

# [There relating to individuals, including the obtaining, holding,](https://assignbuster.com/there-relating-to-individuals-including-the-obtaining-holding/)

[Business](https://assignbuster.com/essay-subjects/business/), [Management](https://assignbuster.com/essay-subjects/business/management/)

There are different uses of the word privacy, however the legal meaning varies slightly to the everyday meaning. Within internationaldocuments and laws there has been many definitions proposed however there is nouniversal definition of privacy. AmenehMalmir and Mohammad Malmir gave a range of definitionswithin their journal ‘ Government’s civil liabilitytowards individuals’ privacy in cyberspace’1.  “ Privacy is markingthe boundary line which allows the society to enter the private affairs of aperson. Privacy is the realm of private life which a typical person does notallow himself to violate in any condition by understanding society needs. Individuals’ tendency to their own dignity is the most important objective ofprivacy…Collecting sensitive information without the permission or knowledge ofthe person can be considered as a potential weapon in the hands of those inpower…Therefore, this value is not less than other fundamental values, as inthe era of information culture, some privacy is required for security andprosperity of human beings.

“ Currently, every member state ofthe EU follows the current 1995 Data Protection Directive which regulated theprocessing of personal data within the European Union. However, every state hastheir own laws, we operate under the Data Protection Act2. In thepreamble, it was said to be “ An Act to make new provision for the regulation of the processing ofinformation relating to individuals, including the obtaining, holding, use ordisclosure of such information.

”  The GDPR (General Data Protection Regulation) willcome into force on 25th May 2018 and will supersede the DataProtection Directive. This will change the way that customers information canbe handled, this will replace the Data Protection Directive which as abovestated our current legislation operates under. The EU’s GDPR website3 states; “ The EU General DataProtection Regulation…replaces the Data Protection Directive 95/46/EC and wasdesigned to harmonize data privacy laws across Europe, to protect and empowerall EU citizens data privacy” The underpinning regulation anddirective have been published in the EU official Journal4 whichstates when it will come into force with a two-year preparation period foranyone covered by the regulation.

The new UK data protection legislation5 waspublished on 14th September 2017, which revealed that it implementedmost of the GDPR, and some exemptions6, including added protection for journalists, scientific and historicalresearcher and anti-doping agencies. Because we are implementing our own lawsBrexit isn’t an issue here because the Data Protection Bill largely includesthe provisions of the GDPR. Therefore, there will only be minor changes to ourlaws and we are not relying on the EU for our privacy laws.  However, there have been a fewcases where the UK has allowed data protection laws to be breached and whenthey have reached the EU courts they have been stopped and the UK has been toldto change this. In the EU, there are two legal systems, the European Court ofHuman Rights (ECHR) and the Charter of Fundamental Rights of the European Union(CFREU), when we leave the EU we will only be leaving the latter. The European Court of Human Rightsis the first legal system within the EU, this is an international court whichdeals with cases of states alleged violations of our rights which are definedin the European Convention on Human Rights. The ECHR dealt with the appeals ofMr S and Mr Marper7who had both been accused of committing crimes which subsequently they wereprosecuted for however, their finger print and DNA samples were kept on record.

They appealed multiple times within the UK and were rejected so they eventuallyappealed to the ECHR on the basis that under Articles 8 and 14 the authoritieshad continued to keep their data on record unnecessarily. The court found thatthere had been a breach of Article 88 – theright to respect for privacy and family life, this wouldn’t have been establishedwithout the ECHR. The Charter of Fundamental Rightsis a text on basic but necessary human rights of every citizen in the EU.

Thecharter is in place to clarify rights into a single document which can changeand adapt as society does.  Court of Justice in the EuropeanUnion dealt with two cases at the same time being, the cases of Tele29 andWatson10. Bothcases concerned the ability of member states to make electronic communicationsservice providers to retain traffic and location data, this was in issue inrelation to the CFREU. This happened under the ePrivacy Directive exemption11 whichallows member states to restrict rights on the confidentiality ofcommunications.  In the judgment, the Court ofJustice in the European Union (CJEU) said which parts of national legislation wouldbe deemed as unlawful under EU law of the Charter of Fundamental Rights.

