THE RIGHT TO BE FORGOTTEN

PRIVACY AND THE MEDIA IN THE DIGITAL AGE

GEORGE BROCK

Published by I.B.Tauris & Co. Ltd in association with the Reuters Institute for the Study of Journalism, University of Oxford
About the Book
The human race now creates, distributes and stores more information than at any other time in history. Frictionless and cheap digital networks circulate information in ways which either authors or subjects are unable to trace or control. Servers store data which can be found on the world wide web years after it has ceased to be accurate or relevant to its original use. These developments have given rise to a movement promoting a “right to be forgotten”: an argument that freedom of expression should be balanced by a right to erase information which affects an individual, under certain conditions. Rights to privacy need extending and strengthening in the digital era.

This strand of thinking influenced a significant judgement delivered by the European Court of Justice in May 2014. As a result, the dominant internet search engine in Europe, Google, has been required to remove links to hundreds of thousands of pieces of information on application from individuals who considered their interests harmed. We know very little of how these delinking choices are made. This Challenge looks at the implications of this controversial decision for free expression, journalism and information in the digital public sphere. Two rights – free speech and privacy – collide in a new way in an age of information saturation. Is the judgement a threat to freedom of information and the accuracy of the historical record or the first step in establishing essential new rights in the digital era?

An eloquent account offering valuable cultural and historical context to help us grapple with the problematic idea of the Right to be Forgotten being developed inside and outside the EU.
Judith Townend, Lecturer in Media and Information Law, University of Sussex

Data regulation is creaking under the strain of information abundance, leaving both freedom of expression and privacy at risk. The politics and policy of the competing rights involved are a mess. Brock elegantly highlights the confusion while offering positive insights into possible solutions.
Charlie Beckett, Professor, Department of Media and Communications, LSE; and Director, POLIS

About the Author
George Brock is Professor of Journalism at City University London, and the author of Out of Print: Newspapers, Journalism and the Business of News in the Digital Age.

What follows is a short extract from this book.
More information can be found at: www.ibtauris.com/reuters
RISJ CHALLENGES

CHALLENGES present findings, analysis, and recommendations from Oxford’s Reuters Institute for the Study of Journalism. The Institute is dedicated to the rigorous, international comparative study of journalism, in all its forms and on all continents. CHALLENGES muster evidence and research to take forward an important argument, beyond the mere expression of opinions. Each text is carefully reviewed by an editorial committee, drawing where necessary on the advice of leading experts in the relevant fields. CHALLENGES remain, however, the work of authors writing in their individual capacities, not a collective expression of views from the Institute.

EDITORIAL COMMITTEE

Timothy Garton Ash
Ian Hargreaves
David Levy
Geert Linnebank
John Lloyd
Rasmus Kleis Nielsen
James Painter
Alan Rusbridger
Jean Seaton
Katrin Voltmer

The Reuters Institute would like to acknowledge the assistance of Peggy Valcke and Timothy Garton Ash as editorial advisers on behalf of the Institute.
Contents

About the Author vi
Acknowledgements vii

1. Law, Power, and the Hyperlink 1
2. The Search Society 17
3. Striking the Balance 31
4. Google Spain 38
5. Reactions and Consequences 45
6. Beyond Europe 63
8. Alternative Approaches 82
9. Conclusions: The Future 89

Notes 102
Bibliography 111
Index 113
About the Author

George Brock is Professor of Journalism at City, University of London, where he directed studies in journalism 2009–14. He is co-leader of a research team at the university investigating search tools for journalism which has received grants from Google in 2015 and 2016 under the company’s computational journalism and digital news initiatives. He has worked for the Observer and The Times. At The Times he was Foreign Editor and Managing Editor; he was the paper’s correspondent in Brussels, 1991–5. He has been on the board of the World Editors Forum and the International Press Institute. In 2013 he published Out of Print: Newspapers, Journalism and the Business of News in the Digital Age.
Acknowledgements

I am grateful first and foremost to David Levy of the Reuters Institute for encouraging this study and to his colleagues Rasmus Kleis Nielsen and Alex Reid for their scrupulous editorial care and attention. I would also like to thank Peggy Valcke, Timothy Garton Ash, Daniel Wilsher, Judith Townend, and Martin Moore for their helpful comments. None bear any responsibility for faults. My greatest debt, as always, is to my wife Kay.
Law, Power, and the Hyperlink

Until recently, the English phrase a ‘right to be forgotten’ suggested fiction rather than reality. Fans of the Men In Black films think immediately of the ‘neuralyser’, the pen-shaped device which, when pointed at someone’s head and activated, wipes out memory. Or it might bring to mind Winston Smith, the protagonist of George Orwell’s 1984, whose dreary job as a censor of history involves removing articles no longer thought politically acceptable from back copies of The Times.

