IS IT POSSIBLE TO BREACH PRIVACY WHEN THERE IS NO HUMAN IN THE LOOP?

Introduction

Privacy is a word which is frequently bounded around without proper consideration of what it actually means, or what the user intends it to mean. It is one of those words that can mean different things to different people. We will all know someone who happily ticks all boxes required to allow them to use a given mobile phone app, granting countless unknown third parties access to not just their activity on their app, but in some cases other data stored on their smartphone, such as location data, contacts, or access to the microphone. We will also all know someone who reads every privacy policy they come across with a fine toothed comb and may forego use of the given service due to outrage at the invasion of their privacy contained in the terms; how many of your Facebook friends have disappeared from the platform in recent years? To an extent, therefore, any consideration of this question involves subjectivity, and scope for debate. This paper considers one interpretation of the question and puts forward a position as to whether it is possible to breach privacy when there is no human in the loop based upon that interpretation. It is intended to provoke discussion about both the range of possible interpretations of, in particular, the words “privacy” and “breach”, and to argue, ultimately, that within the paradigm considered, the breach occurs whether there is a human in the loop or not. The paper will also consider, briefly, whether the use of “consent”, in the form of tick-boxes, small print, or privacy policies, is enough to authorize the use of private information, and potential routes forward from a policy position.

The Meaning of Privacy

To consider whether privacy can be breached when there is no human in the loop, therefore, one must set a definition for privacy. The Merriam-Webster dictionary provides one definition of privacy as “*freedom from unauthorized intrusion*”.[1] The Cambridge Dictionary online provides a slightly different definition: “*someone’s right to keep their personal matters and relationships secret*.”[2] These definitions place a slightly different emphasis on the action required to maintain privacy; the implicit emphasis of the former is that it is the third party making an unauthorized intrusion that would mean privacy ceases to exist, the latter that the onus is on the individual to maintain their own privacy. That said, the implication of “unauthorized” is that the individual whose privacy is in question may authorize such intrusion, and the implication of “secret” is that the information is kept from third parties who would otherwise seek the information out.

So both definitions set up a dichotomy between the individual and the other. The question therefore becomes whether the other refers only to something human, or whether the other can entail a machine or algorithm.

To take an example, in the UK, Babylon Health is a company which provides GP and other medical services via a mobile app. In particular, Babylon Health employs an AI-based symptom assessor, an online chatroom where the user describes symptoms or asks questions, the AI either provides guidance or advices the user to take further action such as book a GP appointment, or call the non-emergency NHS helpline 111. Clearly, medical information is of a genre that most individuals wish to keep private. The user voluntarily logs their symptoms in the symptom-tracker, so the programme using it to provide advice would not be an unauthorized intrusion, but what if the information is also

passed to a wider analytics algorithm which tracks cold and flu symptoms during flu season, or, during the current pandemic, tracks the numbers of users making enquiries about COVID-19 symptoms, or the types of symptoms contained in these queries. When using the symptom-tracker, the user isn't informed of this, would this be an unauthorized intrusion into their privacy by the algorithm?

Another way to look at this concept, is to consider when it is that a breach of privacy actually occurs. Is the breach when information is removed from an individual, for example when a bug on a telephone line records a conversation, or is it when that information actually reaches another human being, i.e. when the recording is listened to? As the proverb goes, if a tree falls in the woods and nobody is there to hear it, does it make a sound?

Privacy in Practice

In the tech and telecoms sphere in the EU, this is often considered through the lens of data protection legislation and data breaches. In the EU the main applicable legislation is the General Data Protection Regulation ("**GDPR**"), pursuant to which companies must follow certain rules if they wish to control or process personal data which is defined as "*any information relating to an identified or identifiable natural person*".[3]

Often therefore, when we think we are considering privacy breaches, what we are actually discussing is data breaches under the GDPR. Such data breaches happen regularly and can be very high profile, with consequences for the business entity that has suffered the breach. For example, in 2019 British Airways was fined a record £183 million by the Information Commissioner's Office ("**ICO**") in relation to a 2018 breach whereby users of their website were diverted to a fraudulent site, resulting in 500,000 having their personal data disclosed to a third party.[4] The loyalty schemes of Tesco supermarkets and Boots pharmacies in the UK have been conduits for data breaches in early 2020,[5] and easyJet has warned customers of a breach caused by "*an attack from a highly sophisticated source*" resulting in personal data of 9 million customers being "*accessed*" along with the credit card details of 2,208 customers.[6]

The GDPR is interesting in that it puts an onus on business entities to help us to keep personal data private. The GDPR defines a personal data breach as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*."[7] The ICO specifies that this includes, *inter alia* "*access by an unauthorized third party*", "*deliberate or accidental action (or inaction) by a controller or processor*", "*computing devices containing personal data being lost or stolen*" and "*loss of availability of personal data*".[8] This extends responsibility for protecting private information from the individual, as implied in the Cambridge Dictionary definition above, to businesses. The British Airways, Tesco, and easyJet examples above provide examples where, on the face of it, it is not necessarily the action of these entities which caused the breach, rather the failure to prevent cyber-attacks which resulted in the breaches.