Themain issues were in regard to, the use of traffic and location data, thepurpose of retaining data, how the data can be accessed, data subjects beinginformed quickly, and containing the data within the EU.  Clearly in both these cases memberstates have violated EU laws and when we leave the EU we won’t be protected byEU courts in cases like these. As we are only leaving the CFREU this would bethe only one effected but this is clearly a big issue which may lead to thepublics privacy being invaded. In addition to the new GDPR, thereare new ePrivacy rules coming into force because without these the GDPR wouldbe incomplete. Because of the changing society it is necessary to haveprotection of the right to private life as promised in Article 712 of theCharter of Fundamental Rights and this relies on having online protection aswell. Currently, our protection comes from the ePrivacy Directive 200213 whichwas revised in 200914, thiswas referred to by many as the cookie law, because this is where the pop upconsent cookies came from. Increasing government surveillancewould be good in the sense that it would allow us to have a fuller picture ofwhat is happening within the country and anything which may affect us. Forexample, in the case of R (Catt) v ACPO & Metropolitan Police15, MrCatt appealed after a judgment that his records could be kept under ‘ review’ bythe police even though he has no criminal convictions and has never beenviolent personally at anti-arms trade rallies.

It is argued that deleting thisevidence would leave the police with a lack of awareness, Lady Hale16commented that; “ It is well known that, for avariety of reasons, complaints of domestic violence are often not followedthrough to prosecution and conviction. But it is vital for the police, whenresponding to any new complaint, to know whether there have been similarcomplaints in the past.” As this appeal was subsequentlyrejected this leaves the government in a good position because it supports theidea of increased surveillance, however as new laws are being developed for theUKs exit of the EU it is likely that this would still be deemed unlawful andthis would have to be established through case law. A newspaper article in theGuardian17explained the case of 2016 European court of justice (ECJ) ruling ina case brought by Labour’s deputy leader, Tom Watson, initially with David Davis, now theBrexit secretary. In the article18, it quotes Watson’s argument that; “ The current legislation fails toprotect people’s fundamental rights or respect the rule of law”. This is againa clear breach of Article 819as treating every member of the public like a suspect and gathering informationon them is not a respect for privacy and family life. However, not having thisinformation creates a lack of awareness for both our government and the policewhich could in term lead to crime which could have been prevented if we’d havehad the knowledge.

Therefore, this creates the difficult line between keepingpeople safe by having information on people and infringing on people’s basicrights to privacy. From this information, it is clear that we heavily rely on the EU for allof our privacy laws however, it is too early to say that we are too dependenton the EU because it may be the case that we continue to have legal protectionbut this will depend on the outcome of negotiations. 1 Ameneh Malmir and Mohammad Malmir, ‘ Government’scivil liability towards individuals’ privacy in cyberspace’, (2015)International Journal of Law & Management https://login-westlaw-co-uk.

lcproxy. shu. ac. uk/maf/wluk/app/document?&srguid= i0ad69f8e000001606f0d0ebcc8dba8c9&docguid= I3969BFC03D5E11E5A757FDD8BCA9A1B5&hitguid= I3969BFC03D5E11E5A757FDD8BCA9A1B5&rank= 5&spos= 5&epos= 5&td= 3889&crumb-action= append&context= 25&resolvein= true Accessed 19th December 2017 2 DataProtection Act 1998 c.

293 ‘ GDPRPortal: Site Overview’, (EUGDPR. org) < https://www. eugdpr. org/eugdpr. org. html> Accessed 20th December 20174 Regulation (EU) 2016/679 of the European Parliament and of the Council of27 April (2016) http://eur-lex. europa. eu/legal-content/EN/TXT/? uri= CELEX: 32016R0679&qid= 1513877377270Accessed 21st December 2017 5Data Protection Bill (HL Bill 66)6Data Protection Bill (HL Bill 66) Part 1, Chapter 147 8 Conventionfor the Protection of Human Rights and Fundamental Freedoms (EuropeanConvention on Human Rights, as amended) (ECHR) Art 89 10  11 Privacy andElectronics Communications Data 2002 OJ 2 201/37, Art 1012The Charter of Fundamental Rights 2000/C 364/01 Art 713 Directive on Privacy andElectronic Communications 2002/58/EC14 Directive on Privacy andElectronic Communications 2009/136152015 UKSC 9162015 UKSC 9, Para 54 17 AlanTravis, ‘ UK police to lose phone and web data search authorisation powers’ The Guardian (30th November2017)18Ibis. 19 Conventionfor the Protection of Human Rights and Fundamental Freedoms (EuropeanConvention on Human Rights, as amended) (ECHR) Art 8