC") investigated Facebook Inc.'s new practices for protecting personal data.[113] The Irish social network base explained that SCCs supervised many transfers it made to the US.[114] In response, Maximilian Schrems maintained that adopting SCCs did not compensate for the lack of adequacy of US surveillance laws since these devices did not bind American public authorities.[115] Faced with such reasoning, the DPC seized the High Court of Ireland to determine whether the SCCs should be invalidated.[116] In turn, the Irish Court of Justice seized the CJEU with a series of questions for a preliminary ruling.[117]

At first, the problem raised by *Schrems II* is relatively easy to understand. Suddenly, and overnight, a significant amount of cross-border processing of personal data changed status.[118] Transfers that were taking place in some of the most dynamic cross-border flows in the world suddenly went from "compliant" to

113. Caitlin Fennessy, *'Schrems II' DPA Investigations and Enforcement: Lessons Learned*, INT'L ASS'N PRIV. PRO. (June 17, 2021), https://perma.cc/PX4F-YRKT.
114. *Data Prot. Comm'r*, ECLI:EU:C:2020:559, ¶¶ 54, 74.
115. *Id.* ¶¶ 54-57.
116. *See* Fennessy, *supra* note 113.
117. *Data Prot. Comm'r*, ECLI:EU:C:2020:559, ¶ 68.
118. *Id.* ¶¶ 197-201.

"non-compliant" regarding the legal requirements in force in the European territory.[119]

To deal with this situation, the CJEU referred to Article 49 of the GDPR, specifying that the said legal provision allows the absence of "the creation of a legal vacuum."[120] This article lists derogations from the general mechanisms that regulate cross-border data transfers.[121] Nevertheless, the interpretation given to this article by the supervisory authorities has always been quite restrictive, making it almost unusable by confining it to "occasional" transfers.[122] Therefore, the various market players find themselves deprived of the possibility of continuing the transfers which existed before, under the aegis of legality, July 16, 2020.[123]

After the *Schrems II* judgment, the various market players awaited the position of the supervisory authorities to know the main guidelines on the interpretation and practical applications of the new CJEU decision.[124] The problem arising from *Schrems II* is understanding how it affects transfers of personal data with the US and how they will be regulated.[125] Without the legal support of the Privacy Shield, there is still practical work to be carried out to know how to operationally process the transfer of data from a company responsible for the personal data of Europeans but needing to have recourse to a US contact or to a subsidiary and to store or process personal data.[126]

Considering this new paradigm of personal data protection handling, it is necessary to think about how sectors of society are adapting to the new regulation. Thus, several conventional agricultural input providers have attempted to create data services to gain a piece of the promised value.[127] Big data analytics is being used to provide farm-specific decision support tools in a competition between John Deere, one of the industry leaders in providing data-generating technologies on their farm machine equipment, and Monsanto and DuPont Pioneer, which jointly control most of the US's corn and soybean seed markets.[128] Monsanto predicted that the market for data science in agriculture could be worth up to twenty billion dollars when it announced its acquisition of The Climate Corporation in 2013.[129] The Climate Corporation is an atmospheric data science company that creates micro-weather forecasts to help farmers make management decisions.[130]

---

119. *Id.*

120. *Id.* ¶ 202.

121. Commission Regulation 2016/679, art. 49, 2016 O.J. (L 119) 64, 65 (EU).

122. Elisabeth Deharegn, *Data Transfer: Derogations for Specific Sitioations (Art. 49 GDPR)*, BAKER MCKENZIE (Mar. 11, 2020), https://perma.cc/B5UR-7QBB.

123. *Data Prot. Comm'r*, ECLI:EU:C:2020:559.

124. Romain Boucq, Free Speech on the Decision of the Council of State of October 13, 2020 Relating to the Health Data Platform, DALLOZ (Oct. 21, 2020), https://perma.cc/XP3M-78XU.

