1) On May 13, 2014, the Court of Justice of the EU ruled against Google that individual EU residents have a “right to be forgotten.”

a) This allows EU residents the right to ask search engines to remove or delist links to their personal information.

Online reputation management in Europe hit a significant milestone on May 13, 2014, when the Court of Justice of the EU ruled that individual EU residents have a “right to be forgotten” online. In other words, individual EU residents have the right, under certain circumstances, to ask internet search engines—like Google, Bing and Yahoo!—to remove or delist links to personal information about themselves.

This landmark data protection ruling against Google (the most used internet search engine) requires that search engines delist links to content that is “inadequate, irrelevant or no longer relevant, or excessive,” or be subject to fines. Such Google delisting affects the link to the underlying content, but not to the underlying content itself. The landmark ruling states that the data subject’s “right to be forgotten” overrides not only the economic interests of the internet search engine, but also the general public’s right to have access to search results based on the name of the data subject; however, the data subject’s “right to be forgotten” should be overridden by the public’s right to know. When citing the role played by the data subject in public life, the Court of Justice implied that this balancing act should take into account activity of public interest, such as alleged wrongdoing, political exposure and creditworthiness.

On May 29, 2014, Google responded to this landmark ruling by launching an official delisting request process for itself that is still in place today. Google operationalized a procedure for receiving personal information delisting requests from individual European residents of 33 selected countries, whose request must meet certain criteria including proof of identity. The individual European resident forwards the delisting request directly to Google for their decision, without directing it first through a reviewing court, government agency or other third party. Yahoo!, Bing and other search engines have their own link delisting request forms and processes.

The 33 countries in the Google delisting program include 1) the 28 EU countries; 2) Iceland, Liechtenstein and Norway (which, when added to the 28 EU countries, make up the European Economic Area); and 3) Switzerland and Andorra (neither is a member of the EU or the European Economic Area, but both are acceptable European continent

---

3 Andorra, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.
data transfer destinations per Article 25 of the EU Data Protection Directive, as discussed below in the section on Argentina).4

On February 11, 2016, it was reported that Google would expand its “right to be forgotten” delisting of personal information links to include not only information links from EU versions of Google, but also from the global Google website when it is accessed by browsers located in the EU. Specifically, that would include local EU versions of Google, such as google.es which has local Spanish language content from Spain, and global google.com when it is accessed from a browser that has an Internet Protocol (IP) address associated with the European Union.5 On March 4, 2016, Google confirmed this report.6 This EU coverage is consistent with rights to privacy and data protection in the Charter of Fundamental Rights of the EU7 and the European Convention on Human Rights,8 as noted in the final report of Google’s Advisory Council on the Right to Be Forgotten.9

b) How does/will delisting affect AML/CTF investigations?

Within 48 hours of Google setting up their delisting process, over 12,000 individual European residents requested delisting. Most of those delisting requests were reportedly related to pedophilia, fraud, arrests, convictions, and from public officials.10 At last count, the number of individual Europeans requesting Google delisting has ballooned to 401,905.11

Google’s delisting form asks the requester to select the country whose law applies to the request, providing a drop-down menu that lists the selected 33 European countries.12 Google’s delisting form does not ask for the requester’s own country of citizenship or residency. However, Google’s delisting program was set up, in May 2014, to assist European citizens and residents who reside in the selected 33 European countries, regardless of their nationality. Google’s delisting program applies broadly to citizens of any country who are residents in Europe, but not to European citizens who reside outside the selected 33 European countries.13 Unlike Google, delisting request forms for Bing14 and Yahoo!15 do ask for verification of the requester’s country of European residency.

---

14 Request to Block Bing Search Results In Europe. https://www.bing.com/webmaster/tools/eu-privacy-request.
Concurrently, May 2014 marked an unprecedented surge in wealthy foreigners applying for European residency through golden investor visa programs, which allow a fast track to European residency, and possible citizenship, in exchange for investments in real estate, government bonds or businesses. Interest and applications soared upward for the Golden Visa residency programs that are tied to real estate investments in Spain, Portugal, Greece, Cyprus and Malta. Golden investor visa programs have long been criticized as being open to abuse and as potential tools for laundering improperly-obtained money from other countries in exchange for European residency. Conditions vary from country to country, including different euro investment minimum amounts and in some instances proof that the source of funds are AML-compliant. Greece reportedly offers the lowest cost to European residency at 250,000 euros plus taxes and fees (just over 300,000 euros) with “No requirement to reside,” there is a family application for the five-year Greek golden investor visa that can include children up to age 21 and is renewable, so long as property investment is retained. Significant demand for European golden investor visas comes from Middle Eastern countries, China, Russia, Pakistan, India, African nations and the Americas. There has been recent news coverage of corruption, influence peddling and money laundering allegations directed at politically exposed persons associated with Portugal’s Golden Visa program.

May 2014 is also when investigators shut down one of Europe’s biggest money laundering operations, an alleged conspiracy to launder $20 billion that was centered in the U.K. and involved individuals, firms and accounts from Eastern Europe. As reported publicly in 2014, Russian companies and a Moldovan would co-guarantee a fake loan or scam business deal set up between at least 19 U.K.-based front companies, which would sue each other for nonpayment in Moldovan courts. This resulted in at least 50 signed Moldovan court orders that were reportedly used to give the appearance of legitimacy to laundered cash payments from Russia, so that they might be deposited into Moldovan bank accounts for the U.K.-based front companies, before being transferred to another country as property investment is retained.


