number of those have technically given their approval by clicking 'yes' on privacy conditions or cookie access requests without, in most cases, having much idea of exactly what they've agreed to. Three-quarters of Europeans polled wanted to be able to delete personal information on a website whenever they decided to do so. Sixty-three per cent said that disclosing personal information was a 'big issue' for them. Exactly the same percentage had not heard of any public authority responsible for the protection of rights on personal data.[23] Research from 2012 by Consumer Futures found that one in ten consumers had not realised any data was collected on them via online services, and a further fifth thought that the provider only collected the minimum amount required to make the service work better. Privacy, Facebook's founder Mark Zuckerberg once said, is no longer the 'social norm' that it once was.[24]

Attitudes and knowledge vary considerably between EU countries. A 2014 survey found that 1 per cent of respondents in the UK had heard of the national data protection authority, the Information Commissioner's Office. The figure for France was almost 70 per cent, up from 50 per cent only two years before. There is nothing particularly surprising in these variations. Policies and laws which manage a shifting reconciliation between free speech and privacy are usually the product of long, delicate compromise-making inside a single political culture.

Reputation and remembering

One purpose of this study is to point the way to how wired societies might best deal with digital platforms which are new sources of influence and power, often not 'publishers' in the classic sense, but making decisions which shape, edit, colour, and rank what people can find. The creation and distribution of information, news, and opinion has always been subject to some constraints imposed by society. Strong allegiance to the value and ideas of free speech does not prevent societies – America included – from occasionally restraining self-expression. Simply to equate freedom of speech with lack of regulation is to dodge the difficult issue of how such laws and rules can be as limited as possible and work as precisely and effectively as possible.

Professor Viktor Mayer-Schönberger of Oxford thinks that we should worry less about remembering than about forgetting – something human societies were good at before the internet. He sees the accumulation,

search, and retrieval of the twenty-first century as the culmination of a long historical process by which human societies have become steadily more exact and retentive about information. European societies archived little until the eighteenth century; the nineteenth century brought name registers, listed place names, collective memory with mass media. In the second half of the twentieth century, people began to worry about the misuse of data, but protection of data rarely kept up with the advances of technology. Now, he says, we need pragmatic ways to remember less. We do not need to delete things but to think about how easy or hard it is to reach them. 'Until now, we have mostly worried about how things are recorded,' he says, 'now, we have to think about how they are retrieved. That is because the default has shifted from forgetting to remembering.'[25]

In law, one of those efforts has been 'data protection'. Laws about data protection long predate the accelerating anxieties about social media and privacy in the early years of the new millennium. The Google Spain judgment of 2014 was based on an EU directive of 1995 which, not surprisingly, makes no mention of the internet.[26] The directive, whose scope is sweeping, generated laws which altered many business practices but it also established a tradition of such law declaring grand and noble aims which were then ignored and bypassed by proliferating digital innovations. Internet researcher Joris van Hoboken, who advised the European Commission on new data protection law, noticed this gap between theory and practice:

> *The web is full of legal issues. And that's a direct consequence of the fact that people can publish things themselves without having the information checked by an editorial office. Quite a bit of what's published on social media, and especially pictures, is just plainly illegal in Europe. Small and large violations of privacy are commonplace.*[27]

The key ideas which formed that 1995 directive (a template for laws in each EU state) have long antecedents and are strongly held by a majority of governments. People worry about the misuse of data but share personal information energetically. Many of the ideas from the first directive are reproduced in the new regulation on data protection, due to enter force in 2018.[28] The regulation will bind governments more tightly than a directive and it aims to reduce inconsistencies in enforcement between states.

The protection of honour

The protection of personal data from unauthorised misuse has its roots in strong legal traditions – especially in France, Germany, Spain, and Italy – which allow individuals to control their reputation, image, and 'honour' (the best equivalent in English of a term for which there is no exact translation).[29] Those ideas are also popular in Central Europe. Germany remembers the information control of both the Nazi regime and the East German secret police, the Stasi. The drive to protect personal data has powerful momentum derived from recent memory. Thirteen European countries have put data protection in their constitutions. The head of France's data protection authority, when recommending to a parliamentary commission that rights to data protection should be included in the French constitution, stressed that the right to control personal data is now distinct from the right to protect private life.

The internet is massively accumulative, searchable in a second, and, despite the extensive decay of hyperlinks, can preserve information indefinitely. That changes the nature of debates about rectification, something legal scholars call 'practical obscurity' (referring to a piece of information not erased but hard to find), and forgetting. The internet is both retentive and imperfect. The first page of search results for any given term, perhaps ten hyperlinks, is by far the commonest source of internet information.

Put the same term into three different search engines and you will get different results. They may overlap, but they will not be identical. So algorithms written by humans make value judgements. They may process data automatically and at extraordinary speed but they have power to affect human lives by choosing what the searcher sees and sees first.

This was exactly what bothered Mario Costeja Gonzalez, a lawyer and calligraphy expert living in Barcelona. In 1998, Sr Costeja had been the subject of a court order which allowed the authorities to auction his property to recover social security debts. The auction was publicised in two unadorned 36-word announcements a week apart in Barcelona's principal daily newspaper, *La Vanguardia*. When anyone searched for 'Mario Costeja Gonzalez' on Google in 2010, the 12-year-old notice of his bankruptcy and auction of his furniture was at the top of the results.