However, data protection and privacy are not synonymous, and personal data as defined under the GDPR does not necessarily cover all information that an individual might consider to be private. For example, the fact that a person has dated Boris Johnson alone, without an indication of time or place, is unlikely to be enough to constitute personal data – is the person identifiable from that fact? Potentially not, as Mr Johnson has reportedly dated a number of individuals. However, would that individual wish to keep the fact of their dating history with Mr Johnson private? Potentially.

Another approach is found in the Human Rights Act 1998 which enshrines the right in the European Convention on Human Rights ("**ECHR**") "respect for his private and family life, his home and his correspondence"[9] in UK legislation. Case law at the European Court of Human Rights has interpreted the term "*private life*" broadly, to include a "right to self-determination",[10] a right to reputation,[11] and in some cases professional and business activities.[12] However,

this right is not absolute. It is commonly understood that article 8 ECHR must be balanced against the right to freedom of expression, usually as exercised through the media provided in article 10 ECHR. It is up for debate whether the implication of this is that a privacy breach does not occur where the contravention of an individual's right to a private life is justified by freedom of expression, or whether the position is that while an individual's privacy has been breached, some breaches are justified

In practice, privacy rights are also addressed, in the UK, through the common law tort of misuse of private information.[13] Under this tort, the court will decide, through a two-stage test, whether there has been a misuse of private information.[14] First, the court will ask whether there was a reasonable expectation that the information disclosed would be kept private. Then the court will consider the balancing exercise referred to above between articles 8 and 10 of the ECHR. Under this paradigm, however, as article 10 ECHR is used as a defence to the tort, it seems that the balancing exercise becomes more a question of justifying the privacy breach, than of negating its occurrence. In Campbell v MGN, for example, it was held that this balancing act went against the model, Naomi Campbell's claim in relation to (i) the fact she was a drug addict, and (ii) the fact that she was receiving rehabilitation treatment for the addiction, but it went in her favour in relation to (i) the organization she was receiving treatment from, (ii) details the location and timing of this treatment, and (iii) photographs of the model leaving a rehabilitation meeting.

Does the combination of GDPR and, human rights legislation, and legal protection against misuse of private information add up to privacy? It is likely there are still some gaps between public perceptions of privacy, philosophical definitions of privacy, and the protections which exist at law. Ms Campbell, for example, clearly wished for her drug addiction to be kept secret.

The Timing of Breach

The definition in article 4(12) of the GDPR for personal data breach does not require the personal data to be seen by another human being, or used in any way. The breach, at law, happens when the personal data is accessed or removed from where it should be. This is most clear in the example of a personal data breach whereby the personal data is simply lost. If, in the course of employment, an individual has personal data on their laptop, and they accidentally wipe the laptop memory, this would be a personal data breach, even though there has been no unauthorized access to the personal data in question. However, would loss of personal data amount to a privacy breach?

Through the lens of the ECHR, arguably the breach would occur at the time the private and family life is intruded upon, whether by individual or machine. However, under the tort of misuse of private information, the tort arguably takes place when the information is *used*, not when it is acquired by the tortfeasor. Under this approach, a relevant consideration would therefore be whether a non-human's use of private information would constitute a breach in the same way that an individual's use would. Google Streetview is an online service which photographs roads all over the world in order to allow people to view online a given location, as if standing on that particular street. In the event that the photographs were taken by some kind of drone or unmanned vehicle, processed and uploaded to the Streetview platform by a computer programme, and included private information therein, could this fall under the tort? There is no reason to suppose that a machine or algorithm run by a company which resulted in the publication of private information would not potentially make that company liable for the tort of misuse of private information.

Under the two definitions described above, the Merriam-Webster interpretation hints at the timing of breach being when the information is taken from the individual in question – the moment at which that unauthorized intrusion takes place. Conversely, under the Cambridge Dictionary definition, there is a more arguable case that the moment of

breach takes place at the point in which the information in question is seen by another human – the point at which it is no longer secret because another human being knows. It is clear, therefore, that one's approach to when exactly a privacy breach occurs influences one's approach to whether a human is necessary in the loop.

The Efficacy of Consent

There is a question within this about the interplay between consent and privacy breaches. This is in part because it is generally accepted that the individual giving consent precludes a privacy breach. Under the GDPR, one of the legal bases for processing personal data is data subject consent.[15] There is an ongoing debate, however, about the nature of consent required.