125. *Id.*

126. *Id.*

127. Sykuta, *supra* note 34, at 58.

128. *Id.*

129. *Id.*

130. *Id.*

A. REPERCUSSIONS OF THE *SCHREMS II* RULING

The CJEU interprets European legislation to guarantee its uniform application in all countries belonging to the EU. This court is also responsible for adjudicating legal disputes between member state governments and EU institutions. In the *Schrems II* case, the Irish supervisory authority brought an action before the High Court of Ireland to refer the application to the Court of Justice, seeking a preliminary ruling.[131] Thus, the *Schrems II* judgment has significant repercussions since the decisions of the CJEU are binding and enforceable on the territory of the member states.[132]

Furthermore, in the *Schrems II* judgment, the CJEU examined Decision 2010/87 through the EU Charter of Fundamental Rights, which revealed nothing that could affect the validity of this decision.[133] Therefore, the court affirmed that its reasoning did not represent an infringement of fundamental human and civil rights in US surveillance laws.[134] However, the court invalidated decision 2016/1250, and even without being explicit, recognized that the US surveillance laws constitute an infringement of fundamental rights.[135]

Schrems II was also essential to spread awareness about the importance of cybersecurity when transferring personal data. The protection of farmers' privacy is an important element to be taken into consideration when discussing data security.[136] Proactive measures must be taken to monitor for data leakages, loss, unauthorized access or use of personal information, deletion, alteration, and incorrect disclosure to protect the security of the farmers' data.[137] One tactic that can be used in this regard is to look for potential vulnerabilities and system problems.[138] Training employees on privacy protection, threat monitoring, and intrusion detection is also another strategy that might assist with this.[139] Another measure to be put in place is the adoption of end-to-end data encryption. This will help ensure that only the right recipient receives the information.[140] Finally, using network security and two-layer authentication as supplementary cybersecurity measures can help to protect farmers' privacy rights.[141]

In the EU, *Schrems II* reflected that the farmer should control who has access to and uses their data. For instance, the farmer is awarded ownership of the data

131. Case C-311/18, Data Prot. Comm'r v. Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 53 (July 16, 2020).
132. *See id.* ¶ 203.
133. *Id.*
134. *Id.*
135. *Id.*
136. Kaur, *supra* note 65, at 5.
137. *Id.* at 5-6.
138. *Id.* at 6.
139. *Id.*
140. *Id.*
141. *Id.*

created on the farm or during farming activities and can utilize it wisely.[142] Generally, unless otherwise stated in the contract, the data originator has the right to transfer the agricultural data to another user.[143] Where technically possible, and as agreed by the parties, the data originator should have the right to request that the data be sent directly from one data user to another.[144]

1. Repercussions in the United States

The *Schrems II* case has instilled doubt in European companies and those subject to the laws of the US.[145] The CJEU struck down the European Data Protection Board's decision establishing the adequacy of the Privacy Shield, highlighting the conflict between US surveillance and EU data protection laws.[146] This judgment caused significant repercussions, as over 5,000 companies in the US use the Privacy Shield framework to process and transfer EU data.[147]

The NSA has established surveillance programs, such as PRISM,[148] which may infringe on the fundamental rights of European citizens. One of the issues raised in this regard has been the lack of effective judicial review and remedies to protect data from Europe.[149] This point undermined the Privacy Shield as a valid mechanism to regulate data transfer.[150] Following the reasoning presented in the *Schrems II* ruling, the most appropriate solution for the US would be a federal law to protect data privacy, like the GDPR. In this way, the US would more easily be considered an adequate jurisdiction to process European data.

Furthermore, the CJEU has retained the validity of mechanisms such as SCCs, but these are insufficient as the only legal basis for data transfers across the Atlantic.[151] Contractual arrangements only bind individual signatories; they cannot create a legal "fit" for the whole of the US with the same level of protection offered by the GDPR.[152] *Schrems II* involved a review of the adequacy of the overriding mechanisms for protecting personal data.[153] This new scenario has forced American technology giants to adapt to continue their business

142. EUROPEAN COMPOUND FEED MANUFACTURERS' FEDERATION ET AL., EU CODE OF CONDUCT ON AGRICULTURAL DATA SHARING BY CONTRACTUAL AGREEMENT 8 (July 2020), https://perma.cc/PA4N-SBNC.