Sr Costeja lodged a complaint with the Spanish data protection authority (the AEPD[30]) to have the announcements erased from both

Google Spain and from *La Vanguardia*'s archive. The AEPD's then director, Artemi Rallo Lombarte, took a close interest in how individuals could strengthen control of their reputation. He had long been convinced, he said, that a compromise was possible by which the record would not be taken out of the original archive but that it would be made harder to find by being removed from a search engine. One of the first complaints to come before him was from a university teacher who had been fined in the 1980s for urinating in the street. Every year, his students would Google his 25-year-old minor conviction, their clicks on the link keeping the item near the top of the search results.

So the AEPD broke new ground by ruling that Sr Costeja did have the right to ask Google to erase its links to the notices even if the original newspaper archive still held them. In the later words of the European Court,

> *The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense …*[31]

The AEPD's decision went to the Spanish high court and was promptly referred to the EU judges in Luxembourg.

The claim that a search engine link breached 'the fundamental right to data protection' is crucial. Many legal systems allow restrictions on freedom of expression when a litigant claims that information circulated or published has done harm. All EU states and America have such laws. Examples would include defamation (or libel), breaches of privacy, or certain kinds of incitement. Many states forbid, under varying conditions, the republication of criminal convictions to help the rehabilitation of offenders. But data protection laws, drawn from from an EU directive, include wider powers to control personal information which do not depend on being able to show that harm has been done. Data protection law was originally conceived to give individuals rights of access and rectification concerning information held on them by states, companies, and organisations. It was not designed to regulate speech or expression.

There is further detailed discussion of the EU court's reasoning in Chapter 4. Two points stand out here. First, any debate over how to manage conflicting rights is upended in the final judgment by the sweeping and powerful phrasing of data protection as an emerging right. Second, the

tests which determine whether or not information can be removed from public view are framed in words which are so vague as to multiply confusion and not to reduce it.

The new infrastructure of knowledge

Open democracies have long legislated to remove some information from circulation. Companies like Google edit their output. Before the Spanish case, Google already had in place a system for handling deletion requests: bank account and credit card numbers, images of signatures are taken down as well as around a million links a day in response to requests arising from claims of copyright breach.[32] Courts in the UK and elsewhere can order certain sorts of information – libel, breaches of confidence or privacy, the identification of children in litigation, for example – not be published.

Many European states have laws which prohibit mention of past lesser crimes when the crimes are 'spent'. Several have media conventions that people convicted of (at least some) crimes are not referred to afterwards by their full names. But these measures differ from country to country. Victims of domestic abuse, often named when their partners are on trial, want to start new lives free from association with their past. Should they be granted anonymity in court or a right to be forgotten afterwards? Who should decide? The best argument for a 'right to delisting' is empowerment – that people who are harmed or distressed by something about them on the internet and who do not have the resources to hire lawyers can fix something that is wrong.

The Google Spain case reveals a gap in thinking about the new infrastructure of knowledge. We rely completely on intermediaries like Google, Bing, and Yahoo to use the colossal archives stored online. This study could not have been written without the ability, provided largely by google.co.uk, for the author to locate hundreds of relevant items. But the law has not yet adapted to intermediaries. As Joe McNamee of the European Digital Rights Initiative summarises:

> *We have a big problem in Europe with how we treat online intermediaries. Should risks of terrorism, hate speech and simple abuse or embarrassment all be handled in the same way or not? We don't seem to know. The current political approach appears to assume that the internet giants can solve all the world's problems.*[33]

The Google Spain judgment provoked noisy outcry which immediately engaged the spokespersons of the 'deletionists' and the 'preservationists'. Much of the fuss died down as soon as the complexities of the law and background emerged. Data protection is intricate and a 'right not to be found by Google' is considerably less dramatic than a 'right to be forgotten'. Google complained about the decision (and discreetly encouraged other voices to do so) but the company had good reason to fulfil the court's requirement without delay. Google faces two huge anti-trust investigations by the European Commission which will last for years and either of which, if the decision goes against Google, could derail or seriously damage its business model across the EU.

Google set up a web form which allows complainants to identify links which they want taken down and to justify their complaint. Google provides only bare statistics about how many complaints it has processed. By August 2016 and over two years after the judgment, a total of 539,384 applications had been made; 1,652,417 URLs had been 'evaluated', and 43.1 per cent of the total had been de-indexed.[34] A sample of figures by country is given in the following table.

Country	Applications	URLs evaluated	Percentage de-indexed
UK	94,937	218,682	38.9
France	133,066	337,634	49.0
Germany	80,598	291,865	48.3
Spain	46,029	140,465	38.3
Italy	37,780	115,910	32.3
Poland	12,623	48,447	42.2
Sweden	12,260	45,935	41.8
Netherlands	27,104	94,748	45.7

Google has resisted all calls to provide a deeper or more detailed analysis of how it decides these cases, although its executives have given broad and general descriptions of the tests they use. A number of UK news publishers, including the BBC, either kept a public list of links taken down or republished stories which they thought should have stayed in the record. As Google's force of paralegals fielded hundreds of thousand requests, a relatively small proportion led to adjudications by national data protection authorities or to court cases.[35] The only leak of detailed data suggests

that the large majority of requests are not about news or directed at news sites.[36]

Evaluating risks to freedom of speech or privacy is not a question of quantity. For the time being the system which has been tacked together on the back of existing data protection law seems to have worked quite well. But does it nevertheless represent a risk of harm – either to freedom of speech or to privacy, or to both – in the longer term? Data protection began with the understandable and laudable aim of protecting individuals from the misuse of state and corporate information. But does the pursuit of those aims in practice satisfy the public interest? The answer to that requires a look at the intellectual roots of data protection.