The phrase often used in this context is "*informed consent*", in part due to the conditions for consent set out in Article 7 of the GDPR. The idea of informed consent is that individuals voluntarily give their consent to the use of their private information; ideally this won't be a simple tick-box exercise but rather individuals will be provided with a full understanding of the implications of giving consent, and will voluntarily give it.

Data has been called the new oil, the world's most valuable resource,[16] as it is increasingly necessary for businesses' success. This is particularly the case in the technology sector, where would technology giants such as Google or Facebook be if they did not have access to our data? How would the many myriad of apps available on smartphones at no cost to the user generate revenue if they had no access to our data to sell on for advertising or other purposes?

This is legitimized by the fact that the information is voluntarily given, and, in the case of personal data, the users consent through agreement to the applicable privacy notice. As such, there is no privacy breach because it has been authorized by the individual. However, the extent to which individuals are aware of the full extent to which their private information will be circulated, whether among different people or across different algorithms, is not apparent to many individuals. It is therefore debatable whether *informed* consent has truly been given by the individuals in question. If the position is taken that such consent has not been given, there are potentially millions of privacy breaches taking place every day, a number which is likely much higher where a privacy breach is deemed to occur without a human in the loop. This point emphasizes the importance of this question; most individuals like to think that they are entitled to privacy, and they are in control of when or if that entitlement is waived. However, the reality is that this entitlement is increasingly encroached upon by the onward march of technology into every aspect of our lives, often behind the façade of consent of dubious quality.

The Necessity of Humanity

If, as discussed above, a privacy breach is complete at the moment that the relevant information is taken from the individual to which it pertains, or the individual interested in keeping its secrecy, then there is no need for a human in the loop. Under this approach, a dog removing mail from someone's letterbox and running off with it would theoretically be a privacy breach. As technology has developed, such events are more and more frequent, except the entity taking the information is no longer your friendly neighbourhood dog, but rather technology, algorithms, CCTV, and so on.

Alternatively, if one takes the view that the privacy breach is complete at the moment that the relevant information is published to a wider audience, while the publishing can be done without a human in the loop, as per the hypothetical Streetview example above, the implication of publication is that information is made available to a wider (human) audience. Under this interpretation, therefore, it is less arguable that a privacy breach can occur without a human in the loop.

As this paper has discussed, under the different definitions of privacy discussed above, either approach is arguable. However, approaching the question from the point of view of the individual, it is likely that it is the loss or theft of the private information, that feels like the breach in privacy. Any dissemination or viewing of that information by other humans is ultimately a consequence of this theft. When one's home is burgled, the loss of the items taken is the event experienced by the individual(s) affected, the use of those items by others is the salt rubbed into the wound. As such, no human is required in the loop for the breach of privacy to occur, but human participation in the loop is likely to worsen the experience for the individual whose privacy has been breached.

Conclusions

Ultimately, the tree makes a sound when it falls, regardless of whether anyone is present to hear it. In my opinion, the breach in privacy takes place at the moment that private details about an individual are taken from that individual's control without their (informed) consent, not when that information is viewed or perhaps used by another human being. As such, it is possible for a privacy breach to take place where there is no human in the loop. Not only is it possible, but it's something which is arguably occurring on a daily basis as individuals fail to appreciate the scope of access to private information which is given through everyday use of our smartphones and other devices. Much of this is likely to be occurring without humans in the loop. As technology develops and extends further into our lives, this is trend is likely to continue.

One way of addressing such privacy breaches would be a policy change to address the question of informed consent. Particularly in relation to personal data, a higher standard must be set for the quality of consent required to allow for intrusion into our private lives. Ultimately, it is important that individuals are fully informed about the nature of intrusions into their private lives, whether authorized or not, by both human and non-human intervention.

[1]https://www.merriam-webster.com/dictionary/privacy

[2]https://dictionary.cambridge.org/dictionary/english/privacy

[3] Article 4(1), Regulation (EU) 2016/679

[4]https://www.bbc.co.uk/news/business-48905907

[5] https://www.which.co.uk/news/2020/03/boots-advantage-card-tesco-clubcard-both-suffer-data-breaches-in-same-week/

[6] https://www.easyjet.com/en/infoalert

[7] Article 4(12), Regulation (EU) 2016/679

[8] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

[9] Article 8(1), ECHR

[10] Pretty v United Kingdom, Application no. 2346/02

[11] White v Sweden, Application no. 42435/02

[12] Niemietz v Germany, Application no. 13710/88

[13] Vidal Hall v Google Inc [2015] EWCA Civ 311

[14] Campbell v MGN [2004] UKHL 22

[15] Article 1(a) GDPR

[16] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data