In May 2014, arguments erupted over the ‘right to be forgotten’ in real life. The phrase had been written and spoken before then, but very largely in the specialised world of ‘data protection’. The controversy began with a landmark judgment by the European Court of Justice, the highest court in the European Union.

The court decided that the vast, US-based search engine Google was subject to EU data protection law, that it had responsibilities under that law, and that it was required to remove search links when requests from citizens to do so met certain tests. The third of these decisions came instantly to be known as ‘the right to be forgotten’. The name is variously used to cover both the de-indexing (or delisting) of internet search results and the deletion of digital material. The phrase is neither new nor, when applied to de-indexing, wholly accurate. But as a slogan it was an instant and resounding success. That success owed a lot to accumulated anxieties about the potential harm which can be caused by some information stored and searchable on the internet.

The judgment in the case formally known as C-131/12 Google Spain SL and Google Inc v. AEPD and Mario Costeja Gonzalez (and usually known as ‘Google Spain’) was a shock.1 Google had expected to win the case. Advice to the court from its Advocate-General had recommended that the balance between freedom of speech and privacy should be struck by refusing the request to take the information out of Google’s search index. The court’s decision came as a surprise for another reason: very few
people knew much about data protection law and especially about this aspect of it.

The ‘right to be forgotten’ is only one part of data protection but its workings deserve to be much better known and debated. The question of whether the law should require personal information to be delisted by search engines (or deleted altogether) sits at the new, shifting, and disputed border between free speech and privacy in the online world. Battles over privacy have now become struggles over digital information rights. A new dispensation between freedom of information and rights to protect privacy and reputation is being hammered out in courts and political systems across the world. The search for a way to manage this collision of rights did not start with the Google Spain case, but that judgment tilted, polarised and fired up the debate.

Digital technology, by making possible vastly greater creation, storage, and search of information, poses new questions about free speech, privacy, and rights of rectification. Timeless values need to be applied in new contexts. This study examines the origins of, and fallout from, Google Spain and questions whether the balance is being struck in the right place. Any intervention at the junction of journalism, law, and technology should be closely examined and monitored. Journalism also plays a role in public memory. Exactly how much do we want to be able to recall? How do we determine what that is?

Free speech and privacy have been colliding for centuries. Rights which clash often cannot be reconciled; they can only be balanced by reasoning from the facts of a case. The debate over the ‘right to be forgotten’ opens a window on our attempts to adapt long-established values and principles to the online world. It poses questions for law and democracy raised by globalisation and instant communication. The issue is not only the competition of free speech and privacy but of discovery, historical memory, forgetting, the integrity of the public record, the right to know, and forgiveness. We are gradually assembling the conventions, software code and laws of a new public sphere.

The basic questions asked in the Google Spain case were: can Google’s search algorithm cause harm? If so, what should be done? Much of the immediate reaction to the case was overblown: it was not legal authority for the neuralyser or real-life Winston Smiths. The fact that people overreacted to the judgment does not mean that the European Court issued a good decision, nor does it mean that there are no future risks to
free speech built into it. The decision in Google Spain will come, I would argue, to be seen as one of the poorest in the court’s history. It makes the best balance between both freedom of speech and of knowledge – fundamental to good journalism – and the protection of privacy harder to achieve.

The judgment stores up trouble for the future by leaving important questions unresolved. A central one, still in dispute at the time of writing, turns on the territorial scope and enforceability of legal rulings about the internet, which by its nature recognises no borders. Regulatory jurisdiction and the transnational flow of information are mismatched. The judges said nothing about how far the right to be forgotten should reach. Google interpreted the ruling as applying to Europe: links removed were at first visible to those searching on the relevant names from an EU domain (google.co.uk, google.de, google.fr, etc.) but could be found by switching to google.com. European data protection authorities said that restricting the judgment’s effect to Europe would make it too easy to evade. The French authority began legal action against Google. The company attempted to defuse the stand-off by limiting the workaround. But the French authority insists that anything less than worldwide effect frustrates enforcement of the court’s wish. Google argues that worldwide application harms the information rights of people who are not EU citizens.