15 Yahoo! Help UK & Ireland: Requests to Block search results in Yahoo Search: Resource for European Residents. https://o2 help.yahoo.com/contact/indexy?v=PROD_SRCH&token=w5FCh8B4dWGbc2RE0kcijJu56u6QGoeUIkmqTBcuO %255BLu%252FtUq9c3BzwNZtXp6XEXn65Yw6Bu6A9MYyw7SzoY6BySKI6Upol0zwg5S7JZtSQQyAvs20zM2TM otsisbD%251XsQx1q%253D%251localse=en_GB&page=contactform&selectedChannel=email-icon&isVip=false.
EU regulated bank accounts in Latvia. Thanks to exemplary AML investigations and news coverage, it is increasingly possible to see these elaborate scams in a broader context and identify more red flags, such as:

- Personal names of specific individuals alleged to be money launderers and tax evaders, their extensive business activities in countries where a “right to be forgotten” may be in place, planned or discussed, and their relationships to each other and to politically exposed persons and other prominent third parties;
- Increased use of Scottish Limited Partnerships (SLPs) for U.K.-based front companies; such SLPs have been reportedly promoted in Eastern Europe as not requiring financial reporting or tax registration if business is conducted overseas; and
- Other common characteristics, including the complex sequence of transactional events and countries involved, financial institutions used, account numbers, and front company names, addresses and post office boxes.  

Google does not publicize its case-by-case approval or denial of each delisting request. In addition, the following notice now appears on Google’s European search result pages when personal names are searched: “Some results may have been removed under data protection law in Europe. Learn more.”

Therefore, AML/CTF investigators cannot know for sure which specific links to underlying content are now investigative blind spots, if one searches based on the name(s) of the data subject.

2) Internet search engines, like Google, Bing and Yahoo!, provide valuable support for AML/CTF investigations.

a) What are these search engines used for in regards to AML/CTF investigations?

Search engine results can provide context for a wide variety of AML/CTF matters, such as know your customer, know your customer’s customer, know your third party, and know your employee activities; suspicious activity report (SAR) management;

---


23 “Syed Farook” - Some results may have been removed under data protection law in Europe, Reddit, dated December 3, 2015. https://www.reddit.com/r/european/comments/3y9d6k/syed_farook_some_results_may_have_been_removed/.

24 Please check with your firm’s legal and human resources teams to confirm what background screening regulations, policies and practices might apply to the collection, verification, use, and data minimization of negative employee personal information that has been publicly available online before being delisted by Internet search engines. Moreover, data protection laws and related exemptions might apply, like the United Kingdom’s Data Protection Act of 1998, in which “sensitive personal data” is defined to include several categories such as the commission or alleged commission of any
enhanced due diligence for higher risk accounts; fraud investigations; and fact-finding on beneficial ownership issues, shell companies, human trafficking, illegal weapons trading, trade-based money laundering and politically exposed persons, their friends, relatives and close associates.

For example, when investigating suspicious activity on specific financial transactions, search engines often provide AML/CTF investigators with context that can be helpful when deciding whether to develop and file a SAR, put it on hold, or refrain from pursuing it altogether.25

b) How are AML/CTF investigations affected by the ruling?

For financial transactions affecting European residents, search engine delisting could create new AML/CTF investigative blind spots, as links to underlying content may or may not disappear. Google does not publicize specifics, which adds uncertainty. AML/CTF investigators cannot confirm details related to delisting requests and Google’s favorable or unfavorable response to them. AML/CTF investigators will likely have to spend more time on search engines digging for information links, which could be delisted.

The landmark Court of Justice ruling resulted in a search engine delisting process that will likely grow in influence. At this time, Google, Bing and Yahoo! are only receiving delisting requests from individual European residents, but the “right to be forgotten” appears to be gaining traction internationally and here to stay for the long-term. Following Europe’s lead, countries in other parts of the world have reportedly implemented, or are expected to implement, versions of the “right to be forgotten” including, but not limited to, the following 17 countries: Russia,26 China,27 Kazakhstan,28 Turkey,29 Japan,30 Hong Kong,31 South Korea,32 South Africa, Canada,33 Chile,34 Brazil,35

---


Costa Rica, Uruguay, Nicaragua, Argentina, Colombia and Mexico. The “right to be forgotten” is being discussed in many other countries in the Americas, Eastern Europe, Asia, Africa and the Middle East.

The Court of Justice portrayed the delisting process as an inconvenient expense for search engines. In fact, search engines may actually profit financially from more “stickiness” and advertising revenue, since visitors, including AML/CTF investigators, have to spend more time digging for information links, which could be delisted pursuant to this landmark ruling.

36 What are the implications of the right to be forgotten in the Americas?, IFEX. https://www.ifex.org/americas/2015/09/22/derecho_olvido/


c) The practical and evolving impact of this landmark ruling on Google.

Following this landmark ruling, Google delists personal information on its own based on the request received, rather than seeking advance confirmation on removal from European data protection authorities or other third parties, such as the judiciary or law enforcement, who are competent to clarify whether there is “a public interest in the information.” Should Google decline to delist personal information that determination is subject to appeal to the EU data protection agency where the requester resides.

The Court of Justice’s landmark ruling and Google’s delisting process have endured significant criticism and second-guessing. For example, on November 11, 2014, Sajid Javid, the U.K.’s Secretary of State for Culture, Media and Sport, delivered a speech to the Society of Editors Conference 2014, where he alleged that Google’s delisting process is being used to shield criminals and terrorists, as excerpted below in his own words:

“Since Luxembourg’s unelected judges created the so-called ‘right to be forgotten,’ Google has been receiving a demand for deletion every 90 seconds. Each day, a thousand requests pour in from people who, for one reason or another, would prefer their pasts to be kept secret. Criminals are having their convictions airbrushed from history even if they have since committed other, similar crimes. Terrorists have ordered Google to cover up stories about their trials. The search engine’s own lawyer has warned of unscrupulous companies abusing the system so that links to their competitors are hidden. The ‘right to be forgotten’ is censorship by the back door. Stories are not being deleted from archives because of the ruling, but if they cannot be found by the search engines they may as well not be there at all.”

Although it is common for judicial entities to balance rights and interests between parties, the Court of Justice ruling has been criticized for imposing such an obligation on private internet search engines. This has raised concerns, such as consistency, fairness, transparency, public accountability, conflicts of interest, lack of coordination with law enforcement, and due process, to name a few. Google has been accused of censorship for determining when private information should be delisted in search engine
results. Such “privatization” of censorship effectively immunizes the EU and its member states from direct criticism, which has been directed instead at search engines, such as Google.

