Öhman, Carl; Aggarwal, Nikita

Article

What if Facebook goes down? Ethical and legal considerations for the demise of big tech

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Öhman, Carl; Aggarwal, Nikita (2020) : What if Facebook goes down? Ethical and legal considerations for the demise of big tech, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 3, pp. 1-21, https://doi.org/10.14763/2020.3.1488

This Version is available at:
https://hdl.handle.net/10419/224932

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

What if Facebook goes down? Ethical and legal considerations for the demise of big tech

Carl Öhman
Oxford Internet Institute, University of Oxford, United Kingdom, carl.ohman@oii.ox.ac.uk

Nikita Aggarwal
Faculty of Law, University of Oxford, United Kingdom

Published on 11 Aug 2020 | DOI: 10.14763/2020.3.1488

Abstract: Society is becoming increasingly dependent on data-rich, "Big Tech" platforms and social networks, such as Facebook and Google. But what happens to our data when these companies close or fail? Despite the high stakes involved, this topic has received only limited attention to date. In this article, we use the hypothetical failure of Facebook as a case study to analyse legal and ethical risks related to the closure of data-rich, Big Tech platforms. Focusing on the EU, we argue that existing governance frameworks are inadequate for addressing these risks and make preliminary recommendations with a view to setting an agenda for future research and policymaking on the demise of Big Tech platforms and data-rich companies more broadly.

Keywords: Facebook, Social media, Data protection, Privacy, Insolvency, Digital ethics, Big tech

Article information

Received: 12 Dec 2019 **Reviewed:** 22 Mar 2020 **Published:** 11 Aug 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/what-if-facebook-goes-down-ethical-and-legal-considerations-demise-big-tech

Citation: Öhman, C. & Aggarwal, N. (2020). What if Facebook goes down? Ethical and legal considerations for the demise of big tech. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1488

INTRODUCTION

Facebook[1] has, in large parts of the world, become the *de facto* online platform for communication and social interaction. In 2017, the main platform reached the milestone of two billion monthly active users (Facebook, 2017), and global user growth since then has continued, reaching 2.6 billion in April 2020 (Facebook, 2020). Moreover, in many countries Facebook has become an essential infrastructure for maintaining social relations (Fife et al., 2013), commerce

(Aguilar, 2015) and political organisation (Howard and Hussain, 2013). However, recent changes in Facebook's regulatory and user landscape stand to challenge its pre-eminent position, making its future demise if not plausible, then at least *less implausible* over the long-term.

Indeed, the closure of an online social network would not in itself be unprecedented. Over the last two decades, we have seen a number of social networks come and go — including Friendster, Yik Yak and, more recently, Google+ and Yahoo Groups. Others, such as MySpace, continue to languish in a state of decline. Although Facebook is arguably more resilient to the kind of user flight that brought down Friendster (Garcia et al., 2013; Seki and Nakamura, 2016; York and Turcotte, 2015) and MySpace (boyd, 2013), it is not immune to it. These precedents are important for understanding Facebook's possible decline. Critically, they demonstrate that the closure of Facebook's main platform does not depend on the exit of all users; Friendster, Google+ and others continued to have users when they were sold or shut down.

Furthermore, as we examine below, any user flight that precedes Facebook's closure would probably be geographically asymmetrical, meaning that the platform remains a critical infrastructure in some (less profitable) regions, whilst becoming less critical in others. For example, whilst Friendster started to lose users rapidly in North America, its user numbers were simultaneously growing, exponentially, in South East Asia. It was eventually sold to a Filipino internet company and remained active as a popular social networking and gaming platform until 2015.[2] The closure of Yahoo! GeoCities, the web hosting service, was similarly asymmetrical: although most sites were closed in 2009, the Japanese site (which was managed by a separate subsidiary) remained open until 2019.[3] It is also important to note that, in several of these cases, a key reason for user flight was the greater popularity of another social network platform: namely, MySpace (Piskorski and Knoop, 2006) and Facebook (Torkjazi et al., 2009). Young, white demographics, in particular, fled MySpace to join Facebook (boyd, 2013).

These precedents suggest that changing user demographics and preferences, and competition from other social networks such as Snapchat or a new platform (discussed further below) could be key drivers of Facebook's decline. However, given Facebook's pre-eminence as the world's largest social networking platform, the ethical, legal and social repercussions of its closure would have far graver consequences than these precedents. Rather, the demise of a global online communication platform such as Facebook could have *catastrophic* social and economic consequences for innumerable communities that rely on the platform on a daily basis (Kovach, 2018), as well as the users whose personal data Facebook collects and stores.

Despite the high stakes involved in Facebook's demise, there is little research or public discourse addressing the legal and ethical consequences of such a scenario. The aim of this article is therefore to foster dialogue on the subject. Pursuing this goal, the article provides an overview of the main ethical and legal concerns that would arise from Facebook's demise and sets out an agenda for future research in this area. First, we identify the headwinds buffeting Facebook, and outline the most plausible scenarios in which the company — specifically, its main platform — might close down. Second, we identify four key ethical stakeholders in Facebook's demise based on the types of harm to which they are susceptible. We further examine how various scenarios might lead to these harms, and whether existing legal frameworks are adequate to mitigate them. Finally, we provide a set of recommendations for future research and policy intervention.

It should be noted that the legal and ethical considerations discussed in this article are by no means limited to the demise of Facebook, social media, or even "Big Tech". In particular, to the extent that most sectors in today's economy are already, or will soon become, data-driven and

data-rich, these considerations, many of which relate to the handling of Facebook's user data, are ultimately relevant to the failure or closure of any company handling large volumes of personal data. Likewise, as human interaction becomes increasingly mediated by social networks and Big Tech platforms, the legal and ethical considerations that we address are also relevant to the potential demise of other social networks, such as Google or Twitter. However, focusing on the demise of Facebook — one of the most data rich, social networks in today's economy — offers a fertile case study for the analysis of these critical legal and ethical questions.

WHY AND HOW COULD FACEBOOK CLOSE DOWN?

This article necessarily adopts a long-term perspective, responding to issues that could significantly harm society in the long run if we do not begin to address them today. As outlined in the introduction, Facebook is currently in robust health: aggregate user growth on the main platform is increasing, and it continues to be highly profitable, with annual revenue and income increasing year-over-year (Facebook, 2017; 2018). As such, it is unlikely that Facebook would shut down anytime soon. However, as anticipated, the rapidly changing socio-economic and regulatory landscape in which Facebook operates could lead to a reversal in its priorities and fortunes over the long term.

Facebook faces two major headwinds. First, the platform is coming under increasing pressure from regulators across the world (Gorwa, 2019). In particular, tighter data privacy regulation in various jurisdictions (notably, the EU General Data Protection Regulation [GDPR][4] and the California Consumer Privacy Act [CCPA])[5] could severely inhibit the company's ability to collect and analyse user data. This in turn could significantly reduce the value of the Facebook platform to advertisers, who are drawn to its granular, data-driven insights about user behaviour and thus higher ad-to-sales conversion rates through targeted advertising. In turn, this would undermine Facebook's existing business model, whereby advertising generates over 98.5% of Facebook's revenue (Facebook, 2018), the vast majority of which on its main platform. More boldly, regulators in several countries are attempting to break up the company on antitrust grounds (Facebook, 2020, p. 64), which could lead, *inter alia*, to the reversal of its acquisitions of Instagram and WhatsApp — key assets, the loss of which could adversely affect Facebook's future growth prospects.

