University of Baltimore Journal of International Law

Volume 6 | Issue 1 Article 9

2018

# In the Face of Brexit, the United Kingdom Has No Choice but to Provide Data Protection for Individuals, Organizations and Law Enforcement Agencies by Updating Their Legal Framework, which is Based Upon a 20-Year-Old Act.

Logan Hayes

# In the Face of Brexit, the United Kingdom Has No Choice but to Provide Data Protection for Individuals, Organizations and Law Enforcement Agencies by Updating Their Legal Framework, which is Based Upon a 20-Year-Old Act.

**Logan Hayes**

## Introduction

The United Kingdom currently relies upon the Data Protection Act of 1998 (DPA 1998) to set the legal framework for the protection of data.[1] That act is nearly 20-years-old and should be updated to echo the way in which data is now used and generated in an ever-evolving digital world.[2] Due to Brexit, there is a need to protect data through stronger laws governing data protection that will also set up appropriate safeguards.[3] The Data Protection Bill, introduced to the House of Lords on September 13, 2017 has the potential to do just that.[4] Not only does this Bill have the potential to set new standards for data protection, but it can provide people with more control over their data, including rights to either move or delete personal data, all while assisting both law enforcement and intelligence services in the protection of rights of witnesses, suspects, and victims.[5]

1. DEPT. FOR DIGITAL, CULTURE, MEDIA AND SPORT, *Data Protection Bill: summary assessment*, 1 (July 9, 2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644636/2017-09-12_Data_Protection_Bill_IA_final.pdf.
2. *Id*.
3. *Id* ("With the increasing volumes of personal data held by businesses and government there is an increasing need to protect and to create strong data protection laws and appropriate safeguards. The Bill will do this and also ensure that, following the UK's exit from the EU, our criminal justice agencies can continue to share data with other EU Member States to tackle crime and threats to our security.").
4. DEPT. FOR DIGITAL, CULTURE, MEDIA AND SPORT, https://www.gov.uk/government/collections/data-protection-bill-2017.
5. *Data Protection Bill: summary assessment*, *supra* note 1.

## Background

Currently, personal data is protected in the United Kingdom under the DPA 1998.[6] Within the past 20 years several major technological developments have occurred, including the emergence of social media, the growing importance of smart phones, and the rapid expansion of the internet.[7] In January 2012, the European Commission proposed the General Data Protection Regulation (GDPR) and Data Protection Directive "(commonly known as the Law Enforcement Directive (LED))," which aimed to give citizens more control over their personal data.[8]

The LED intends to give consistent high level protection of data in order to enable better data sharing between authorities of EU Member States.[9] The LED seeks to establish "an equal level of protection to the rights and freedoms of natural persons across the EU and to remove barriers to data sharing that occur where different countries apply different standards of protection."[10] The Data Protection Bill was announced on June 21, 2017 in the Queen's Speech as a commitment to update previous data protection laws to prepare the United Kingdom for Brexit.[11]

## Thesis and Analysis

In their efforts to address the legal framework for data protection in light of Brexit, the United Kingdom has identified two policy options: do nothing, or create new law.[12] If new law is not created, chaos and disorder will erupt as contradicting laws will be enforceable without anyone knowing which is the ultimate law.[13] The accountability for

6. *Data Protection Bill: summary assessment*, *supra* note 1 at 2.
7. *Id* ("The UK is at the forefront of data innovation and the UK data economy continues to grow in both size and significance . . . in order to guarantee the UK's continued growth and prosperity, and maximize future trading opportunities, it is crucial that we are able to guarantee effective, unrestricted data flows.").
8. *Id*.
9. *Id*.
10. *Id*.
11. DEPT. FOR DIGITAL, CULTURE, MEDIA AND SPORT, *Data Protection Bill: Fact Sheet - Overview*, 2 (Sept. 13, 2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644634/2017-09-13_Factsheet01_Bill_overview.pdf
12. *Data Protection Bill: summary assessment*, *supra* note 1.
13. *Id* (If they were to do nothing, "The EU General Data Protection Regulation (GDPR), as a directly applicable regulation, would apply in the UK but so too would the 1998

lack of proper data protection would be nearly nonexistent and unenforceable. By doing nothing, the government would be unable to meet their objectives because they become subject to both the GDPR and the DPA 1998.[14] This results in legal chaos for both individual citizens and organizations in applying the law.[15]

By creating a new legal framework for data protection, the government could incorporate the GDPR and transpose the LED to fit the best interests of the United Kingdom.[16] The latter option would be the most beneficial to the United Kingdom, more specifically in the following areas: protecting individuals, protecting organizations, tougher regulations, and an adapted regime for law enforcement.[17]

The United Kingdom aims to "protect privacy, strengthen rights and empower individuals" by granting easier access to their private data and therefore, more control over said data.[18] With stronger rules regarding consent to access of private data, individuals will have more control over their "digital footprint."[19] Having more control over their footprint would allow individuals to have protection in the modernized world where every answer is a simple search away. Stronger laws would also grant people with the option to decide how much private information is available about the person within the digital realm. This option is invaluable in a world where everything is a search or click away. People not only get to control how the world perceives them, but also how much the world is able to learn about them.

