

# Brexit and Software Safety



**Dai Davis, is a Technology Lawyer with his own specialist law practice, Percy Crow Davis & Co. For over three decades, Dai has been practising in high-tech product safety, including advising on safety related software, CE Marking and product recall. In this article, Dai discusses the impact Brexit has had on three important areas of law dealing with software safety.**

I recall reading years ago about what the writer said was the first recorded death caused by software, or perhaps I should say, badly programmed software. It was the story of an unfortunate worker in a car factory in New York State in the early 1960's being welded to death by an automatic robot welding machine. This was not a pleasant death, I imagine. Incidentally, if anyone has more details of this or another "first recorded death by software" story, I would be pleased to hear it.

It has taken a long time to see snippets of law, and they are only snippets of law, deal specifically with software safety, but interestingly those that are found in law are changing after Brexit. In this article I will discuss three areas of divergence in a post Brexit world:

- CE Marking which governs product safety
- the freedom of the United Kingdom to make new un-harmonised law, the example I will use is of car charging port legislation
- database rights.

For each of those areas I will explain the changes and the link to safety related software.

## European Union Product Safety Legislation

Software is found in a multitude of products. In the European Union, as part of what was then called the “1992 process”, freedom of movement of goods was introduced. In practice it was later in the 1990’s before much of the necessary European legislation came into force. The primary legislation underpinning this process is the “CE Marking” legislation, which requires most, though not all, products to bear the “CE Marking” and adhere to certain qualitative criteria.



The United Kingdom has taken many steps to ensure that appropriate changes were made to legislation in the United Kingdom to smooth the transition to Brexit. For political reasons, the European Union did not take the equivalent steps. Therefore, in almost all areas affecting commerce, we have what is commonly termed a “hard Brexit”.

The area covered by the CE Marking Directives is a good example of the effect of this hard Brexit. The United Kingdom amended the CE Marking legislation by the “Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019” regulations [1], which run to some 793 pages. The European Union made no changes to its equivalent legislation. As a result, this means, for example, that we now have two<sup>1</sup> entirely separate CE Marking regimes, one for the United Kingdom<sup>2</sup>, the other for the European Union.

One of the requirements of the CE Marking Directives is that a manufacturer must meet the appropriate standards. There is a hierarchy of standards:

- if there is a European standard formally adopted by the European Union, that standard must be followed
- otherwise the relevant international standard (if there is one)
- otherwise the relevant national standard.

However the hierarchy now to be followed in the United Kingdom is:

- if there is a British standard formally adopted by the United Kingdom government, that standard must be followed
- otherwise the relevant international standard (if there is one)
- otherwise the relevant (not formally adopted) British national standard.

At the moment there are no significant differences in these hierarchies of standards. Furthermore, the British have always pulled far beyond their national weight when it comes to influencing both European and International standards. The United Kingdom has also been allowed to retain its seats on the European standards making bodies: CEN and CENELEC. While eventually there will be divergences between the United Kingdom and European Union standards regimes which underpin the CE and UKCA Marking legislation, those differences will take a long time to come to the fore.



<sup>1</sup> Actually, this is incorrect, as we will have three regimes: one for Great Britain, another for Northern Ireland and a third for the European Union. However, a discussion of the special regime for Northern Ireland and the associated UKNI Marking is outside the scope of this article.

<sup>2</sup> In the United Kingdom the product will, if it is placed on the market on or after 1 January 2023, need to bear the UKCA Marking rather than the CE Marking.

Importantly, the Electromagnetic Compatibility legislation requires that electronic equipment meets qualitative criteria to ensure that it does not unduly emit electromagnetic interference and that it is immune from undue influences from external electromagnetic sources. Since software must reside on an electronic device, that means that the device must comply with that legislation. Having said that, there are no explicit provisions in the Electromagnetic Compatibility legislation dealing with software. However, that is not the same in respect of all the CE Marking legislation. In particular, the Machine Safety legislation and the Medical Device legislation both contain explicit provisions regarding software. By way of example I look at the former in detail below.

## Machine Safety legislation

There are two basic requirements which must be satisfied in order to comply with the Machine Safety legislation. First, the legislation contains a list of specific attributes that must be satisfied, second, the relevant machine must satisfy the appropriate standards.