Secondly, the longevity of the main Facebook platform is under threat from shifting social and social media trends. Regarding the latter, social media usage is gradually moving away from public, web-based platforms in favour of mobile-based messaging apps, particularly within younger demographics. Indeed, in more saturated markets, such as the US and Canada, Facebook's penetration rate has declined (Facebook, 2020, pp. 31-33), particularly amongst teenagers who tend to favour mobile-only apps such as Snapchat, Instagram and TikTok (Piper Jaffray, 2020). Although Facebook and Instagram still have the largest share of the market in terms of time spent on social media, this has declined since 2015 in favour of Snapchat (Furman, 2019, p. 26). They also face growing competition from international players such as WeChat with over 1 billion users (Tencent, 2019), as well as social media apps with strong political leanings, such as Parler, which are growing in popularity.[6]

A sustained movement of active users away from the main Facebook platform would inevitably impact the preferences of advertisers, who rely on active users to generate engagement for their clients. More broadly, Facebook's business model is under threat from a growing social and political movement against the company's perceived failure to remove misinformation and

hateful content from its platform. The advertiser boycott in the wake of the Black Lives Matter protests highlights the commercial risks to Facebook of failing to respond adequately to the social justice concerns of its users and customers.[7] As we have seen in the context of both Facebook as well as precedents such as Friendster, due to reverse network effects, any such exodus of users and/or advertisers can occur suddenly and escalate rapidly (Garcia et al., 2013; Seki and Nakamura, 2016; Cannarella and Spechler, 2014).

Collectively, these socio-technical and regulatory developments may force Facebook to shift its strategic priorities away from being a public networking platform (and monetising user data through advertising on the platform), to a company focused on private, ephemeral messaging, monetised through commerce and payment transactions. Indeed, recent statements from Facebook point in this direction:

> I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever. This is the future I hope we will help bring about.
>
> We plan to build this the way we've developed WhatsApp: focus on the most fundamental and private use case -- messaging -- make it as secure as possible, and then build more ways for people to interact on top of that.(Zuckerberg, 2019)

Of course, it does not automatically follow that Facebook would shut down its main platform, particularly if it still has sufficient active users remaining on it, and it bears little cost from keeping it open. On the other hand, closure becomes more likely once a sufficient number of active users and advertisers (but, importantly, not necessarily all) have also left the platform, especially in its most profitable regions. In this latter scenario, it is conceivable that Facebook would consider shutting down the main platform's developer API (Application Programming Interface — the interface between Facebook and client software) instead of leaving it open and vulnerable to a security breach. Indeed, it was in similar circumstances that Google recently closed the consumer version of its social network Google+ (Thacker, 2018).

In a more extreme scenario, Facebook Inc. could fail altogether and enter into a legal process such as corporate bankruptcy (insolvency): either a reorganisation that seeks to rescue the company as a going concern, typically by restructuring and selling off some of its assets; or liquidation, in which the company is wound down and dissolved entirely. Such a scenario, however, should be regarded as highly unlikely for the foreseeable future. Although we highlight some of the legal and ethical considerations arising from a Facebook insolvency scenario, the non-insolvent discontinuation or closure of the main platform shall be our main focus henceforth. It should be noted that, as a technical matter, this closure could take various forms. For example, Facebook could close the platform but preserve users' profiles; alternatively, it could close the platform and destroy, or sell parts or all of its user data etc. Whilst our focus is on the ethical and legal consequences of Facebook's closure at the aggregate level, we address technical variations in the specific form that this closure could take to the extent that it impacts upon our analysis.

KEY ETHICAL STAKEHOLDERS AND POTENTIAL HARMS

In this section, we identify four key ethical stakeholders who could be harmed[8] by Facebook's closure. These stakeholders are: *dependent communities,* in particular the socio-economic and media ecosystems that depend on Facebook to flourish; *existing users*, (active and passive) individuals, as well as groups, whose data are collected, analysed and monetised by Facebook, and stored on the company's servers; *non-users*, particularly deceased users whose data continues to be stored and used by Facebook, and who will represent hundreds of millions of Facebook profiles in only a few decades; and *future generations,* who may have a scientific interest in the Facebook archive as a historical resource and cultural heritage.

We refer to these categories as *ethical* stakeholders, rather than user types, because our categorisation is based on *the unique types of harm* that each would face in a Facebook closure, not their way of using the platform. That is, the categorisation is a tool to conduct our ethical analysis, rather than corresponding to some already existing groups of users. A single individual may for instance have mutually conflicting interests in her capacity as an existing Facebook user, a member of a dependent community, and as a future non-user. Thus, treating her as a single unit, or part of a particular user group, would reduce the ethical complexity of the analysis. As such, the interests of the stakeholders are by no means entirely compatible with one another, and there will unquestionably be conflicts of interest between them.

Furthermore, for the purposes of the present discussion, we do not intend to rank the relative value of the various interests; there is no internal priority to our analysis, although this may become an important question for future research. We also stress that our list is by no means exhaustive. Our focus is on the *most significant* ethical stakeholders who have an interest in Facebook's closure and would experience *unique* harms due to the closure of a company that is both a global repository of personal data, and the world's main communication and social networking infrastructure. As such, we exclude traditional, economic stakeholders from the analysis — such as employees, directors, shareholders and creditors. While these groups certainly have stakes in Facebook's potential closure, there is nothing that significantly distinguishes their interests in the closure of a company like Facebook from the closure of any other (multinational) corporation. This also means that we exclude stakeholders that could *benefit* from Facebook's closure, such as commercial competitors, or governments struggling with Facebook's influence on elections and other democratic processes. Likewise, we refrain from assessing the relative overall (un)desirability of Facebook's closure.

DEPENDENT COMMUNITIES

The first key ethical stakeholders are the 'dependent communities', that is, communities and industries that have developed around the Facebook platform and now (semi-)depend on its existence to flourish.[9]

Over the last decade, Facebook has become a critical economic engine and a key gateway to the internet as such (Digital Competition Expert Panel, 2019). The growing industry of digitally native content providers, from major news outlets such as Huffington Post and Buzzfeed, to small independent agencies, is sometimes entirely dependent on exposure through Facebook. For example, the most recent change in Facebook's News Feed algorithm had devastating consequences for this part of the media industry — some news outlets allegedly lost over 50% of their traffic overnight (Nicholls et al., 2018, p. 15). If such a small change in its algorithms could lead to the economic disruption of an entire industry, the wholesale closure of the main

Facebook platform would likely cause significant economic and societal damage on a global scale, particularly where it occurs rapidly and/or unexpectedly, such that news outlets and other dependent communities do not have sufficient time to migrate to other web platforms.