New and improved access to private data would make it even easier for individuals to determine what information an organization may have on file about themselves.[20] Individuals will be empowered to take ownership over their data. They can also decide whether they wish to

Act, causing legal uncertainty and confusion for both individuals and organizations in applying the law.").

14. *Id*.
15. *Id*.
16. *Id*.
17. DEPT. FOR DIGITAL, CULTURE, MEDIA AND SPORT, *A New Data Protection Bill: Our Planned Reforms*, 8-11 (Aug. 7, 2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_Statement_of_Intent.pdf.
18. *A New Data Protection Bill: Our Planned Reforms*, *supra* note 16 at 8.
19. *Id*.
20. *Id* ("Personal data is information that is attributable to an individual and may help to identify them." The new bill "will expand the definition of 'personal data', reflecting the growth in technology over the past 20 years to include IP addresses, internet cookies and DNA.").

alter information about themselves or have it removed entirely. This would cause no harm to citizens of the United Kingdom because the government would still have access to their information as well as the ability to keep it on file.

This bill ensures that citizens can determine what entities may be allowed to access private data about themselves. The deletion of data provides citizens with more security, knowing that their private information is being handled by the strongest legal and governmental framework. By streamlining the discovering what private data is on file, the government provides individuals the security that certain information about them will not be stolen or used against them. Allowing citizens to decide what private information is processed and stored would increase their faith in the organizations with which they regularly conduct business. This would improve the economic sector as it would make sense for individuals to work with business and government bodies whom they trust to maintain or delete certain data about them.

The removal of information is dubbed "the right to be forgotten," meaning that individuals will be allowed to ask for personal data on themselves to be erased.[21] This provision of the bill includes the ability to require social media platforms to remove any information posted by an individual during their adolescence.[22] By deleting posts, people could have more job opportunities. There is a safety in knowing that individuals will not have immature posts hanging over their head throughout the rest of their lives. This also means that citizens will not have to worry about organizations being able to find old pictures or posts that they could ultimately try to use against them. Individuals can achieve peace of mind knowing that their data would not be used with bad intentions. Through the deletion of these types of posts, individuals will have even more control over how they are profiled through

21. *A New Data Protection Bill: Our Planned Reforms*, *supra* note 16 at 9.
22. *Id* (The new bill would widen "the existing 'right to be forgotten', including the right for individuals to obtain erasure of personal data relating to them and the abstention from further dissemination of such data. The principle difference is a strengthening of the law from being applicable when substantial damage or distress is likely to be caused, to whenever a data subject withdraws their original consent for the data to be available, as long as it is no longer necessary or legally required for the grounds on which it was originally collected, or there are no overriding legitimate grounds for processing.").

automated processing.[23] This sort of choice promoted the concept of "data portability" that is supported by the bill.[24]

Data portability would increase as new laws and make it simpler for customers to transfer their data between various service providers.[25] Individuals would have more control over what information is retained within each data processor. Businesses of all varieties would have the opportunity to expand their clientele by offering individuals with a sense of security and peace of mind that their data is securely being sent from one service provider to another. With potential economic growth being a result of increased individual data protection, it is also important that organizations are afforded data protections of their own.

By protecting organizational data, the bill would build accountability on behalf of data controllers.[26] Ideally, new laws would lessen both financial and administrative burdens on data controllers with the expectation that controllers would have more accountability for their actions.[27] Under the new bill, businesses would have 72 hours to notify the Information Commissioner's Office (ICO) of a breach.[28] This ensures that all organizational data, which can include stored individual data, is handled with the utmost care in breach situations. Not only does this benefit organizations, but it also benefits citizens themselves in making sure that all parties involved are as secured as possible. The new bill would also insure that in instances where there is a high risk, the businesses would have to notify the affected individuals themselves.[29]

The new bill aims to reduce the exposure to business oriented data protection breaches as well as reputational damage and associated fines.[30] This will be done by placing additional requirements on organizations to keep up with the high demand of an evolving digital world.

23. *Id*.
24. *Id*.
25. *Id* ("This not only gives consumers greater choice, but will promote competition and innovation in a range of sectors.").
26. *Id* (Organizational data being the stored information about an organization such as its structure, processes and defining characteristics. Private data is the stored information relevant to specific individuals that is not available to the public such as names, financial information, addresses and passwords.).
27. *Id*.
28. *Id*.
29. *Id*.
30. *A New Data Protection Bill: Our Planned Reforms*, *supra* note 16 at 10.