It is noteworthy that Bing’s delisting request form includes two questions about the requester’s role in society and the community, presumably because the delisting could be less likely to be approved by Bing if the requester were associated with such a role. In these two Bing questions, the public figure category is broadly defined to include politicians and celebrities, and the community role category is defined to include leadership, trust or safety professional roles on a local level, such as teachers, clergymen, community leaders, police and doctors.

Bing’s public figure and community role questions do not map to politically exposed persons who are entrusted with prominent (generally national) public functions, their immediate family member or their close associates. Terms like “public figure” and “politician” that appear on Bing’s delisting request form are not synonymous with the term politically exposed person, which includes not only senior politicians, but also heads of state or government, senior officials in executive, legislative, judicial or military branches of government, senior executives in state-owned entities or corporations and important political party officials. Bing’s delisting request form does not inquire about alleged, convicted or acquitted criminal activity that may be newsworthy. Nevertheless, Bing’s two questions about the requester’s role in society and the community sets Bing apart from Google and Yahoo! As of March 12, 2016, Google and Yahoo! delisting request forms do not include similar questions.

3) Is there reason to question Google’s decisions to delist or not delist links to personal information?

Google’s delisting decisions appear to be straightforward, if one reviews only the limited summary information that Google discloses to the public. However, the situation is far less clear if we look at information that Google is disclosing to website operators, who are at times publicizing specific link delisting decisions reportedly disclosed to them by Google.

a) Review of favorable and unfavorable link delisting decisions (based on requests from individuals) that have been provided publicly by Google.

41 Bing delisting request form questions: Are you a public figure (politician, celebrity, etc.)? Do you have a role or expect to have a role in your local community or more broadly that involves leadership, trust or safety (for example, teacher, clergy, community leader, police, doctor, etc.)? Request to Block Bing Search Results In Europe. https://www.bing.com/webmaster/tools/eu-privacy-request.
Google’s summary delisting reports show clear-cut examples of delisting requests that have been accepted and delisted. As of March 12, 2016, Google reported having received 401,905 delisting requests from individuals as of May 29, 2014, the launch date of Google’s official delisting request process. The total Uniform Resource Locator (URL) number of web addresses evaluated for removal is 1,409,025—42.6 percent have been removed; 57.4 percent have not been removed. Google noted that these figures reflect the total evaluated; not included were URLs requiring more context or pending review.

In addition, as of March 12, 2016, Google publicized details related to 23 of the 401,905 delisting requests that have been received. As of March 12, 2016, the “right to be forgotten” has been associated with 12,089 Facebook URLs and 4,682 Twitter URLs being delisted from Google search results. Going forward, this delisting practice may be in the news, as postings on social media websites, like Facebook and Twitter, are scrutinized for hints leading up to terrorist attacks.

b) Review of favorable and unfavorable delisting decisions (based on requests from individuals) that have been made public by specific website operators who were notified by Google about link delistings.

Soon after Google set up its delisting program, news articles stated that delisting details would likely be archived at www.chillingeffects.org. This website, now www.lumendatabase.org, includes archives that are often redacted heavily; several appeared when the search term “EU – Right to Be Forgotten” was inputted, although several take-down requests based on alleged defamation, copyright infringement, and other claims appeared to be mixed in.

Although not required, Google reserves for itself, on its request form, the option to notify website operators that their content had been delisted. That practice has resulted in at least one website—HiddenFromGoogle.com—reportedly being created, on July 5, 2014, to collect and show links for website pages previously delisted by Google.

On August 6, 2014, the Wikimedia Foundation established its own webpage of Wikipedia search result links that have been delisted by Google. Since its inception, this regularly updated list of Google search result removals has drawn news media attention,

---

46 Ten things you need to know about the EU’s decision on the ‘right to be forgotten’ on Google, SEO Blog, dated June 2, 2014. http://www.searchenginoptimizations.co/2014/06/02/ten-things-need-know-eus-decision-right-forgotten-google/.
47 Google Legal Help - Search removal request under data protection law in Europe, which states, “We may provide details to webmaster(s) of the URLs that have been removed from our search results.” https://support.google.com/legal/contact/lr_eudpa?product=websearch.
since it includes the delisting of Wikipedia search results about Renato Vallanzasca, an Italian mobster, and Gerry Hutch, a convicted Irish bank robber.\textsuperscript{51}

On March 5, 2015, website Finextra announced that one of its noteworthy articles had been delisted by Google.\textsuperscript{52} The delisted article was a November 24, 2003, report on a London gang of six men who had been convicted and imprisoned for conspiracy to defraud through the creation of fake identities. Reportedly, such “synthetic” false identities were obtained online to forge documents, open bank accounts, and apply for loans, which were then used to obtain 315,000 euros from Lloyds TSB plc and 30,000 euros from the Halifax and Co-operative banks.\textsuperscript{53} It is unclear which of the six men made the delisting request to Google, or why Google would have delisted this article of public interest to banks, other financial institutions, lawmakers, regulators, cyber security analysts, and anyone who accepts payments for products and services.

On September 3, 2015, The Telegraph, a British news website operator, published a list of 94 news article summaries and links that Google reportedly delisted.\textsuperscript{54} It is unclear why Google delisted most of the 94 news articles on investigations, accusations, arrests, acquittals, or imprisonment for a wide range of alleged violations, such as domestic violence, human trafficking, assault with a deadly weapon, public intoxication, murder, terrorism, fraud, sex scandals, theft, insider trading, drug possession, sexual orientation harassment, suicide, sexual assault, employment discrimination, racial discrimination, wrongful deportation, and malpractice. On November 13, 2015, Google’s delisting of personal information links was in the news again. This was in response to Google’s reported decision to delist links to an article in The Telegraph on Anders Breivik, a Norwegian gunman convicted of killing 77 people in a bomb and shooting rampage.\textsuperscript{55}