To be clear, our main concern here is not with the individual media outlets, but with communities that are dependent on a functioning Facebook-based media ecosystem. While the sudden closure of one, or even several media outlets may not pose a threat to this ecosystem, a sudden breakdown of the entire ecosystem would have severe consequences. For instance, many of the content providers reliant on exposure through Facebook are located in developing countries, in which Facebook has become almost synonymous with the internet, acting as the primary source of news (Mirani, 2015), amongst other functions. Given the primacy of the internet to public discourse in today's world, it goes without saying that, for these communities, Facebook effectively *is* the digital public sphere, and hence a central part of the public sphere overall. A notable example is Laos, a country which has so recently been digitised, that its language (Lao) has not yet been properly indexed by Google (Kittikhoun, 2019). This lacuna is filled by Facebook, which has established itself not only as the main messaging service and social network in Laos, but effectively also as the web as such.

The launch of Facebook's Free Basics platform, which provides free access to Facebook services in less developed countries, has further increased the number of communities that depend solely on Facebook. According to the Free Basics website,[10] 100 million people who would not otherwise have been connected are now using the services offered by the platform. As such, there are many areas and communities that now depend on Facebook in order to function and are thus susceptible to considerable harm were the platform to shut down. Note that this harm is not reducible to the individuals using free basics, but is a concern for *the entire community,* including members not using Facebook. As an illustrative example, consider the vital role played by Facebook and other social media platforms in disseminating information about and keeping many communities connected during the COVID-19 pandemic. In a time of crisis, communities with a large dependency on a single platform become particularly vulnerable.

Of course, whether the closure of Facebook's main platform harms these communities depends on the reasons for closure and the manner in which it closes down (sudden death vs slow decline). If closure is accompanied by the voluntary exodus of these communities, for example to a different part of the Facebook Inc. group (e.g., Messenger or Instagram), or a third-party social network, they would arguably incur limited social or economic costs. Furthermore, it is entirely possible to imagine a scenario in which the main Facebook platform is shut down because it is unprofitable to the company as a whole, or does not align with the company's strategic priorities, yet remains systemically important for a number of dependent communities. These communities could still use and depend on the platform however may simply not be valuable or lucrative enough for Facebook Inc. to justify keeping the platform open. Indeed, many of the dependent communities that we have described are located in regions of the world that are the least profitable for the company (certainly under an advertising-driven revenue model).

The question arises how these dependent communities should be protected in the event of Facebook's demise. Indeed, existing legal frameworks governing Facebook do not make special provision for its systemically important functions. As such, we propose that a new concept of 'systemically important technological institutions' ('SITIs') — drawing on the concept of 'systemically important financial institutions' ('SIFIs') — be given more serious consideration in managing the life and death of global communications platforms, such as Facebook, that

provide a critical societal infrastructure. This proposal is examined further in the second part of this article.

EXISTING USERS

'Existing users' refers broadly to any living person or group of people who uses or has used the main Facebook platform, and continues to maintain a Facebook profile or page. That is, both daily and monthly active users, as well as users who are not actively using the platform however still have a profile where their information is stored (including 'de-activated' profiles). Invariably, there is an overlap between this set of stakeholders and 'dependent communities': the latter includes the former. Our main focus here is on ethical harms that arise at the level of the individual user, by virtue of their individual profiles or group pages, rather than the systemic and societal harms outlined above.

It is tempting to think that the harm to these users in the event of Facebook's closure is limited to the loss of the value that they place on having access to Facebook's services. However, this would be an incomplete conclusion. Everything a user does on the network is recorded and becomes part of Facebook's data archive, which is where the true potential for harm lies. That is, the danger stems not only from losing access to the Facebook platform and the various services it offers, but from future harms that users (active and passive) are exposed to as they lose control over their personal data. Any violation of the trust that these users place in Facebook with respect to the use of their personal data threatens to compromise user privacy, dignity and self-identity (Floridi, 2011). Naturally, these threats also exist today. However, as long as the platform remains operational, users have a clear idea of who they can hold accountable for the processing of their data. Should the platform be forced to close, or worse still, sell off user data to a third party, this accountability will likely vanish.

The scope for harm to existing users upon Facebook's closure depends on how Facebook continues to process user data. If the data are deleted (as occurred, for example, in the closure of Yahoo! Groups),[11] users could lose access to information — particularly, photos and conversations — that are part of their identity, personal history and memory. Although Facebook does allow users to download much of their intentionally provided data to a hard drive — in the EU, implementing the right to data portability[12]— this does not encompass users' conversations and other forms of interactive data. For example, Facebook photos in which a user has been tagged, but which were uploaded by another user, are *not* portable, even though these photos arguably contain the first user's personal data. Downloading data is also an impractical option for the hundreds of millions of users accessing the platform only via mobile devices (Datareportal, 2019) that lack adequate storage and processing capacity. Personal archiving is an increasingly constitutive part of a person's sense of self, but, as noted by Acker and Brubaker (2014), there is a tension between how users conceive of their online personal archives, and the corporate, institutional reality of these archives.

On the other hand, it is highly plausible that Facebook would instead want to retain these data to train its machine learning models and to provide insights on users of other Facebook products, such as Instagram and Messenger. In this scenario, the risk to existing users is that they lose control over how their information is used, or at least fail to understand how and where it is being processed (especially where these users are not active on other Facebook products, such as Instagram). Naturally, involuntary user profiling is a major concern with Facebook as it stands. The difference in the case of closure is that many users will likely not even be aware of the *possibility* of being profiled. If Facebook goes down, these users would no longer be able to view their data, leading many to believe that it in fact is destroyed. Yet, a hypothetical

user may for instance create an Instagram profile in 2030 and still be profiled by her lingering Facebook data, despite Facebook (the main platform) being long gone by then. Or worse still, her old Facebook data may be used to profile *other* users who are demographically similar to her, without her (let alone their) informed consent or knowledge.

Existing laws in the EU offer limited protection for users' data in these scenarios. If Facebook intended to delete the data, under EU data protection law it would likely need to notify as well as seek the consent of users for the further processing of their data,[13] offering them the opportunity to retrieve their data before deletion (see the closure of Google+[14] and Yahoo! Groups). On the other hand, if Facebook opted to retain and continue processing user data in order to provide the (other) services set out under its terms and conditions, it is unlikely that it would be legally required to obtain fresh consent from users — although, in reality, the company would likely still offer users the option to retrieve their data. Independently, users in the EU could also exercise their rights to data portability and erasure[15] to retrieve or delete their data.

In practice, however, the enforcement and realisation of these rights is challenging. Given that user data are commingled across the Facebook group of companies, and moreover have 'velocity' — an individual user's data will likely have been repurposed and reused multiple times, together with the data of other users — it is unlikely that all of the data relating to an individual user can or will be identified and permanently 'returned'. Likewise, given that user data are commingled, objection by an individual user to the transfer of their data is unlikely to be effective — their data will still be transferred with the data of other users who consent to the transfer. As previously mentioned, the data portability function currently offered by Facebook is also limited in scope.