Any organization utilizing high risk data processing will be required to perform an impact assessment.[31] The goal here is to help organizations understand the risks involved in their data processing as well as to mitigate potential inappropriate usage.[32] By doing these risk assessments, organizations will be made aware of potential issues that may arise. This would result in appropriate plans being set in place to address those situations should they ever occur. This benefits individuals by requiring organizations to prioritize personal privacy rights while handling personal and private data.[33] As previously stated, when organizational data is protected, it ensures that any personal private data involved will be handled adequately and in accordance with the proposed bill. The bill would ensure that these goals are met by providing organizations with clearer, more concise rules. These rules are more fair to data controllers and processors to ensure they are aware of data handling expectations.[34]

Through the ICO, the designated data protection regulator, the Information Commissioner would gain the authority to impose greater sanctions on organizations in the event of a data breach.[35] From this power comes the ability to perform investigations.[36] The ICO will be able to "request information from data controllers and processors, enter and inspect any premises, carry out audits and require improvements."[37] It is up to the Information Commissioner to determine when or if these sort of inspections are to be made. If these inspections were to result in fines, the proposed bill would allow larger fines of up to £ 17 million (€ 20 million) or 4% of global turnover for the organization.[38] The larger fines would ensure that organizations handle both their data and private data with the utmost care. This would grant the ICO the ability to respond to serious data breaches in a more proportionate manner than what is currently allowed (the current maximum is £ 0.5 million).[39]

31. *Id* (As a sort of "trade off" the rules that organizations must follow will be consolidating into a simpler system).
32. *Id*.
33. *Id*.
34. *Id*.
35. *Id*.
36. *Id*.
37. *Id*.
38. *Id*.
39. *Id*.

While the possible repercussions of civil sanctions are expanding, so are the possibilities of criminal sanctions. The ICO will continue to process offenders, but the most serious offences will become recordable.[40] This ensures that those tasked with data protection would follow the new law rather than risk their mistakes being recorded. The bill also aims to modernize offenses to "ensure that prosecutions continue to be effective" as well as create "new offenses to deal with emerging threats."[41]

There are several new offenses that would be generated if this bill were to pass. A new offense of "intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data" would be introduced.[42] Anyone who knowingly handles or processes such data will be found guilty and subject to a maximum penalty of an unlimited fine.[43] Another new offense would be "altering records with intent to prevent disclosure following a subject access request," applying to both public authorities and all data controllers and processors.[44] The maximum penalty for this offense would be an unlimited fine in England and Wales or the maximum fine in Scotland and Northern Ireland.[45] An expansion of an existing offense would be "unlawfully obtaining data to capture people who retain data against the wishes of the controller."[46] The new bill will also afford greater protection to whistleblowers and journalists because they play an important role in holding organizations accountable. [47]

This bill will play a different role in the law enforcement system. It will create an adapted framework to increase access to shared information in order to "protect the public and fight crime."[48] The challenge

40. *Id* ( By allowing offenses to become "recordable," this means that they can be disclosed as part of previous conviction or criminality checks).
41. *A New Data Protection Bill: Our Planned Reforms*, *supra* note 16 at 11.
42. *Id*.
43. *Id* (Another new offense would be "altering records with intent to prevent disclosure following a subject access request," applying to both public authorities and all data controllers and processors).
44. *Id*.
45. *Id*.
46. *Id*.
47. *Id*.
48. *Id* ("Criminal justice agencies require a data protection framework that continues to allow them to tackle the changing nature of the threats [they] face – without compromising the world class data protection standards we expect.").

here lies in adapting the data protection framework without compromising "world class data protection standards" that are expected.[49]

The bill offers several new proposals on how to successfully implement the bill into law enforcement agencies. The first of which is the requirement of a Data Protection Officer in every agency/department.[50] This new role ensures that data controllers are being advised, complaints are being handled and that the law enforcement agency is complying with the Data Protection Law Enforcement Directive.[51] This will protect the public by making sure private information is properly maintained and protected by law enforcement agencies.

The proposed bill would also assist in international transfers so that vital data sharing can take place between different agencies.[52] This would help law enforcement agencies fight crime because information will easily flow between different countries and agencies. If the proposed bill works as the government intends, law enforcement agencies will be able to protect individuals and fight crime through the protection and secured flow of private data.

## Conclusion

In the face of Brexit, the United Kingdom finds itself at a crossroads on how to best move forward, while still affording both individuals and organizations with the data protection needed to keep them safe. If the new Data Protection Bill is passed, it would adapt older data protection laws (the GDPR and LED) while providing new protections needed in today's digital world. If data protection laws are not updated to reflect the modern world, the United Kingdom runs the risk of exposing their citizens and organizations to data breaches, dismantling both the economy and law enforcement agencies. The passing of this bill guarantee individual control, organizational accountability, and an increased flow of data between law enforcement agencies. Although the bill is 20-years-old, it would not be too difficult to modernize it. This bill would offer the United Kingdom the opportunity to stand tall after Brexit while providing the legal framework on how to

49. *Id*.
50. *Id*.
51. *Id* (Additionally, there will be "a more prescriptive logging requirement applied to specific operations of automated processing systems including collection, alteration, consultation, disclosure, combination and erasure of data, so a full audit trail will be available.
52. *Id*.

protect the data individuals, organizations, and law enforcement agencies.