In addition, on January 4, 2016, the British Broadcasting Corporation published a regularly updated list of about 270 news article links that Google reportedly delisted, similarly drawing attention to the delisted articles.\textsuperscript{56} It is unclear why Google delisted most of about 270 news articles on investigations, allegations, arrests, settlements, acquittals, overturned convictions, or imprisonment for a wide range of alleged violations, such as misrepresentation, credit card theft, assault with a deadly weapon, battery, property damage, murder, professional misconduct, attempted murder, drug possession, drug injection of another without consent, employment discrimination, wrongful deportation, indecent exposure, theft, sexual misconduct with minors, drug sales, missing persons, child abduction, kidnapping, robbery, conspiracy, aggravated burglary, firearms offenses, prostitution, intoxicated driving, possible terrorist activity, corruption in law enforcement, cybercrime, missing persons, war in the Middle East,


\textsuperscript{56} December 2015: List of BBC web pages which have been removed from Google’s search results, dated January 4, 2016. http://www.bbc.co.uk/blogs/internet/entries/f4b01ccf-9128-45d8-8cac-23c1cf3455c1?ns_mchannel=social&ns_campaign=bbc_internet_blog&ns_source=twitter&ns_linkname=corporate.
counterfeit sports ticketing, insider trading, fraud, health issues, arson, indecent exposure, financial crimes, government mismanagement, torture, extortion, tax evasion, illegal pyramid schemes, sexual assault, smuggling, traffic violations, pornography, an anthrax hoax, malpractice, identity fraud (including Google’s delisting of the BBC’s coverage of the same “synthetic” identity fraud case whose Finextra coverage was delisted by Google, as noted above), mail theft and embezzlement.

Such published lists of delisted news links have been criticized for drawing undue attention to some of the individuals and circumstances involved. The “right to be forgotten” has inspired individuals with “spent” criminal convictions to request Google delisting of “unwanted” search results, consistent with laws such as the Rehabilitation of Offenders Act 1974 in the U.K. 58

The Rehabilitation of Offenders Act 1974 is designed, in part, to penalize unauthorized disclosure of previous “spent” criminal convictions, but it is generally limited to helping people with few and/or minor convictions and its reported complexities must be interpreted with great care. Although “spent” convictions do not need to be disclosed when applying for most jobs, they must be disclosed to certain prospective employers. Specifically, some jobs are exempt from the Rehabilitation of Offenders Act 1974, such as working with children, elders and the disabled; senior roles in banking and financial services; certain law enforcement positions, including police and the judiciary; national security; certain prison service positions; certain professions in the health, pharmacy and legal fields; and private security. 59 Other limitations apply, such as the Rehabilitation of Offenders Act 1974 being specifically excluded by the Terrorism Prevention and Investigation Measures Act 2011. 60

4) Is the “right to be forgotten” making its way to the U.S.?

a) Court rulings?

The May 13, 2014, landmark ruling of the Court of Justice of the EU has sparked considerable public debate on whether the U.S. should have a “right to be forgotten.” 61 The U.S., with its time-honored constitutional protections of free expression, does not have a “right to be forgotten” similar to the one in the EU. 62 However, as of March 12, 2016, Google publicized details related to eight responses to search delisting requests from U.S. court orders, officials or residents. Google is the source of these details (which do not include content or alleged copyright infringement removal requests). 63

61 The U.S. Should Adopt The ‘Right To Be Forgotten’ Online, IntelligenceSquared Debates, dated March 15, 2015. https://www.youtube.com/watch?v=yvDzZ2q1ZQ&ebc=ANyPxKo3yp-3Y6wAwWcLMCOa0NSICOJo-XiwLyYrifVMVsnQr766639NwqPwLyZwlu03E7.
• Request Period: January to June 2014
  Request: We received an order to block several blog posts and search query results in relation to a cyberstalking case.
  Outcome: We discovered the court order was fraudulent. We reinstated the posts and search results.

• Request Period: July to December 2013
  Request: We received a third-party court order forwarded by a Tampa pharmacist asking us to remove two news articles from search results relating to his arrest for sexual solicitation of a minor over the internet pursuant to the court order.
  Outcome: We did not remove content in response to the order.

• Request Period: July to December 2013
  Request: We received a request accompanying a third-party court order by a CEO of a credit company who requested we remove 333 search results for articles that suggested he was engaged in fraudulent business dealings.
  Outcome: We did not remove content in response to the request as the court order was irrelevant to the content in question.

• Request Period: January to June 2013
  Request: We received a court order directed at a third party to remove six search results linking to news articles and to claims on the Ripoff Report website that allegedly defamed a company by suggesting it was involved in illegal activities.
  Outcome: We removed the search results linking to the Ripoff Report, but did not remove the news articles.

• Request Period: January to June 2013
  Request: We received a request from a local law enforcement official to remove a search result linking to a news article about his record as an officer.
  Outcome: We did not remove the search result.

• Request Period: July to December 2012
  Request: We received three court orders from different individuals that were addressed to third parties, along with requests to remove 452 search results that linked to websites that allegedly contain defamatory content.
  Outcome: We removed 70 search results that we determined to fall within the scope of the orders.

• Request Period: January to June 2012
  Request: We received three court orders to remove 641 search results for linking to websites that allegedly defame organizations and individuals.
  Outcome: We removed 233 of the search results requested, which fell within the scope of the orders.

• Request Period: July to December 2011
  Request: We received a court order to remove 218 search results that linked to allegedly defamatory websites.
Outcome: We removed 25 percent of the results cited in the request.”.64

b) Entity requests?

Google’s practice of delisting personal information links only for its EU version was challenged on June 12, 2015. On that date, France’s Commission Nationale de l’Informatique et des Libertés (CNIL) ordered Google to delete removed links not only from EU versions (e.g., google.fr in France), but also from other Google versions that appear internationally (e.g., google.com in the U.S.).65

In addition, on July 7, 2015, Consumer Watchdog, a citizen advocacy group, filed a U.S. Federal Trade Commission complaint, which essentially states that Google’s failure to offer the “right to be forgotten” in the U.S. is unfair and deceptive.66

Google disagreement with the CNIL’s order is recorded in a Google Europe blog dated July 30, 2015.67 In its response, Google cited reasons why it did not agree with the June 12, 2015, CNIL order, noting that the “right be forgotten” is the law in the EU but not internationally.