Notwithstanding these practical challenges, a broader problem with the existing legal framework governing user data is that it is almost entirely focused on the rights of *individual* users. It offers little recognition or protection for the right of *groups* — for example, Facebook groups formed around sports, travel, music or other shared interests — and thus limited protection against group-level ethical harm within the Facebook platform (i.e., when the ethical patient is a multi-agent-system, not necessarily reducible to its individual parts [Floridi, 2012; Simon, 1995]).

This problem is further exacerbated by so called 'ad hoc groups' (i.e., groups that are formed only algorithmically [Mittelstadt, 2017]), which may not necessarily correspond to any organic communities. For example, 'dog owners living in Wales aged 38–40 that exercise regularly' (Mittelstadt 2017, p. 477) is a hypothetical, algorithmically formed group. Whereas many organically formed groups are already acknowledged by privacy and discrimination laws, or at least have the organisational means to defend their interests (e.g., people with a certain disability, sexual orientation etc.), ad hoc algorithmic groups often lack organisational means of resistance.

NON-USERS

The third key ethical stakeholders are those who never, or no longer, use Facebook, yet are still susceptible to harms resulting from its demise. This category includes a range of disparate sub-groups, including individuals who do not have an account, but whose data Facebook nevertheless collects and tracks from apps or websites that embed its services (Hern, 2018). Facebook uses these data, *inter alia*, to target the individual with ads encouraging them to join the platform (Baser, 2018). Similarly, the non-user category includes individuals who may be tracked by proxy, for example by analysing data from their relatives or close network (more on

this below). A third sub-group is minors who may feature in photos and other types of data uploaded to Facebook by their parents (so-called "sharenting").

The most significant type of non-users, however, are *deceased users,* i.e., those who have used the platform in the past but have since passed away. Although this may currently seem a rather niche concern, the deceased user group is expected to grow rapidly over the next couple of decades. As shown by Öhman and Watson (2019), Facebook will soon host hundreds of millions of deceased profiles on their servers.[16] This sub-group is of special interest since, unlike living non-users who generally enjoy at least *some* legal rights to privacy and data protection (as outlined above), the deceased do not qualify for protection under existing data protection laws.[17] The lack of protection for deceased data subjects is a pressing concern even without Facebook closing.[18] Facebook does not have any legal obligation to seek their consent (nor that of their representatives) before deleting, or otherwise further processing, users' data after death (although Denmark, Spain and Italy are exceptions).[19] Moreover, even if Facebook tried to seek the consent of their representatives, it would have a difficult time given that users do not always appoint a 'legacy contact' to represent them posthumously.

The closure of the platform, however, opens an entirely new level of ethical harm, particularly in the (unlikely but not impossible) case of bankruptcy or insolvency. Such a scenario would likely force Facebook to sell off its assets to the highest bidder. However, unlike the sale or transfer of data of living users, which under the GDPR and EU insolvency law requires users' informed consent, there is no corresponding protection for the sale of deceased users' data in insolvency, such as requiring the consent of their next of kin.[20] Moreover, there are no limitations on who could purchase these data and for what purposes. For example, a deceased person's adversaries could acquire their Facebook data in order to compromise their privacy or tarnish their reputation posthumously. Incidents of this kind have already been reported on Twitter, where the profiles of deceased celebrities have been hacked and used to spread propaganda.[21] The profiles of deceased users may also remain commercially valuable and attractive to third party purchasers — for instance, by providing insights on living associates of the deceased, such as their friends and relatives. As in genealogy — where one individual's DNA also contains information about their children, siblings and parents — one person's data may similarly be used to predict another's behaviour or dispositions (see Creet [2019] on the relationship between genealogy websites and big pharma).

In sum, the demise of a platform with Facebook's global and societal significance is not only a concern for those who use, or have used it directly, but also for individuals who are indirectly affected by its omnipresence in society.

FUTURE GENERATIONS

It is also important to consider indirect harms arising from Facebook's potential closure due to *missed opportunities*. The most important stakeholders to consider in this respect are future generations, which, much like deceased users, are seldom directly protected in law. By 'future generations' we refer mainly to future historians and sociologists studying the origins and dynamics of digital society, but also to the general public and their ability to access their shared digital cultural heritage.

It is widely accepted that the open web holds great cultural and historical value (Rosenzweig, 2003), and thus several organisations — perhaps most notably the Internet Archive's Way Back Machine[22]— as well as researchers (Brügger and Schroeder, 2017) are working to preserve it. Personal data, however, have received less attention. Although (most) individual user data may

be relatively inconsequential for historical, scientific and cultural purposes, the aggregate Facebook data archive amounts to a digital artefact of considerable significance. The personal digital heritage of each Facebook user is, or will become, part of our shared cultural digital heritage (Cameron and Kenderdine, 2007). As Varnado writes:

> Many people save various things in digital format, and if they fail to alert others of and provide access to those things, certain memories and stories of their lives could be lost forever. This is a loss not only for a descendant's legacy and successors but also for society as a whole. [...] This is especially true of social networking accounts, which may be the principal—and eventually only—source for future generations to learn about their predecessors (Varnado, 2014, p. 744)

Not only is Facebook becoming a significant digital cultural artefact, it is arguably the first such artefact to have truly *global* proportions. Indeed, Facebook is by far the largest archive of human behaviour in history. As such, it can legitimately be said to hold what Appiah (2006) calls 'cosmopolitan value' — that is, something that is significant enough to be part of the narrative of our species. Given its global reach, and thus its interest to all of human kind (present and future), this record can even be thought of as a form of future *public good* (Waters, 2002, p. 83), without which we risk falling into a 'digital dark age' (Kuny, 1998; Smit et al., 2011) — a state of ignorance of our digital past.

The concentration of digital cultural heritage in a single (privately controlled and corporate) platform is in and of itself problematic, especially in view of the risk of Facebook monopolising private and collective history (Öhman and Watson, 2019). These socio-political concerns are magnified in the context of the platform's demise. For such a scenario poses a threat not only to the control or appraisal of digital cultural heritage, but also to its very existence — by decompartmentalising the archive, thus destroying its global significance, and/or by destroying it entirely due to lack of commercial or other interest in preserving it.

These risks are most acute in an insolvency scenario, where, as discussed above, the data are more likely to be deleted or sold to third parties, including by being split up among a number of different data controllers. Although such an outcome may be viewed as a positive development in terms of decentralising Facebook's power (Öhman and Watson, 2019), it also risks dividing and therefore diluting the global heritage and cosmopolitan value held within the platform. Worse still would be a scenario in which cosmopolitan value is destroyed due to a lack of, or divergent, commercial interests in purchasing Facebook's data archives, or indeed the inability to put a price on these data due to the absence of agreed upon accounting rules over a company's (big) data assets (Lyford-Smith, 2017). The recent auction of Cambridge Analytica's assets in administration, where the highest bid received for the company's business and intellectual property rights (assumed to include the personal data of Facebook users) was a mere £1, is a sobering illustration of these challenges.[23]

However, our concerns are not limited to an insolvency scenario. In the more plausible scenario of Facebook closing the shutters on one of its products, such as the main platform website and app, the archive assembled by the product would no longer be accessible *as such* to either the public or future generations, even though the data and insights would likely continue to exist and be utilised within the Facebook Inc. group of companies (*inter alia*, to provide insights on users of other products such as Instagram and Messenger).