The right to be forgotten and journalism

Decisions which mark the new frontier between the right to free expression, the right to know, privacy, and data protection have significant implications for journalism. Journalism may pursue long-established aims, but the channels of communication have changed. If we define journalism as the systematic attempt to establish the truth of what matters to society in real time, that aim remains as important as ever in an information-saturated world. There are more providers and sources of information; that multiplies opportunities to learn but it also provides new opportunities to deceive. I have argued elsewhere that journalism in the twenty-first century faces four ‘core’ tasks: verification, sense-making, eye-witness, and investigation (of wrongdoing or dishonesty). Free expression rights underpin journalism and are pivotal in an additional sense. Journalism sometimes operates at the edge of what is permitted, tolerated, or legal in
order to disclose unexpected, concealed, or unwanted facts. This is true outside totalitarian or authoritarian states in which the law’s boundaries are often journalists’ main preoccupations.

Those tasks face new challenges in a world of newly malleable information. In the words of a Dutch court giving judgment in a case about the ‘right to be forgotten’, the internet is ‘an ocean of information’ which can change at any moment.\(^5\) Previous ideas of free speech underpinning journalism rested on the assumption that a fixed (printed) record should not be suppressed or interfered with. The quantity of recorded information and the ability instantly to change it suggest that long-standing principles must be rethought and applied in different ways. This study outlines one part of that rethinking.

Journalism must also navigate new distribution routes. Access to the consumers of news is now increasingly by search engines and social networks, predominantly Google and Facebook. As one study of this new information power puts it:

\[
\text{Almost accidentally, these global tech giants have taken on civic roles, and with these roles, civic power. This includes the power to enable collective action, the power to communicate news, and the power to influence people’s vote.}^{6}
\]

From the seventeenth to twentieth centuries, journalism’s move to be independent (above all of the power of the state) altered the governance of democracies. New communications technologies raise the same issues of making power accountable, but in new form in the twenty-first century. Journalists have celebrated the freedoms, diversity, and new opportunities that digital distribution offers but are now looking at the consequences of a major shift in control. This new power also needs to be accountable. To hold power to account, journalism depends on the understanding that neither individuals nor organisations have an unqualified right to control information about themselves. The issue at the heart of the right to be forgotten is how much control should be given to individuals to deal with the unforeseen effects of new technologies.

In the words of James Ball of Buzzfeed (writing in the Guardian):

\[
\text{Whether you are an ardent First Amendment advocate or a passionate believer that networks must do more to police their backyards, the worst of all possible worlds for the flow of information is one in which we shift}
\]
from the rule of democratic law to one governed by the arbitrary, inconsistent and perhaps kneejerk rulings of a tiny group of large companies.7

Digital downside

Most new means of communication, from air travel to the internet, are greeted with uncritical enthusiasm. As risks and disadvantages become more obvious after the initial promise, anxieties emerge. The cheap processors, sensors, and networks which drive digital information at such speed and volume have radically lowered the cost of access to that information. Digital communications are both an engine of opportunity and an unprecedented opportunity for surveillance. New public policies can be tried, new businesses are born, new means of accountability are available. An unprecedented scale of commercial ambition is possible: companies like Google and Facebook aim to persuade the whole population of the planet to become their customers.

These technologies have put publishing power in the hands of a few billion people. We have discovered that they are empowering and disempowering at the same time. Digital devices knit together our private, social, and working lives. Our ability to capture, store, and distribute information has multiplied the amount of information in existence by huge orders of magnitude. One leading estimate of the world’s data reckons that its total quantity doubles every two years. By this count, the world held 4.4 zettabytes in 2013 and will hold 44 zettabytes by 2020.8 The more data the world gathers, the further the opportunities extend for comparison and data crunching. Some of this analysis is innovative and useful, but it has a downside. Companies which ‘scrape’ the web dig up old police mugshots and display them online in the hope that people will pay to take them down. There are 16 sensors in the average smartphone. From the data they report, journalism could be adjusted and produced in response to the location, mood, and activity of the phone user. But that data could also rate the user’s sociability or attractiveness to other people. Phones are only the most prominent devices which accumulate data about everyone who uses them. Credit cards and cars do the same.