The following day, on July 31, 2015, the Association of National Advertisers (ANA) sent a letter that essentially urges the U.S. Federal Trade Commission to dismiss Consumer Watchdog’s July 7, 2015, complaint related to Google’s failure to offer the “right to be forgotten” in the U.S.68

Nevertheless, on September 21, 2015, the president of the CNIL issued a final order, rejecting Google’s informal appeal against the CNIL’s formal notice requesting that delisting, per the “right to be forgotten,” include all of the search engine’s international websites as well.69 The CNIL may fine Google up to 150,000 euros ($205,000) if this order is not followed. The CNIL’s ruling would also apply to other search engines, like Bing and Yahoo!.70

As previously noted, on February 11, 2016, it was reported that Google would be delisting not only personal information links from EU versions of Google, but also from the global Google website when it is accessed by a browser with an IP address that is associated with the EU.71 This reported advancement illustrates what appears to be Google’s operational ability to extend “right to be forgotten” delistings to the U.S. and to other local and global versions that serve Google users outside of the European Union.

---

5) Emerging trends with the “right to be forgotten” and the convergence of data protection and AML/CTF concerns in the Fourth EU AML Directive.

a) Requires that data protection rights of data subjects be integrated into AML/CTF policies and procedures related to customer information sharing.

The Fourth EU AML Directive was enacted on June 25, 2015, giving EU countries two years—by June 26, 2017—to implement its rules into their national laws. The “right to be forgotten” and the EU General Data Protection Regulation72 (likely to be adopted in early 2016, and then come into force two years later in 2018) appear to be generally consistent with the Fourth EU AML Directive, which requires that data protection rights of data subjects be integrated into AML/CTF policies and procedures related to customer information sharing.73

However, on closer inspection, the “right to be forgotten” within the framework of the General Data Protection Regulation appears to be subject to different interpretations,74 just as the convergence of data protection and AML/CTF concerns in the Fourth EU AML Directive has been complex and unclear. On July 4, 2013, the European Data Protection Supervisor filed a lengthy opinion that detailed data protection deficiencies in the Fourth EU AML Directive. For example, the opinion notes that customers should not be subject to AML/CTF investigations based on personal data that is inaccurate, collected incorrectly, or stored improperly. In addition, more specific references to data protection laws should replace general ones on certain critical issues, such as international data transfers to countries outside the EU.75 The European Data Protection Supervisor’s opinion was filed on July 4, 2013—about 10 months before the May 13, 2014, landmark ruling by the Court of Justice of the EU—which might help to explain why the “right to be forgotten” was not specifically mentioned in the opinion or later in the Fourth EU AML Directive.

b) Search engine link delistings that result from the “right to be forgotten” may complicate compliance.

On an operational level, search engine link delistings that result from the “right to be forgotten” may complicate compliance with the Fourth EU AML Directive, which requires greater data collection and retention and investigative scrutiny for negative news about client companies, identification and verification of beneficial owners through a registry,

---


and possible affiliations with politically exposed persons, especially when there are accusations of wrongdoing or investigations by regulators.\(^7^6\)

The Fourth EU AML Directive requires greater certainty with respect to information collected, used, and retained on customers and employees. But, the “right to be forgotten” raises operational questions like the following, complicated further by Google not publicizing its case-by-case approval or denial of each delisting request:

- To comply with the Fourth EU AML Directive, will it be acceptable for AML/CTF investigators to collect, use and retain content that has been delisted by private search engines?

- Will such delisted content be off limits in whole or in part?

- If such delisted content will not be off limits, will compliance with the Fourth EU AML Directive exempt a business from violating the “right to be forgotten” and EU data protection regulations?

- Will such collection, use and retention require proof that the delisted content is not “inadequate, irrelevant or no longer relevant, or excessive,” so that the business will not be subject to data protection-related penalties?

- Conversely, if such delisted content will be off limits, will compliance with the “right to be forgotten” and EU data protection regulations exempt a business from violating the Fourth EU AML Directive?

- Will a content delisting decision by a private search engine—like Google, Bing or Yahoo!—be sufficient to exempt a business from violating the Fourth EU AML Directive, or will such an exemption require that a European court or government entity also affirm the private search engine’s content delisting decision?

- To promote compliance with the Fourth EU AML Directive, should the beneficial owner registry be expanded to include a “right to be forgotten” registry that includes data from private search engines, cross-referencing capabilities, and search access by data subject name for a restricted audience that includes AML/CTF investigators and law enforcement?

EU efforts to harmonize the Fourth EU AML Directive and the “right to be forgotten” and EU data protection regulations could help to address such operational questions.

6) **Examples of international influence of the “right to be forgotten” in three selected Western Hemisphere countries—Argentina, Colombia and Mexico.**

Google has numerous top-level domains that correspond to several dozen countries. This section takes a closer look at three of those countries—Argentina, Colombia and Mexico.

Argentina, Colombia and Mexico each has a version of the “right to be forgotten,” which is generally known in Spanish as el derecho al olvido. However, at this time, each of these three countries generally requires a court order for individuals to have search result links to personal information delisted by Google.

Unlike the EU, Google does not have official delisting request processes for Argentina, Colombia and Mexico, which are briefly discussed below. Nevertheless, Google regularly receives requests from courts and government agencies from a wide variety of countries, including Argentina, Colombia and Mexico, to remove information from Google products, such as blog posts, YouTube videos, or search results. In its Google Transparency Report “Explore Requests” from March 12, 2016, Google states: “We closely review these requests to determine if content should be removed because it either violates the law or our community policies.”

a) Examples of favorable and unfavorable link delisting decisions that have been provided publicly by Google for Argentina, Colombia and Mexico.

Argentina

As of March 12, 2016, Google publicized details related to four responses to search delisting requests from the Argentine government. Google is the source of these details (which do not include content or alleged copyright infringement removal requests):

- “Request Period: January to June 2013
  Request: We received a court order to remove 1385 search results for linking to information that allegedly associated an actor with pornography.
  Outcome: We did not remove the search results and we appealed and the order was reversed.