RECOMMENDATIONS

The stakeholders presented above, and the harms to which they are exposed, occupy the ethical landscape in which legal and policy measures to manage Facebook's closure must be shaped. Although it is premature to propose definitive solutions, in this section we offer four broad recommendations for future policy and research in this area. These recommendations are by no means intended to be coherent solutions to "the" problem of big tech closure, but rather are posed as a starting point for further debate.

DEVELOP A REGULATORY FRAMEWORK FOR SYSTEMICALLY IMPORTANT TECHNOLOGICAL INSTITUTIONS.

As examined earlier, many societies around the world have become ever-more dependent on digital communication and commerce through Big Tech platforms such as Facebook and would be harmed by their (disorderly) demise. Consider, for instance, the implications of a sudden breakdown of these platforms in times of crisis like the COVID-19 pandemic. As such, there are compelling reasons to regulate these platforms as systemically important institutions. By way of analogy to the SIFI concept — that is, domestic or global financial institutions and financial market infrastructures whose failure is anticipated to have adverse consequences for the rest of the financial system and the wider economy (FSB, 2014) — we thus propose that a new concept of systemically important *technological* institution, or 'SITI', be given more serious consideration.

The regulatory framework for SITIs should draw on existing approaches to regulating SIFIs, critical national infrastructures and public utilities, respectively. In the insolvency context, drawing upon best practices for SIFI resolution, the *SITI* regime could include measures to fast-track insolvency proceedings in order to facilitate the orderly wind-down or reorganisation of a failing SITI in a way that minimises disruption to the (essential) services that it provides, thus mitigating harm to dependent communities. This might include resolution powers vested in a regulatory body authorised to supervise SITIs (this could be an existing body, such as the national competition or consumer protection/trade agency, or a newly established 'Tech' regulator) — including the power to mandate a SITI, such as Facebook, to continue to provide 'essential services' to dependent communities — for example, access to user groups or messaging apps — or else facilitate the transfer of these services to an alternative provider.

In this way, SITIs would be subject to public obligations similar to those imposed on regulated public utilities, such as water and electricity companies — as "private companies that control infrastructural goods" (Rahman, 2018) — in order to prevent harm to dependent communities.[24] Likewise, the SITI regime should include obligations for failure planning (by way of analogy to 'resolution and recovery planning' under the SIFI regime). In the EU, this regime should also build on the regulatory framework for 'essential services', specifically essential 'digital service providers', under the EU NIS (Network and Information Systems) Directive,[25] which focuses on managing and mitigating cyber security risks to critical national infrastructures.

Whilst the fine print of the SITI regulatory regime requires further deliberation — indeed, the analogy with SIFIs and public utilities has evident limitations — we hope this article will help incite discussions to that end.

STRENGTHEN THE LEGAL MECHANISMS FOR USERS TO CONTROL THEIR OWN DATA IN CASES OF PLATFORM INSOLVENCY OR CLOSURE.

Existing data protection laws are insufficient to protect Facebook users from the ethical harms that could arise from the handling of their data in the event of the platform's closure. As we have highlighted, the nature of 'Big Data' is such that even if users object to the deletion or sale of their data, and request their return, Facebook would be unable as a practical matter to fully satisfy that request. As a result, users face ethical harm where their data is used against their will, in ways that could undermine their privacy, dignity and self-identity.

This calls for new data protection mechanisms that give Facebook users better control over their data. Potential solutions include creating new regulatory obligations for data controllers to segregate user data, in particular as between different Facebook subsidiaries (e.g., the main platform and Instagram), where data are currently commingled.[26] This would allow users to more effectively retrieve their data were Facebook to shut down and could offer a more effective way of protecting the interests of ad hoc 'algorithmic' groups (Mittelstadt, 2017). However, to the extent that segregating data in this way undermines the economies of scale that facilitate Big Data analysis, it could have the unintended effect of reducing the benefits that users gain from the Facebook platform, *inter alia* through personalised recommendations.

Additionally, or alternatively, further consideration should be given to the concept of 'data trusts', as a bottom-up form of data governance and control by users (Delacroix & Lawrence, 2019). Under a data trust structure, Facebook would act as a trustee for user data, holding them on trust for the user(s) — as the settlor(s) and beneficiary(ies) of the trust — and managing and sharing the data in accordance with their instructions. Moreover, a plurality of trusts can be developed, for example, designed around specified groups of aggregated data (in order to leverage the economies of scope and scale of large, combined data sets). As a trustee, Facebook would be subject to a fiduciary duty to only use the data in ways that serve the best interests of the user (see further Balkin, 2016). As such, a data trust structure could provide a stronger legal mechanism for safeguarding the wishes of users with respect to their data as compared to the existing standard of 'informed consent'. Another possible solution involves decentralising the ownership and control of user data, for example using distributed ledger technology.[27]

STRENGTHEN LEGAL PROTECTION FOR THE DATA AND PRIVACY OF DECEASED USERS.

Although the interests of non-users as a group need to be given serious consideration, we highlight the privacy of deceased users as an area in particular need of protection. We recommend that more countries follow the lead of Denmark in implementing legislation that, at least to some degree, protects the profiles of deceased users from being arbitrarily sold, mined and disseminated in the case of Facebook's closure.[28] Such legislation could follow several different models. Perhaps the most intuitive option is to simply enshrine the privacy rights of deceased users in data protection law, such as (in the EU) the GDPR. This can either be designed as a personal (but time-limited) right (as in Denmark), or a right bestowed upon next of kin (as in Spain and Italy). It could also be shaped by extending copyright law protection (Harbinja, 2017) or take place within what Harbinja (2013, p. 20) calls a 'human rights-based regime', (see also Bergtora Sandvik, 2020), i.e. as a universal and inviolable right. Alternatively, it could be achieved by designating companies such as Facebook as 'information fiduciaries' (Balkin, 2016), pursuant to which they have a duty of care to act in the best interests of users with respect to their data, including posthumously.

The risk of ethical harm to deceased users or customers in the event of corporate demise is not

limited to the closure of Facebook, or Big Tech (platforms). Although Facebook will likely be the single largest holder of deceased profiles in the 21st century, other social networks (LinkedIn, WeChat, YouTube etc.) are also likely to host hundreds of millions of deceased profiles within only a few decades. And as more sectors of the economy become digitised, *any* company holding customer data will eventually hold a large volume of data relating to deceased subjects. As such, developing more robust legal protection for the data privacy rights of the deceased is important for mitigating the ethical harms due to corporate demise, broadly defined.

However, for obvious reasons, deceased data subjects have little political influence, and are thus unlikely to become a top priority to policy makers. Moreover, any legislative measures to protect their privacy are likely to be adopted at national or regional levels first, although the problem inevitably remains global in nature. A satisfactory legislative response may therefore take significant time and political effort to develop. Facebook should therefore be encouraged to specify how they intend to handle deceased users' data upon closure in their terms of service, and in particular commit not to sell those data to a third party where this would not be in the best interests of said users. While this private approach may not have the same effectiveness and general applicability as national or regional legislation protecting deceased user data, it would provide an important first step.