Annex 1 of the machine safety legislation contains a list of those specific attributes<sup>3</sup> and clause 1.2 of the Annex contains the following reference to software:

*"Safety and reliability of control systems: Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that ...*

- *a fault in the hardware or the software of the control system does not lead to hazardous situations, [and]*
- *errors in the control system logic do not lead to hazardous situations, ...."*

In addition, where machinery includes a "logic unit to ensure safety functions", a higher level of certification procedure is sometimes required by the legislation.

Ultimately the United Kingdom and European Union interpretation of this identical legislation will change. That will also affect software safety. For example, there have been previous unsuccessful attempts in the United Kingdom to require that safety-related software is written only in approved software languages. If there are such attempts in the future, it would be much easier for them to succeed since they would not need also to be adopted by the remainder of the European Union. The formation of the new UK Cyber Security Council is a good example of the direction in which the United Kingdom is travelling.

## Legislation specific to the United Kingdom



Previously the United Kingdom has been unable freely to legislate in many areas of law. Now, after Brexit, it has much greater freedom to do so. An example of United Kingdom specific legislation appearing, which would not have been as easily adopted if the United Kingdom had remained within the European Union, is the Electric Vehicles (Smart Charge Points) Regulations 2021 [2].

<sup>3</sup> Referred to in the legislation as "Essential Health and Safety Requirements".

Schedule 1 to those Regulations, which must be complied with where a charging point is sold on or after 31 December 2022, imposes (partly software) security requirements for those charging points.

While a full discussion of the relationship between software safety and software security is outside the scope of this article, suffice to say that one cannot have one without the other. By way of example, the charging point must be configured so that the software can be securely updated<sup>4</sup>. One danger if this does not occur could be that the charging point, particularly since some charging points come with large external electricity storage devices, becomes incompatible with the local electricity grid and damages it. While human injury might be relatively fanciful in this example, software safety is not, in law, limited only to injury to humans. Safety in law includes safety to goods, and electricity is goods for these purposes<sup>5</sup>.

## Database Rights

A less direct interaction between Brexit and software safety is in the field of databases. These days the boundary between what is software and data has become increasingly blurred. At one level, one can regard any safety related software as merely data, since it is data which is input into a compiler to produce executable code<sup>6</sup>. An obvious example of a safety related database would be a database in a hospital storing patients' blood types or allergies. Correspondingly, a software program to store, retrieve and manipulate data in that database would be safety related.

Databases are protected by a European Union database right. Unlike most other intellectual property rights, which are based on international conventions, database rights are a peculiarly European invention. Under this legislation, the maker of a database (i.e., a person who creates a database) has the right to prevent the extraction or re-utilisation of the whole or a substantial part of the contents of the database. The legislation came into force on 1<sup>st</sup> January 1998. As indicated, this legislation is specific to the European Union and is not based on an International Treaty.



For these purposes, a database must have an element of selection in it as well as an investment of time and money to create it. For example, a database could consist of the events in a football match, such as the free kicks, corners, penalties and goals, or a database could consist of a list of medicines together with an overview of what the attributes of and indications for each medicine are.

The rights created by the European Union legislation last for 15 years from the date of creation of the database.

<sup>4</sup> The Regulation provides a degree of detail as to how this may and may not be achieved.

<sup>5</sup> See, for example, the express provision in Article 2 of the 1985 Product Liability Directive [3].

<sup>6</sup> Although such a data set (i.e. a computer program) would not satisfy the technical, legal definition of what constitutes a database for the purposes of the database legislation.

The rights are infringed even by a systematic extraction or re-use of insubstantial parts of the contents of the database. Where there is a substantial change to the contents of a database, so that it can be considered as a “substantial new investment”, the database will then qualify for a new term of protection beyond the original 15-year period. In this way, database protection can conceivably last for a long time, provided that “substantial new investments” are regularly made to the database. This will invariably be the case for commercial databases which are continuously being updated.

The key is that there must have been a substantial investment in the obtaining, verification, or presentation of the contents of the database. A further condition is that, in order for the database right to be enforceable in the European Union, the person or organisation who is the creator of the database must be a national of a Member State of the European Union or a company formed under the laws of a Member State and based there from an economic perspective.

The important thing to notice in this condition is the use of the present tense in the phrase commencing “be a national of a Member State”.

Where the person or organisation which owns the database, rights, ceases to be a national or company of a Member State, the database right is lost. So, if a company relocates itself and assets to a country which is not a Member state, such as the United States, the database rights are lost.