143. *Id.* at 9.

144. *Id.*

145. DICKINSON, MACKAMAN, TYLER & HAGEN, P.C., *supra* note 37.

146. *Id.*

147. *Id.*

148. Case C-311/18, Data Prot. Comm'r v. Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 61 (July 16, 2020).

149. *Id.* ¶¶ 65, 191.

150. *Id.* ¶ 168.

151. DICKINSON, MACKAMAN, TYLER & HAGEN, P.C., *supra* note 37.

152. See *id.* (explaining how SCCs alone would be insufficient data privacy protections between the EU and US).

153. *Id.*

operations.[154] Such was the case with the company behind the *Schrems II* debacle, Facebook.[155]

Like other companies, Facebook relies on SCCs to transfer data outside the EU and into the US.[156] Since *Schrems II*, Facebook claims to be making efforts to adapt and follow the steps established by the CJEU to continue to transfer personal data in a way that complies with the principles of the GDPR.[157] These efforts include implementing technical safeguards, policies, and legal initiatives governing how Facebook responds to requests for information from public authorities, such as the US government.[158] Going beyond advocating for a US-based federal data privacy law, Fabrice Naftalski, Ernst & Young Global Head of Data, says:

Following the Schrems II decision, some SAs declared any data transfer to the US to be illegal, and called for caution and minimization of transfers. The European Data Protection Supervisor (EDPS), tasked with safeguarding the EU's own data protection policies and compliance (pdf), also called on the EU institutions to "to avoid processing activities" that involve transfers of personal data to the US and instructed the EU institutions to complete "a mapping exercise identifying which on-going contracts, procurement procedures and other types of cooperation involve transfers of data." At the same time, other SAs noted that Schrems II validated the use of SCCs as a transfer mechanism, providing that additional measures were implemented.[159]

V. CONCLUSION

Intelligence agencies worldwide, including those in constitutional democracies, operate, concerning the processing of foreign data, outside a framework of the primacy of the democratic rule of law.[160] The European Court of Human Rights and the CJEU clearly announced that this was unacceptable.[161] This issue can be resolved in a manner consistent with the international rule of law if the activities of these bodies are fully integrated into a legal framework consistent with the rule of law.[162]

Precision agriculture cannot succeed without the vast amounts of data that big data technologies can collect and interpret from data subjects.[163] The requirement for data confidentiality and privacy has presented its own set of

154. *Id.*

155. *Id.*

156. Nick Clegg, *Securing the Long Term Stability of Cross-Border Data Flows*, META (Sept. 9, 2020), https://perma.cc/FVT8-BZWA.

157. *Id.*

158. *Id.*

159. Fabrice Naftalsk, *What are the Main Trends in Regulatory Responses to Schrems II*, EY (Mar. 31, 2021), https://perma.cc/EA5H-6VNA.

160. BROWN & KORFF, *supra* note 80, at 11.

161. *Id.*

162. *Id.*

163. Kaur, *supra* note 65, at 8.

challenges for the agricultural sector.[164] The issues include, among others, a lack of appropriate legal frameworks, legislation, and contractual obligations, as well as a lack of standards and best practices for the protection of agricultural data.[165] Farmers are reluctant to share data or even use new technologies due to these problems and the limited adoption of privacy best practices by agricultural technology providers and other supply-chain partners.[166]

That said, case law such as *Schrems II* is necessary in order, in the Internet era, to protect the citizen against the arbitrariness of institutions and governments. Nevertheless, case law advances should be straightforward and provide practical guidance on how to protect privacy.

164. *Id.*
165. *Id.*
166. *Id.*