CREATE STRONGER INCENTIVES FOR FACEBOOK TO SHARE INSIGHTS AND PRESERVE HISTORICALLY SIGNIFICANT DATA FOR FUTURE GENERATIONS.

Future generations cannot directly safeguard their interests and thus it is incumbent on us to do so. Given the societal, historical and cultural interest in preserving, or at least averting the complete destruction of Facebook's cultural heritage, stronger incentives need to be created for Facebook to take responsibility and begin acknowledging the global historical value of its data archives.

A promising strategy would be to protect Facebook's archive as a site of digital global heritage, drawing inspiration from the protection of physical sites of global cultural heritage, such as through UNESCO World Heritage protected status.[29] Pursuant to Article 6.1 of the Convention Concerning the Protection of World Cultural and Natural Heritage (UNESCO, 1972), state parties acknowledge that, while respecting the sovereignty of the state territory, their national heritage may also constitute *world heritage,* which falls within the interests and duties of the 'international community' to preserve. Meanwhile, Article 4 stipulates that:

> Each State Party to this Convention recognizes that the duty of ensuring the identification, protection, conservation, presentation and transmission to future generations of the cultural and natural heritage [...] situated on its territory, belongs primarily to that State. It will do all it can to this end, to the utmost of its own resources and, where appropriate, with any international assistance and co-operation, in particular, financial, artistic, scientific and technical, which it may be able to obtain. (UNESCO, 1972, Art. 4)

A digital version of this label may similarly entail acknowledgement by data controllers of, and a pledge to preserve, the cosmopolitan value of their data archive, while allowing them to continue using the archive. However, in contrast to physical sites and material artefacts, which fall under the control of sovereign states, the most significant digital artefacts in today's world are under the control of Big Tech companies, like Facebook. As such, there is reason to consider a new

international agreement between corporate entities, in which they pledge to protect and conserve the global cultural heritage on their platforms.[30]

However, bestowing the label of global digital heritage does not resolve the question of *access* to this heritage. Unlike Twitter, which in 2010 attempted to donate its entire archive to the Library of Congress,[31] Facebook's archive arguably contains more sensitive, personal information about its users. Moreover, these data offer the company more of a competitive advantage compared to Twitter (the latter's user accounts are public, in contrast to Facebook, where many of the profiles are visible only to friends of the user). These considerations could reduce Facebook's readiness to grant public access to its archives. Nevertheless, safeguarding the existence of Facebook's records and its historical significance remains an important first step in making it accessible to future generations.

It goes without saying that the interests of future generations will at times conflict with the interests of the other three ethical stakeholders we have identified. As Mazzone (2012, p. 1660) points out, 'the societal interest in preserving postings to social networking sites for future historical study can be in tension with the privacy interests of individual users.' Indeed, Facebook's data are proprietary, and any interventions must respect its rights in the data as well as the privacy rights of users. Yet, the mere fact that there are conflicts of interests and complexities does not mean that the interests of future generations ought to be neglected altogether.

CONCLUSION

For the foreseeable future, Facebook's demise remains a high risk, low probability event. However, mapping out the legal and ethical landscape for such an eventuality, as we have done in this article, allows society to better manage the fallout should this scenario materialise. Moreover, our analysis helps to shed light on lower risk but higher probability scenarios. Companies regularly fail and disappear — increasingly taking with them troves of customer-user data that receive only limited protection and attention under existing law. The legal and ethical harms that we have identified in this article, many of which flow from the use of data following Facebook's closure, are thus equally relevant to the closure of other companies, albeit on a smaller scale. Regardless of which data-rich company is the next to go, we must make sure that an adequate governance framework is in place to minimise the systemic and individual damage. Our hope is that this article will help kickstart a debate and further research on these important issues.

ACKNOWLEDGEMENTS

We are deeply grateful to Luciano Floridi, David Watson, Josh Cowls, Robert Gorwa, Tim R Samples, and Horst Eidenmüller for valuable feedback and input. We would also like to add a special thanks to reviewers James Meese and Steph Hill, and editors Frédéric Dubois and Kris Erickson for encouraging us to further improve this manuscript.

REFERENCES

Acker, A., & Brubaker, J. R. (2014). Death, memorialization, and social media: A platform perspective for personal archives. *Archivaria*, *77*, 2–23. https://archivaria.ca/index.php/archivaria/article/view/13469

Aguilar, A. (2015). *The global economic impact of Facebook: Helping to unlock new opportunities* [Report]. Deloitte. https://www2.deloitte.com/uk/en/pages/technology-media-and-telecommunications/articles/the-global-economic-impact-of-facebook.html

Aplin, T., Bentley, L., Johnson, P., & Malynicz, S. (2012). *Gurry on breach of confidence: The protection of confidential information*. Oxford University Press.

Appiah, K. A. (2006). *Cosmopolitanism: Ethics in a world of strangers*. Penguin.

Balkin, J. (2016). Information fiduciaries and the first amendment. *UC Davis Law Review*, *49*(4), 1183–1234. https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf

Baser, D. (2018, April 16). Hard questions: What data does Facebook collect when I'm not using Facebook, and why? [Blog post]. *Facebook Newsroom*. https://newsroom.fb.com/news/2018/04/data-off-facebook/

Bergtora Sandvik, K. (2020). Digital dead body management (DDBM): Time to think it through. *Journal of Human Rights Practice*, *uaa002*. https://doi.org/10.1093/jhuman/huaa002

boyd, d. (2013). White flight in networked publics? How race and class shaped american teen engagement with MySpace and facebook. In L. Nakamura & P. Chow-White (Eds.), *Race after the internet*.

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cannarella, J., & Spechler, J. (2014). Epidemiological Modelling of Online Social Network Dynamics. *ArXiv*. https://arxiv.org/pdf/1401.4208.pdf

Competition & Markets Authority. (2020). *Online Platforms and Digital Advertising* (Market Study) [Final report]. Competition & Markets Authority. https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

Creet, J. (2019). *Data mining the deceased: Ancestry and the business of family* [Documentary]. https://juliacreet.vhx.tv/

DataReportal. (2019). *Global digital overview*. https://datareportal.com/?utm_source=Statista&utm_medium=Data_Citation_Hyperlink&utm_campaign=Data_Partners&utm_content=Statista_Data_Citation

Delacroix, S., & Lawrence, N. D. (2019). Disturbing the 'One size fits all' approach to data governance: Bottom-up. *International Data Privacy Law*, *9*(4), 236–252. https://doi.org/10.1093/idpl/ipz014

Di Cosmo, R., & Zacchiroli, S. (2017). Software heritage: Why and how to preserve software source code. *iPRES 2017 – 14th international conference on digital preservation*. 1–10.

F, C., & S, K. (2007). *Theorizing digital cultural heritage: A critical discourse*. MIT Press.

Facebook. (2017). *Form 10-K annual report for the Fiscal Period ended December 31, 2017*.

Facebook. (2018). *Form 10-K annual report for the fiscal period ended december 31, 2018*.