- Request Period: January to June 2013
  Request: We received a phone call to remove a Google Autocomplete entry linking a politician’s name with an illicit drug.
  Outcome: We did not remove the entry.

- Request Period: January to June 2012
  Request: We received a court order to remove 120 search results for linking to sites that allegedly reference individuals.
  Outcome: We did not remove content in response to this request because the URLs listed did not reference the individuals cited in the order.

---


• Request Period: January to June 2010

Request: The courts in Argentina issued two orders that sought the removal of every search result mentioning a particular individual’s name in association with a certain category of content. The number of search results at issue well exceeds 100,000 results.

Outcome: We did not attempt to approximate the number of individual items of content that might be encompassed by those two court orders. Google appealed those orders.\(^80\)

Colombia

As of March 12, 2016, Google did not publicize details related to search delisting requests from the Colombian government (although Google publicized details on one content removal request).\(^81\)

Mexico

As of March 12, 2016, Google did not publicize details related to search delisting requests from the Mexican government (although Google publicized details on one content removal request).\(^82\)

b) Key case(s) in Argentina, Colombia and Mexico.

Argentina

Argentina has an uncommon relationship with the EU that Colombia and Mexico do not have. Article 25 of the European Union Data Protection Directive states that data can be sent to a country outside the EU only if the destination country is able to ensure an adequate level of data protection.\(^83\) Argentina is included in this report, because it is one of a few countries globally that the European Commission has recognized as providing adequate data protection and, therefore, deemed as acceptable destinations for data transfers. Other such acceptable data transfer destinations include Andorra, Canada (commercial organizations), Faeroe Islands, Guemsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.\(^84\)

---

http://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=all.

http://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=all.

http://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=all.

\(^83\) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.  

\(^84\) Commission decisions on the adequacy of the protection of personal data in third countries, The European Commission.  
Note: Not included in the above list are the U.S. Department of Commerce’s Safe Harbour Privacy Principles, which were invalidated by the ruling of the Court of Justice of the European Union in Maximilian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, dated October 6, 2015.  
The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid, The Court of Justice of the European Union, dated October 6, 2015.  
Despite Argentina’s uncommon relationship with the EU, Google’s delisting request process for individuals is not set up at this time to receive requests from citizens of Argentina. Individual citizens of Argentina wanting to delist links to personal information about themselves basically have two options: 1) petition a public judicial entity for a decision ordering the internet search engine to delist links to personal information; or 2) send an ad hoc request to the internet search engine itself and hope for the best.

Instead of an Argentine “right to be forgotten” per se, Section 43 of Argentina’s Constitution and Section 16 of the Data Protection Act of Argentina - Law 25,326 includes a right of suppression. Accordingly, the data subject can file a complaint if it appears that the data bank is not protecting personal information based on Argentinean law. Section 43 of Argentina’s Constitution further provides for “habeas data,” a special judicial remedy called “amparo” that essentially elevates personal data protection to the status to that of a fundamental right.

In one notable 2009 lawsuit, Google and Yahoo were co-defendants when Virginia Da Cunha, an Argentine celebrity, sued the search engines for removal of photographs that had been posted on sex-oriented websites. Although Da Cunha’s suit was initially successful at the trial level, an Argentine appellate court reversed the trial court’s decision in 2010, finding that the search engines were not responsible for the posting. Several dozen similar suits have reportedly been filed, similar to the one filed by Da Cunha.

Colombia

Google’s delisting request process for individuals is not set up at this time to receive requests from citizens of Colombia. Individual Colombian citizens wanting to delist links to personal information about themselves basically have two options: 1) petition a public judicial entity for a decision ordering the internet search engine to delist links to personal information; or, 2) send an ad hoc request to the internet search engine itself and hope for the best.

Instead of a Colombian “right to be forgotten” per se, reputation and privacy are treated as fundamental rights protected by Article 15 of Colombia’s Constitution of 1991. When privacy rights, data protection or habeas data are allegedly not protected, data owners may file a writ of protection (or acción de tutela) before a Colombian magistrate, per Colombian decree 2591 of 1991. In addition, Article 8, Rights of Holders, of the Colombia Statutory Law of 2012 1581 general provisions for the protection of personal data includes a right of deletion. Such a right of deletion gives the data subject, or the

---

data subject’s legal representative, the right to file a complaint if the individual feels that the data controller is not protecting personal information based on Colombian law.

Influence of the "right to be forgotten" in Colombia often points to two cases against Google Colombia. In the first case, Google Colombia was not held responsible for a newspaper, *El Tiempo*, reporting that Guillermo Martínez Trujillo was associated with a Colombian mafia cartel.92

In the second case—which was brought by a claimant who uses the fictitious name Gloria—the court drew a search engine versus website distinction when it ruled that Google Colombia should not be ordered to delist a human trafficking-related article in *El Tiempo*, because to do so would amount to censorship and violate principles of net neutrality and free expression, but *El Tiempo* itself should take steps to make sure that the article cannot be listed by search engines using existing software tools.93 For example, as Google reports in several languages, a robots.txt file is at the root of a website that indicates which parts should not be accessed by search engine crawlers.94 This second case also references several intervenciones, which appear to be from intervenors (organizations or persons), who want to participate in a proceeding because they believe the proceeding or its outcome may affect their rights or duties. Intervenors should not be confused with a friend of the court (Latin singular, *amicus curiae*; plural, *amici curiae*), who is not a party in the proceeding, but who nevertheless provides advice or suggestions by filing a brief with the magistrate.

**Mexico**

Google’s delisting request process for individuals is not set up at this time to receive requests from citizens of Mexico. Individual Mexican citizens wanting to delist links to personal information about themselves basically have two options: 1) petition a public judicial entity for a decision ordering the internet search engine to delist links to personal information; or, 2) send an ad hoc request to the internet search engine itself and hope for the best.

Instead of a Mexican “right to be forgotten” per se, Article 29 of Mexico’s data protection law, effective in 2010, includes a right of cancellation.95 Such a right of cancellation gives the data subject, or the data subject’s legal representative, the right to file a complaint if the individual feels that the data controller is not protecting personal information based on Mexican law.

