The right to (not) be let alone: Reconciling freedom with privacy in our modern world

By: Carlos Moura Teixeira, Harvard University, Master in Public Policy

Introduction

The quest for freedom is an historical recurrence, but the scope, leader and impact of each wave are ever-changing. Overthrowing authoritarian regimes, escaping from conflict areas or fighting to be full citizens (with the same freedoms as men or white individuals) require unwavering focus and flexibility. Yet, in the digital sphere, the threats to those same fundamental freedoms more easily go unnoticed, due to the disruptive potential that fragmented strategic action may spur in such interdependent complex systems. Recent developments on privacy attempted at shielding users, but these may undermine certain freedoms – unless we reshape the way we protect the public and private spheres.

Internet: a force for good or evil?

Associating the concept of “freedom” with “privacy” does not seem a great leap. Be it a combination of the First, Third, Fourth, Fifth, and Ninth Amendments that created a “zone of privacy” in the US, the Universal Declaration of Human Rights’ Article 12 or the European Convention of Human Rights’ Article 8, the principle that the respect for one’s private life cannot be subjected to “arbitrary interference” has served us reasonably well for several decades. But not anymore.

When Warren and Brandeis asked, in 1890, whether “the courts [shall] thus close the front entrance to constituted authority and open wide the back door to idle or prurient curiosity”, both were far from envisioning how the curious nature of the human being would become so pervasive. Thanks to the Internet, our societies challenge the authors’ claim that “each man is responsible for his own acts and omissions only”.

Around the same time the right to Internet access was being discussed due to the Internet’s power to “hold accountable global players” and “enable freedom of opinion and expression”, the first signs that the Internet could become a potential battlefield of our fundamental values started emerging – and so did the concept of “internet freedom”.

At the core of such transformation is the exploitative and explorative nature that characterizes how humans gather, analyze and interpret data. In 2019, more than 8 billion data records were compromised and 1 in every 2 organizations had more than 1,000 files with sensitive data accessible to all users.
But, at a larger scale, the democratic implications of scandals like Cambridge Analytica, of an Internet ban as the recent one in India and of a limited, partially free access to Internet by 83% of all Internet users challenges the extent to which our freedoms (of speech, choice, assembly) can be fully exercised.

What once was a unfettered, opportunity-filled discovery capable of spurring progress – the Internet – has become a vehicle of exploitation and a source of risk to the survival of our dearest values.

**GDPR: A balancing act of freedom and privacy?**

Over time, the first policy responses started to emerge, but the European Union’s General Data Protection Regulation became the leading instrument when it comes to coping with the challenges that an Internet-centric world poses to fundamental rights. Almost two years since its enactment, the spillover effects of such regulation are undeniable, with multiple jurisdictions, such as California, Brazil and Kenya, developing new instruments that provide several options to reconcile privacy, fundamental freedoms and the digital world.

One of GDPR’s most debated provisions is Article 17. On one hand, it espouses that any data subject should “have the right to have his or her personal data erased and no longer processed” when (a) the original purposes for its collection and processing no longer apply, (b) consent to the processing of data has been withdrawn or (c) the processing of personal data is not GDPR compliant. On the other hand, any controller who has made the personal data public should “inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data”.

The former, commonly known as the “right to erasure” (RtE), or the latter, known as the “right to be forgotten” (RtbF), are not new. The inspiration for Article 17 is said to come from the right to expungement present in criminal justice. More subtle formulations of both RtbF and RtE had been laid out in prior European data protection instruments and the EU Charter of Fundamental Values.

The risks may be too heavy, some argue. With data regulators deciding what users find on the Internet, the RtbF may induce a form of censorship in which the preservation of information flows and historical clarity are undermined and a Eurocentric concept of content curation prevails. The concepts of private and public “memory” become vital, as the Internet shifts from being a tool for information retrieval to an unparalleled archiving technology. Any attempt to reconcile the droit à la mémoire (the right to memory), the droit à l’information légitime du public (the right to legitimately inform the public) and the droit à l’oubli (the right to forget) requires a balancing exercise of our freedoms by each citizen.

The landmark ruling *Google Spain v. AEPD & González* grappled with these questions. In 2010, Mr González asked the Spanish data protection regulator to erase an announcement, diffused in national media and a top result in any Google search, of a public auction where his property was being sold to pay back social security debts.

The Grand Chamber of the European Court of Justice held that, in this case, individuals should be able to ask search engines to remove any data that is “inaccurate, inadequate, irrelevant or excessive” (the so-called “delisting”) but not to require the erasure of a particular piece of content from the original website. This ruling, published before the final draft of GDPR was completed, is deemed to have been an important signal to the legislator on how a strong distinction between RtbF and RtE should be disregarded due to its several risks.

**Freedom is about forgiving, not forgetting**

The discourse around the RtbF and its potential nefarious effects underscores the multiple trade-offs European regulators attempted to address. Yet, European jurisprudence illus-
trates how, to defend our fundamental freedoms, a “right to be forgiven” is more appropriate than a “right to be forgotten”\textsuperscript{16}.

**The paradox of our modern times**

Thinking about privacy is grappling with the public and private spheres of our lives. Yet, any effort towards protecting any of these will fall victim of Post (1990)’s “paradox of public discourse”, i.e., the reality that public discourse can only be effective in guaranteeing democratic legitimation if it is civil and conformant to social mores, whose “enforcement of civility constrains freedom of speech”\textsuperscript{18}.