Facebook. (2019, June 18). Coming in 2020: Calibra [Blog post]. *Facebook Newsroom*. https://about.fb.com/news/2019/06/coming-in-2020-calibra/

Facebook. (2020). *Form 10-Q quarterly report for the quarterly period ended March 31, 2020*.

Federal Trade Commission. (2019, July 24). FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook [Press Release]. *News & Events*. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

Financial Stability Board. (2014). *Key attributes of effective resolution regimes for financial institutions i*. https://www.fsb.org/wp-content/uploads/r_141015.pdf

Floridi, L. (2011). The informational nature of personal identity. *Minds and Machines*, *21*(4), 549–566. https://doi.org/10.1007/s11023-011-9259-6

Floridi, L. (2012). Distributed morality in an information society. *Science and Engineering Ethics*, *19*(3), 727–743. https://doi.org/10.1007/s11948-012-9413-4

Furman, J. (2019). *Unlocking digital competition* [Report]. Digital Competition Expert Panel. https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel

Garcia, D., Mavrodiev, P., & Schweitzer, F. (2013). Social resilience in online communities: The autopsy of Friendster. *Proceedings of the First ACM Conference on Online Social Networks (COSN '13)*. https://doi.org/10.1145/2512938.2512946.

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, *22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Harbinja, E. (2013). Does the EU data protection regime protect post-mortem privacy and what could be the potential alternatives? *Scripted*, *10*(1). https://doi.org/10.2966/scrip.100113.19

Harbinja, E. (2014). Virtual worlds—A legal post-mortem account. *Scripted*, *11*(3). https://doi.org/10.2966/scrip.110314.273

Harbinja, E. (2017). Post-mortem privacy 2.0: Theory, law, and technology. *International Review of Law, Computers & Technology*, *31*(1), 26–42. https://doi.org/10.1080/13600869.2017.1275116

Howard, P. N., & Hussain, M. M. (2013). *Democracy's fourth wave? Digital media and the arab spring*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199936953.001.0001

Information Commissioner's Office. (2019, October). Statement on an agreement reached

between Facebook and the ICO [Statement]. *News and Events*. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico

Kittikhoun, A. (2019). *Mapping the extent of Facebook's role in the online media landscape of Laos* [Master's dissertation.]. University of Oxford, Oxford Internet Institute.

Kuny, T. (1998). A digital dark ages? Challenges in the preservation of electronic information. *International Preservation News*, *17*(May), 8–13. https://doi.org/Article

Lyford-Smith, D. (2017). *Data as an Asset. ICAEW i*. https://www.icaew.com/technical/technology/data/data-analytics-and-big-data/data-analytics-articles/data-as-an-asset

Marcus, D. (2020, May). Welcome to Novi [Blog post]. *Facebook Newsroom*. https://about.fb.com/news/2020/05/welcome-to-novi/

Mazzone, J. (2012). Facebook's afterlife. *North Carolina Law Review*, *90*(5), 1643–1685.

Mirani, L. (2015). Millions of Facebook users have no idea they're using the internet. *Quartz*. https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/

M.I.T. (2013). *An autopsy of a dead social network i*. https://www.technologyreview.com/s/511846/an-autopsy-of-a-dead-social-network/

Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philos. Technol*, *30*, 475–494. https://doi.org/10.1007/s13347-017-0253-7

N, B., & R, S. (Eds.). (2017). *The web as history: Using web archives to understand the past and the present*. UCL Press.

Öhman, C., & Floridi, L. (2018). An ethical framework for the digital afterlife industry. *Nature Human Behaviour*. https://doi.org/10.1038/s41562-018-0335-2

Öhman, C. J., & Watson, D. (2019). Are the dead taking over Facebook? A Big Data approach to the future of death online. *Big Data & Society*, *6*(1), 205395171984254. https://doi.org/10.1177/2053951719842540

Open Data Institute. (2018, July 10). What is a Data Trust? [Blog post]. *Knowledge & opinion blog*. https://theodi.org/article/what-is-a-data-trust/#1527168424801-0db7e063-ed2a62d2-2d92

Piper Sandler. (2020). *Taking stock with teens, spring 2020 survey*. Piper Sandler. http://www.pipersandler.com/3col.aspx?id=5956

Piskorski, M. J., & Knoop, C.-I. (2006). *Friendster (A)* [Case Study]. Harvard Business Review.

Rahman, K. S. (2018). The new utilities: Private power, social infrastructure, and the revival of the public utility concept. *Cardozo Law Review*, *39*(5), 1621–1689. http://cardozolawreview.com/wp-content/uploads/2018/07/RAHMAN.39.5.2.pdf

Rosenzweig, R. (2003). Scarcity or abundance? Preserving the past in a digital era. *The American Historical Review*, *108*(3), 735–762. https://doi.org/10.1086/ahr/108.3.735

Scarre, G. (2013). Privacy and the dead. *Philosophy in the Contemporary World*, *19*(1), 1–16. https://doi.org/10.1063/1.2756072

Seki, K., & Nakamura, M. (2016). The collapse of the Friendster network started from the center of the core. *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 477–484. https://doi.org/10.1109/ASONAM.2016.7752278

Simon, T. W. (1995). Group harm. *Journal of Social Philosophy*, *26*(3), 123–138. https://doi.org/10.1111/j.1467-9833.1995.tb00089.x

Smit, E., Hoeven, J., & Giaretta, D. (2011). Avoiding a digital dark age for data: Why publishers should care about digital preservation. *Learned Publishing*, *24*(1), 35–49. https://doi.org/10.1087/20110107

Stokes, P. (2015). Deletion as second death: The moral status of digital remains. *Ethics and Information Technology*, *17*(4), 1–12. https://doi.org/10.1007/s10676-015-9379-4

Taylor, J. S. (2005). The myth of posthumous harm. *American Philosophical Quarterly*, *42*(4), 311–322. https://www.jstor.org/stable/20010214

Tencent. (2019). *Q2 earnings release and interim results for the period ended June 30, 2019*.

Thacker, D. (2018, December 10). Expediting Changes to Google+ [Blog post]. *Google*. https://blog.google/technology/safety-security/expediting-changes-google-plus/

Torkjazi, M., Rejaie, R., & Willinger, W. (2009). Hot today, gone tomorrow: On the migration of MySpace users. *Proceedings of the 2nd ACM Workshop on Online Social Networks - WOSN '09*, 43. https://doi.org/10.1145/1592665.1592676

U. K. Government. (2019). *Online harms* [White Paper]. U.K. Government, Department for Digital, Culture, Media & Sport; Home Department. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

UNESCO. (1972). *Convention concerning the Protection of the World Cultural and Natural Heritage. Adopted by the General Conference at its seventeenth session Paris, November 16*.