On May 27, 2015, the *Wall Street Journal* reported that Google is appealing a noteworthy January 26, 2015 decision from the Mexican Federal Institute for the Access

---

to Information (IFAI). Citing Mexico’s right of cancellation, the IFAI ruled in favor of Carlos Sánchez de la Peña, a prominent Mexican businessman who requested that Google Mexico remove links to three articles that reference not only his late father’s business dealings, but also the Mexican government’s bailout of several bad loans. Many in Mexico, including journalists and free speech advocates, have criticized this IFAI ruling and Google for not stressing the public interest served by retaining the links in this matter, noting the association between Mr. Sánchez de la Peña’s family and the family of former Mexican President Vicente Fox.

7) AML/CTF investigative tips to consider as search engines respond to delisting requests from individuals and government orders.

✓ Assume that data subjects know about the “right to be forgotten”

Delisted news article examples from HiddenFromGoogle.com, the Telegraph, and the British Broadcasting Corporation illustrate that the “right to be forgotten” is known not only to individuals who would like to protect their private information and reputations justifiably, but also to others who would like to evade detection by keeping “unwanted” search results out of public view. The Moldovan court order case discussed earlier evidences how alleged money launderers and tax evaders can use multidisciplinary knowledge to execute, obfuscate and conceal highly complex conspiracies.

✓ Ask data subjects about all countries of citizenship and residency; request notification of future changes

Citizenship or residency in a country that has or will have the Right to Be Forgotten could be a red flag for an AML/CTF investigative blind spot, especially if the citizenship or residency is obtained relatively recently, through foreign investments, a family member, or without an actual living address in the countries of citizenship or residence. Names on official supporting documents should match; discrepancies should be explained, since they could be a red flag for financial transactions being conducted under more than one name. Some European golden investor visas require proof that the foreign investment is sourced from AML compliant funding, so this line of thinking, documentation, and investigation is essential and not uncommon.

✓ Ask data subjects about all names used in the past and present, including nicknames and aliases; request notification of future changes

Multiple names or discrepancies should be explained, since they could be a red flag for financial transactions being conducted under more than one name. Google’s delisting form allows European residents to request search result delisting based on one or

multiple names used; for example, maiden name, married name(s), nickname(s), and alias(es). Proof of identity is required by Google, but not necessarily from passports or other government issued identification; this might allow other types, such as identification issued by employers, academic institutions, health care entities, financial institutions, or other businesses. Photographs can be obscured in a request to Google, unless the URL for which delisting is requested includes a photograph of the requester.99

✓ Start external online research with metasearch engines, if possible

For AML/CTF investigations, external internet research should start with a metasearch engine 100 that aggregates results from several search engines before narrowing investigative parameters using specific search engines that may have different scopes and capabilities (e.g., Google.es for local content in Spanish from Spain). Using a metasearch engine to access results initially from several search engines makes sense, since no single search engine covers the entire internet.101

The broadest possible search coverage will help to overcome AML/CTF investigative blind spots that could result from search engine link delisting. Just as visual blind spots are harder to detect when visual fields overlap from two eyes open, search result delisting blind spots may disappear when metasearch engines draw from two or more overlapping search engines.

Please note that some metasearch engines—like StartPage and Ixquick—are privacy-oriented, not only incorporating encryption, but also refraining from recording IP addresses, monitoring searches and using cookies.102

Metasearch engines may provide public notice about the Court of Justice’s landmark ruling per the “right to be forgotten.” Both StartPage103 and Ixquick104 do provide such public notice, clarifying that they rely on the search indices of search engines, so it would likely be more efficient to request delisting from search engines (like Google, Bing and Yahoo!) instead.

✓ Keep search queries general and do not rely solely on name searches

When search engines delist links to personal information based on the “right to be forgotten,” they are removing the links only but not disturbing the underlying content. Such content can still be retrieved through the metasearch engine or search engine, if

---

101 Study Guide for the CAMS Certification Examination, Fifth Edition, Association of Certified Anti-Money Laundering Specialists (ACAMS), 2012, (page 263: “A metasearch engine is a search tool that sends user requests to several other search engines and/or databases and aggregates the results into a single list or displays them according to their source.”).
the viewer uses search terms other than the data subject’s name associated with the delisting request.

After a delisting request has been accepted, personal information links would likely not show up if the data subject’s name “John Doe” were typed into the search field. But that should not prevent the same content from showing up if other information related to John Doe were typed into the search query, such as the name of a business, an activity, the names of other associated individuals, or other details included in the content. This would be consistent with search queries encouraged for SAR development. For SARs, research due diligence should not be limited to internet searches on the subject’s name only; rather, it should include other elements, such as typical business activity.\(^\text{105}\)

- Before name searching, mitigate possible unintended consequences

AML/CTF investigations require confidentiality, including when SARs are being developed pursuant to federal law in the U.S.\(^\text{106}\) The “right to be forgotten” may prompt some readers concerned about disappearing search results to react by “Googling” various iterations of a data subject’s name, to see if he or she has been delisted. Assuming cybercriminals are expecting such a reaction, this section focuses on some of the name search leakage hazards that exist and ways to minimize them through increased awareness and collaboration with your internal or external information technology security team.

- Possible search leakage to data subjects through IP address lookup: Internet companies are developing products that will allow individuals to identify who is initiating general internet search queries that include their name. One such internet company, an online reputation management firm called BrandYourself.com, LLC, helps subscribers to determine who is searching on their names on Google.\(^\text{107}\) BrandYourself creates a profile for the subscriber that reportedly shows where profile visitors work and where they are located through IP address lookup. BrandYourself reportedly has a database of publicly-available IP addresses for companies to create this feature. BrandYourself reportedly matches its database of IP addresses for companies with IP addresses of profile visitors.