Our modern times are an empirical illustration of that hypothesis. Not only is the “number of real people participating [in public debates] on the decline”\textsuperscript{19}, but also the coherence of the content being provided is secondary when juxtaposed with multiple, but inconsistent streams of information that bury any substantive purpose of the discussion (the so-called “politics of flow”)\textsuperscript{20}. Any serious effort to defend our fundamental freedoms should square this circle.

**Step 1: Dignity, not data**

Solving the abovementioned paradox can only happen with a strong defense of freedom in the context of privacy instruments. Until now, when mentioning to data privacy, I am referring to the principle that information should be solely used for the particular purposes under which it was initially legally collected (and processed) even if purpose is hard to ascertain – especially for search engines.

Yet, if one focuses on “regulating inappropriate communications” that create harm to an individual through the violation of civility rules, we refer to dignitary privacy. In other words, it attempts to balance the harm to personality (individual freedom) and the harm to public discourse (freedom of speech) when considering whether there is, in fact, a right to be forgotten, instead of purporting an instrumental logic (data privacy) that does not place the value of freedom at the core of the decisions\textsuperscript{21}.

Privileging dignity over data strengthens our fundamental freedoms. If dignitary privacy was the prevailing analytical lens, as it is on regular press today\textsuperscript{22}, legal attention would be focused on the specific link where the announcement was posted and, when reasonable, remedies such as anonymization or the use of exclusion standards to avoid indexing such website to Google could be provided (both measures often applied in national courts and, therefore, more likely to be enforced) without risking a situation in which content may be completely removed\textsuperscript{23}.

**Step 2: Identity, not privacy**

In European caselaw, the RtbF has, de facto, and in general, been scrutinized regarding information already in the public domain (identity) rather than information protected from the public sphere that, for some reason, became public knowledge (privacy)\textsuperscript{24}.

In **CCIAA di Lecce v. Manni**, for example, the request to forget specific personal data contained in the public company registers was not accepted by the ECJ. Instead, access to such data was ruled to be constrained to only those who possess a “specific purpose”. The Court privileged, therefore, the public interest and the principle of business certainty (i.e., the freedom of information) over the right to privacy. In another case, the Italian Court of Cassation upheld the existence of a RtbF by defining it as, first and foremost, “a right to control one’s social image”\textsuperscript{25}.

Both supranational and national instances seem, thus, to give credence to the idea that, rather than a “right to privacy”, the “right to identity”\textsuperscript{26} is a fairer starting point to reconcile freedom and privacy. This lens not only seems coherent with already existing practices in other areas (e.g.: changing name, dropping a nationality), but also defines a more realistic scope of the RtbF that does not interfere with our own fundamental freedoms – namely, the right to define our own identity in a way that
reconciles one’s past without engaging in the rewriting or deletion of history.

The RtbF (and the GDPR) would be, under this hypothesis, what Arendt would call a policy of “judicious forgetting” by which one may build new socio-political relations according to a future one can, at such juncture, envision, while protecting its identity and upholding its freedom.

**Step 3: Protect, not control**

While the GDPR’s prevailing logic is an instrumental one, with its provisions framed around “control” over personal data, any aspiration to address threats to our fundamental freedoms cannot rely on the simple desire to control our personal information.

A ruling like Google Spain is not intended, I believe, to identify who owns and manages the personal data in that announcement. Instead, the goal is to avoid the content of a particular announcement from producing further damages to the dignity of Mr González in the public sphere. The removal of information from the public domain to transfer it to the hands of a private individual has strikingly different implications than the de-indexing of a particularly harmful website from a search engine (without interfering with the preservation of the original content) has.

Just like History, public discourse (and any of its spaces of dialogue as the Internet) cannot endure the test of time as soon as of its subjects attempts to have individual “control” of some piece of it. Thus, while I am not able to impede other historical accounts (where I am involved) from being told to uphold freedom of speech, I will certainly be able to challenge afterwards those which do not protect my dignity as a human being.

**Looking ahead**

Managing the flows of information in the digital agora touches upon our very fundamental values. The GDPR, with its RtbF, attempted at doing so through an instrumental approach to data privacy but, more often than not, that same approach competed directly with fundamental freedoms (e.g.: freedom of expression) and court rulings were poorly enforced as the onus resided on the private sector.

Over time, European caselaw has trailed a path where the hardly ascertainable purpose of a piece of information prevails, but the degree of harm to the individual’s dignity and to the public interest begins to be reflected in the Court’s decisions. While the latter places greater burden on the citizen, who then needs to prove harm, the wider range of remedies – as well as the ability to reconcile both privacy and freedom – pays off.

Rather than forgetting an instrument like GDPR, we should instead forgive it and strengthen it through a focus on the identity, dignity and protection of the data subject rather purely the instrumental value of the data. Only in that way privacy can become more than Warren’s “right to be let alone” and benefit from a substantive coupling with our fundamental freedoms.
Endnotes (incl. bibliographic references)

4. Idem.
11. In the 1995 Data Protection Directive in the EU, Article 12, the document foresees that the “right of access Member States shall guarantee every data subject the right to obtain from the controller: (...) (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort”.
   In the Article 8 of the Council of Europe’s Convention 108, the document calls for “appropriate security measures” and “additional safeguards for the data subject” such as the right to have access to his or her own personal data, the right to obtain, as the case may be, rectification or erasure of such data, and the right to remedy if such rights are not respected.
   On Article 8 of the EU Charter on Fundamental Rights: Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
16. Idem. In the ruling, the ECJ held that “the Court observes in this regard that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where, having regard to all the circumstances of the case, the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed”.
22. Currently, the application of this concept means that it places “a time limit on the publication of information: the press... cannot continue to publicize matters that are no longer in the public interest” and that can “relentlessly harm” persons “beyond a period of newsworthy relevancy”.