Stockpiles of data alter our ideas of how we record the life of a society and how the public space functions. Speaking of newspapers, people used
the phrase ‘paper of record’ to describe a reliably accurate one. This idea could only take shape in a society with a limited amount of public information which could be thought of as a ‘record’. Major national libraries attempt to capture at regular intervals everything that is on the internet. Is that now the historical record? Even if captured, digital information is malleable, correctable, and can be changed quickly. The abundance of information forces us to think more carefully about what we try to record and what we might reasonably lose, forget, or obscure. The internet offers unprecedented opportunities for voyeurism, exhibitionism, and morning-after regret. The internet is not a library: much of it is not edited in any way, much of it is not aimed at public purpose of any kind, websites are more perishable than books and access to it is given by private companies which are occasionally revealed to be manipulating results for commercial ends.

But the sheer range of information now accessible – and even its random and anarchic, unorganised nature – is part of what many people celebrate about the internet. Search engines and social networks increase the diversity of the news people consume.9 Journalists no longer have a monopoly on the production of information which has public value – if they ever did. To protect and preserve information of public value we need to consider carefully the contours and boundaries not only of what helps the public interest now but of what might in the future.

**Uncontrolled heterogeneous documents**

In their original academic paper which laid out the problems of searching the World Wide Web and how they proposed to solve them, the founders of Google, Sergey Brin and Larry Page, wrote: ‘The web is a vast collection of completely uncontrolled heterogeneous documents’.10 Here are three recent examples of the fragments of information which different people wanted removed from the vast collection in public circulation or made harder to find.

- In 2009 lawyers for an ex-convict in Germany, Wolfgang Werlé, attempted to remove his name from the English version of Wikipedia. Werlé, with Manfred Lauber, had been convicted in 1993 of the murder of a prominent German actor, Walter Sedlmayr, in a trial which received wide coverage. Werlé’s lawyers cited German privacy
law precedents which allow the erasure of a criminal’s name once he or she has served the sentence. Wikipedia and its parent, the Wikimedia Foundation, refused the request and successfully defended that decision in US courts. German courts made judgments in favour of the convicted men but the Constitutional Court overruled these as unreasonable restrictions on free speech. On the German-language Wikipedia.de there is no article on either man, while a search in the same site for ‘Walter Sedlmayr’ still carries the names of his killers. The English-language versions were untouched. The editing of the German site was voluntarily done by Wikipedia’s editors in Germany. The Wikimedia Foundation says that this is down to the respective Wikipedia language ‘communities’. ‘We support both user communities in these decisions’, the Foundation says.11

- In 2006, horrible pictures of a young woman who had been decapitated in a car crash in California began circulating on the internet. The pictures had been routinely taken at the scene by Highway Patrol staff who had later posted them on the web for friends at Halloween. American privacy laws do not cover such a case and First Amendment freedoms limit the ability to take down internet material. A recently founded company, Reputation.com, helped to get the pictures off more than 2,000 websites. But, to the continuing distress of the victim’s family, they could still be found years later.12

- In December 2015, a court in Saitama, Japan, ordered Google to remove from their search index reports of the arrest and fine of a man for violating child prostitution and pornography laws. The presiding judge said that convicted criminals were entitled to have their private life respected and their ‘rehabilitation unhindered’. Google is appealing the decision.13

These cases are all reactions to changes in information power over the past two decades: what information can do and who controls that. Public unease has prompted the makers of law and policy to question the ideas which have governed communications until the digital age. Artemi Rallo Lombarte, a Spanish MP and once head of Spain’s data protection agency:

_The right to be forgotten does conflict with freedom of expression. Internet users are not entitled to access personal information on the internet. We have to adapt our ideas of what free expression allows._14
By the end of 2014, there were seven billion mobile phones on the planet, roughly equal to the earth’s population. By 2017, one-third of those will probably be smartphones. We are taking something like a trillion pictures a year on our phones, a number which has doubled in the past five years. In the course of each minute, 200 million people send email messages, YouTube users upload 72 hours of video, and Facebook users exchange 2.5 million pieces of content. Each minute of each day. More than 90 per cent of internet searches in Europe are on Google; its share of mobile search is 96 per cent. A global survey of platforms which capture, transmit, and process data to create giant networks found 64 in the US, 82 in Asia, and 27 in Europe. The aggregate market cap of the American companies in that 2015 survey was $3,123bn. The equivalent figure for Europe $181bn. Some of that valuation lay in a new class of asset: data. Much of that can be classified as ‘personal’.

The scale of these corporations provokes suspicion, envy, and opposition. Blogs and pundits in France refer to ‘GAFA’, standing for Google, Apple, Facebook, and Amazon – all tech giants, all American. Others call those companies ‘Prism’ corporations, a sarcastic reference to the one of the US government’s most notorious and once-secret surveillance programmes, mounted with help from some parts of Silicon Valley. The informatics scholar Shoshana Zuboff describes Google’s ambitions as ‘surveillance capitalism’:

The game is no longer about sending you a mail order catalog or even about targeting online advertising. The game is selling access to the real-time flow of your daily life – your reality – in order to directly influence and modify your behavior for profit.

... We’ve entered virgin territory here. The assault on behavioral data is so sweeping that it can no longer be circumscribed by the concept of privacy and its contests. ... In the fullness of time, we will look back on the establishment in Europe of the ‘Right to be Forgotten’ and the EU’s more recent invalidation of the Safe Harbor doctrine as early milestones in a gradual reckoning with the true dimensions of this challenge.

The excitement with which people adopted search engines and social networks reflected a need which they met. That initial enthusiasm has now worn off and been mixed with suspicion and resentment. Both moods reflect shifts of informational power. The first shift was in favour
of consumers and users who could enjoy a range of instant information never before available. The second shift has been a slowly accumulating resistance to the power of the new gatekeepers who so influence daily life.

Opportunities to capture and distribute information were dispersed by digital devices. But the ability to accumulate, store, search, and analyse expanded the power of the data harvesters by unforeseen magnitudes. The power of instant retrieval alters the normal effects of the passage of time: information need not fade into the past but can be returned to the present with a keystroke.

Whether an ill-advised remark was made this morning or 20 years ago, if it comes up in an online search it is still, in some important sense, part of the here and now. Only with the greatest difficulty can stuff be entirely removed, the published unpublished.20

The idea that information, more and more of it, is simply liberating has given way to a more nuanced picture. Governments have barely begun to work out how to handle the power of the new superpowers of cyberspace. Policymakers have hardly grappled with the questions of how to treat internet intermediaries such as Google and Facebook. The public is the creator of most new data and both the beneficiary and, sometimes, victim of its retention, processing, and deployment. In twenty-first-century life ‘to exist is to be indexed by a search engine’.21

Facebook has over 35 million users in the UK. Ofcom’s survey for 2014 reported that 65 per cent of its users in the UK claimed to have tightened their privacy settings. A YouGov survey reported that Facebook lost 9 per cent of its UK users in the year to the middle of 2014. Half of those who stopped cited targeted advertising or other privacy concerns. ‘In the internet, humans have created an infinite new continent’, Caitlin Moran, a columnist for The Times wrote, ‘A limitless, seething megalopolis in which we do everything in a real megalopolis – shop, chat, meet – but in which we seem to believe the laws that humans painstakingly constructed … don’t count.’ Moran concluded that column: ‘But nothing is free, and everything a human ever does counts.’22

Public opinion is ambivalent and shifting. In a Eurobarometer survey of 2011, 73 per cent of respondents from throughout the EU said that they would like to give their specific approval before the collection and processing of their personal information. But it must be likely that a large
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.’

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. 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.*

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. 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). 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) 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 …*"  

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. 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.*
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. A sample of figures by country is given in the following table.

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

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. The only leak of detailed data suggests
that the large majority of requests are not about news or directed at news sites.\textsuperscript{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.
To purchase this book,
or to see others in the
Reuters Institute Challenges Series,
please visit I.B.Tauris’ website:

www.ibtauris.com/reuters