Unfortunately, it is not absolutely clear that the ambiguous Brexit deal that has been negotiated ensures that United Kingdom citizens and companies will retain their database rights now that the United Kingdom no longer is a Member State. While the intention of the Brexit deal was clearly that United Kingdom citizens and companies should retain their Database Rights, there is at least one counterargument to that position. That stems from the simple fact that the European Union legislature has not, in fact, changed the wording of the Directive.

Conversely, within the United Kingdom, European Union citizens and companies, alongside United Kingdom citizens and companies, will continue to have enforceable Database Rights. This continuation is specifically and unambiguously provided for in the initial Withdrawal Agreement which was agreed in January 2020.

However, for United Kingdom companies and citizens, the reverse position is more complex, and the position cannot be stated with absolute certainty. It is the associated doubt itself which has created a disadvantage for United Kingdom companies. In a situation where a United Kingdom citizen or company seeks to enforce its database rights in Europe it may find itself coming up against an argument that, in fact, it no longer has database rights in Europe.

Not only this, but the enforceability may also depend partly upon the country instantiation of the Member State in which that individual or company is seeking to enforce its database right. The European legislation is found in a 1996 Directive.

**The position of United Kingdom owned databases is therefore at best unsatisfactorily ambiguous, and at worst, there is no continuing protection for United Kingdom databases in Europe.**

All Directives require a country instantiation in order to be enacted in that country. In some countries, the wording of the Directive states that it is sufficient only that the database owner resided in the European Union at the time the database was created. For example, this appears to be the case in the German instantiation of the Directive.

The position of United Kingdom owned databases is therefore at best unsatisfactorily ambiguous, and at worst, there is no continuing protection for United Kingdom databases in Europe.

Either way, it does not reflect the agreed aim in the political declaration entered into between the European Union and the United Kingdom in October 2019. That declaration included an obligation “to preserve the Parties’ current high levels of ... rights [in] ... database[s]”.

Furthermore, database rights are becoming more, not less, important. This is because of the use of artificial intelligence to create those databases. By way of an example, consider a computer generated database of protein molecules and their likely properties. It is perhaps unfortunate, to say the least, that United Kingdom companies appear to be at a legislative disadvantage in the future exploitation of databases.

## References

[1] The Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019, <https://www.legislation.gov.uk/ukxi/2019/696/contents>, accessed April 2022.

[2] The Electric Vehicles (Smart Charge Points) Regulations 2021, <https://www.legislation.gov.uk/ukxi/2021/1467/contents/made>, accessed April 2022.

[3] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, <https://www.legislation.gov.uk/eudr/1985/374#>, accessed April 2022.

Image attribution:

lead: 98579035 © Rangizzz | Dreamstime.com, charger: 191943063 © Álvaro Bueno Lumbreras | Dreamstime.com  
CE marking: 202280360 © Olga Paha | Dreamstime.com, database: 20133225 © Jntvisual | Dreamstime.com

The author retains copyright of this article.

## Dai Davis

Dai Davis is a Technology Lawyer. He practices as a solicitor but is also a qualified Chartered Engineer and Member of the Institution of Engineering and Technology. Dai has consistently been recommended in the Legal 500 and in Chambers Guides to the Legal Profession for over 25 years. He has two master degrees: one in Physics, the other in Computer Science.

Having been national head of Intellectual Property Law and later national head of Information Technology law at Eversheds for a number of years, Dai has for the past decade been a partner in his own specialist law practice, Percy Crow Davis & Co. Dai advises clients throughout the country on intellectual property, computer and technology law subjects. A third “super specialism” that Dai has practised for over three decades is high-tech product safety, including advising on safety related software, CE Marking and product recall.

He is primarily a non-contentious lawyer, advising clients on technology-related commercial agreements. Being a technologist, Dai often works with clients who are involved in cutting edge technologies.

Dai is a non-executive director of FAST (The Federation Against Software Theft) and a Liveryman of the City of London through the WCIT (Worshipful Company of Information Technologists). He has been a Council member of the Licensing Executives Society of the United Kingdom, a body of professionals dealing in intellectual property licensing, for more than a decade. He is widely published and an experienced public speaker and writer. He can be contacted on 07785 771 721 or [mail@davidavis.com](mailto:mail@davidavis.com).