Varnado, A. S. S. (2014). Your digital footprint left behind at death: An illustration of technology leaving the law behind. *Louisiana Law Review*, *74*(3), 719–775. https://digitalcommons.law.lsu.edu/lalrev/vol74/iss3/7

Warren, E. (2019). Here's How We Can Break Up Big Tech [Medium Post]. *Team Warren*. https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c

Waters, D. (2002). Good archives make good scholars: Reflections on recent steps toward the archiving of digital information. In *The state of digital preservation: An international perspective* (pp. 78–95). Council on Library and Information Resources. https://www.clir.org/pubs/reports/pub107/waters/

York, C., & Turcotte, J. (2015). Vacationing from facebook: Adoption, temporary discontinuance, and readoption of an innovation. *Communication Research Reports*, *32*(1), 54–62. https://doi.org/10.1080/08824096.2014.989975

Zuckerberg, M. (2019, March 6). *A privacy-focused vision for social networking* [Post]. https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

FOOTNOTES

1. Unless otherwise stated, references to 'Facebook' are to the main platform (comprising News Feed, Groups and Pages, *inter alia*, both on the mobile app as well as the website), and do not include the wider group of companies that comprise Facebook Inc, namely WhatsApp, Messenger, Instagram, Oculus (Facebook, 2018), and Calibra (recently rebranded as Novi Financial) (Marcus, 2019; 2020).

2. See https://www.washingtonpost.com/news/the-intersect/wp/2015/02/12/8-throwback-sites-you-thought-died-in-2005-but-are-actually-still-around/

3. See https://qz.com/1408120/yahoo-japan-is-shutting-down-its-website-hosting-service-geocities/

4. Regulation (EU) 2016/679 < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

5. California Legislature Assembly Bill No. 375 <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>

6. See <https://www.politico.com/news/2020/07/06/trump-parler-rules-349434>

7. See < https://www.nytimes.com/2020/06/29/business/dealbook/facebook-boycott-ads.html>.

8. We adopt an inclusive definition of ethical harm (henceforth just 'harm') as any encroachment upon personal or collective and legitimate interests such as dignity, privacy, personal welfare, and freedom.

9. Naturally, not all communities with a Facebook presence can be included in this category. For example, the lost marketing opportunities for large multinational corporations such as Coca Cola Inc., due to the sudden demise of Facebook, cannot be equated with the harm to a small-scale collective of sole traders in a remote area (e.g., a local craft or farmers' market) whose only exposure to customers is through the platform. By 'dependent communities' we thus refer only to communities whose ability to *flourish* and *survive* may be threatened by Facebook's sudden demise.

10. See https://info.internet.org/en/impact/

11. See https://help.yahoo.com/kb/understand-data-downloaded-yahoo-groups-sln35066.html

12. See Art 20 GDPR.

13. See Art 4(2) GDPR (defining 'processing' to include, *inter alia*, 'erasure or destruction' of personal data).

14. See Google Help, (2019) 'Shutting down Google+ for consumer (personal) accounts on April 2, 2019' https://support.google.com/plus/answer/9195133?hl=en-GB. Facebook states in its data policy that 'We store data until it is no longer necessary to provide our services and

Facebook Products or until your account is deleted — whichever comes first', which might suggest that users provide their consent to future deletion of their data when they first sign up to Facebook. However, it is unlikely that this clause substitutes for the requirement to obtain specific and unambiguous consent to data processing, for specific purposes — including deletion of data — under the GDPR (see Articles 4(11) and 6(1)(a)).

15. See Art 17 GDPR.

16. Facebook's policy on deceased users has changed somewhat over the years, but the current approach is to allow next of kin to either memorialise or permanently delete the account of a confirmed deceased user (Facebook, n.d.). Users are also encouraged to select a 'legacy contact', that is, a second Facebook user who will act as a custodian in the event of their demise. Although these technical solutions have proven to be successful on an individual, short-term level, several long-term problems remain unsolved. In particular, what happens when the legacy contact themselves dies? For how long will it be economically viable to store hundreds of millions of deceased profiles on the servers?

17. However, note that the information of a deceased subject can continue to be protected by the right to privacy under Art 8 of the European Convention on Human Rights, and the common law of confidence with respect to *confidential* personal information (although the latter is unlikely to apply to data processing by Facebook) (see generally Aplin et al., 2012).

18. Several philosophers and legal scholars have recently argued for the concept of posthumous privacy to be recognised (see Scarre [2014, p. 1], Stokes [2015] and Öhman & Floridi [2018]).

19. Recital 27 of the GDPR clearly states that '[t]his Regulation does not apply to the personal data of deceased persons', however does at the same time allow member states to make additional provision for this purpose. Accordingly, a few European countries have included privacy rights for deceased data subjects in their implementing laws (for instance, Denmark, Spain and Italy — see https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/deceased-persons.) However, aside from these limited cases, existing data protection for the deceased is alarmingly sparse across the world.

20. Under EU insolvency law, any processing of personal data (for example, deletion, sale or transfer of the data to a third party purchaser) must comply with the GDPR (See Art 78 (Data Protection) of EU Regulation 2015/848 on Insolvency Proceedings (recast). However, see endnote 17 with regard to the right to privacy and confidentiality.

21. See https://www.alaraby.co.uk/english/indepth/2019/2/25/saudi-trolls-hacking-dead-peoples-twitter-to-spread-propaganda

22. See https://archive.org/web/

23. See Administrator's Progress Report (2018) https://beta.companieshouse.gov.uk/company/09375920/filing-history. However, consumer data (for example, in the form of customer loyalty schemes) has been valued more highly in other corporate insolvencies (see for example, the Chapter 11 reorganisation of the Caesar's Entertainment Group https://digital.hbs.edu/platform-digit/submission/caesars-entertainment-what-happens-in-vegas-ends-up-in-a-1billion-database/).

24. There is a broader call, from a competition (antitrust) policy perspective, to regulate Big Tech platforms as utilities on the basis that these platforms tend towards natural monopoly (see,

e.g. Warren, 2019). Relatedly, the UK Competition and Markets Authority has recommended a new 'pro-competition regulatory regime' for digital platforms, such as Google and Facebook, that have 'strategic market status' (Furman, 2019; CMA, 2020). The measures proposed under this regime — such as facilitating interoperability between social media platforms— would also help to mitigate the potential harms to Facebook's ethical stakeholders due to its closure.

25. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016*.

26. Facebook has stated that financial data collected by Calibra/Novi, the digital wallet for Libra cryptocurrency, will not be shared with Facebook or third parties without user consent (Facebook 2019b). The segregation of user data is the subject of a ruling by the German Competition Authority, however this was overturned on appeal by Facebook (and is now being appealed by the competition authority — the original decision is here: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html).

27. A related imperative is to clarify the financial accounting rules for the valuation of (Big) data assets, including in an insolvency context.

28. See s 2(5) of the Danish Data Protection Act 2018 <https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf>

29. UNESCO has previously initiated a project to preserve source code (see Di Cosmo R and Zacchiroli, 2017).

30. This could be formal or informal, for example in the vein of the 'Giving Pledge' — a philanthropic initiative to encourage billionaires to give away the majority of their wealth in their lifetimes (see < https://givingpledge.org/>).

31. Although the initiative has ceased to operate as originally planned, it remains one of the best examples of large scale social media archiving (see https://www.npr.org/sections/thetwo-way/2017/12/26/573609499/library-of-congress-will-no-longer-archive-every-tweet).