On March 12, 2016, a general Google “site:brandyourself.com” search yielded “[a]bout 162,000 results,” indicating that there are about 171,000 name profiles that use the BrandYourself subdomain; for example, “johndoe.brandyourself.com.” To find out quickly if John Doe has such a BrandYourself profile (without clicking on it), generally search “site:brandyourself.com john doe” on Google; the BrandYourself profile for “John

\(^{105}\) Study Guide for the CAMS Certification Examination, Fifth Edition, Association of Certified Anti-Money Laundering Specialists (ACAMS), 2012. (page 263: “A metasearch engine is a search tool that sends user requests to several other search engines and/or databases and aggregates the results into a single list or displays them according to their source.”).


Doe” should appear at or near the top of the list, if there is one by that name spelling.108

To avoid BrandYourself profile tracking when using Google, one option is to initiate name searches using Google News, an aggregation service of recent and archived websites that Google offers at no cost to the user. In the test that was conducted on March 12, 2016, BrandYourself profiles appeared in general Google name search results, but not in name search results for Google News.

BrandYourself has other complementary features that could be used by data subjects to disguise themselves or others with the same name, such as:

- The ability to control Google search result positioning using Search Engine Optimization (SEO), so that positive search results might suppress “unwanted” Google search results. Because of this feature, AML/CTF investigators and law enforcement would likely have to dig deeper to detect “unwanted” Google search results for the data subject or others who share the data subject’s name. Arguably, suppressing “unwanted” Google search results may benefit Google, which might actually gain more “stickiness” and advertising revenue when visitors, including AML/CTF investigators, have to spend more time digging for details.109

- A concierge service (plans reportedly start at $399 USD per month), in which a subscriber can purchase ghost-written articles to mimic an industry thought leader online. Publication of these ghost-written articles reportedly helps to overshadow unwanted search results.

- The ability to hide your identity if you visit another person’s BrandYourself profile.

One of BrandYourself’s competitors is Viable Ventures LLC (DBA "Naymz"), another online reputation management firm.110 Naymz subscribers create a visitor profile that can track visit dates, visitor location, visitor IP address, visitor name (if available), and the web page where the visitor found the link to the profile. Such tracking details can be provided to the subscriber instantly through visit notification emails.

Another BrandYourself competitor is Reputation.com, Inc., an online reputation management firm whose services include changing the order of positive and unwanted search results, monitoring privacy vulnerabilities, and creating and disseminating content.111 On its Frequently Asked Questions webpage, Reputation.com stands apart from competitors where stating that it elects not to accept cases where information of public interest might be obscured, such as when there are ongoing court proceedings, indictments for sexual or violent

108 BrandYourself.com is a good idea with only fair execution, Ardamis. https://ardamis.com/2012/03/20/brandyourself-good-idea-fair-execution/.
crime, crime involving children, or felony fraud convictions,\(^{112}\) although such a statement does not clearly cover earlier investigations, allegations, or suspicions of wrongdoing.

Is your firm’s IP address fixed and visible publicly? If so, anonymous internet browsing may be an alternative to prevent such search leakage to data subjects, including options like a Virtual Private Network (VPN), web-based proxies like Proxify and Anonymouse, and manual proxy servers like ProxyNova. One VPN that might be of interest is Disconnect, which allows private, anonymous searches of Google, Bing, Yahoo! and DuckDuckGo on desktop computers, laptops and mobile devices.\(^{113}\)

- **Possible search leakage to data subjects through security vulnerabilities:** Cybercriminals may use word searches (including name searches) to load malware, spyware and spam on computers, lure users to malicious websites, and report keystrokes and online activities,\(^{114}\) for example:
  - **Keystroke logging:**\(^{115}\) Through “keylogging,” cybercriminals may record every keystroke that someone presses using a computer, including the name of the data subject whose transactions are the subject of a confidential AML/CTF investigation.\(^{116}\) Keylogging software is widely available to anyone on the internet.\(^{117}\)
  - **Browser use tracking:** Through malicious browser plugins, cybercriminals may monitor browser use, such as which websites and pages are visited, so that confidential browser use might be reported to an external party.\(^{118}\) As-needed updates to anti-malware software and patches to computer operating systems can help prevent keylogging and malicious browser plug-in threats, among others, in addition to prudent internet and email management.\(^{119}\)
  - **Malware from trusted websites:** Through “maladvertising,” cybercriminals may covertly slip malware onto computers through the lure and loading of legitimate and fraudulent website advertising that may be triggered by

---


\(^{113}\) Disconnect. https://search.disconnect.me.


words (like a data subject’s name) that are typed into search engines.\textsuperscript{120} Maladvertising blocking options include blocking all advertising from your employee’s devices, advertising blocking browser plugins, or browser settings to note malicious webpage content.\textsuperscript{121}

- **Misdirected investigations:** Google has reportedly made significant efforts to curb the external manipulation of search results for a specific word or set of words. However, even the Vatican has been the victim of this unscrupulous practice, known as “Google bombing.”\textsuperscript{122}

Social media website use can expose AML/CTF investigators to malware and other computer threats,\textsuperscript{123} especially when social media profiles have so much professional and personal information that it is relatively easy for cybercriminals to confirm which specific entities, teams, or individuals they want to target. That said, perhaps this report section will result in AML/CTF investigators exercising greater care when posting information about themselves and their professional titles, activities and networks on social media websites.

One option might be for computers used for online AML/CTF investigations at work to not be used to access personal email, work email, social media websites or other online activities. Another option might be for one computer to be used, but with browsers used for separate purposes.\textsuperscript{124} For example, one browser could be used for AML/CTF investigations; another browser, for work email; another browser, for other online activities, such as social media websites and personal email, as needed.

Protecting the confidentiality and privacy of internet searches for AML/CTF investigations also requires attention to web browser security issues. The Electronic Frontier Foundation makes available three privacy-oriented tools that may be of interest when doing online confidential research to support AML/CTF investigations:

- **HTTPS Everywhere:** The Electronic Frontier Foundation provides a web browser extension that encrypts browser communications with many major websites when using Firefox, Firefox for Android, Chrome and Opera.\textsuperscript{125}

\textsuperscript{125} HTTPS Everywhere. Electronic Frontier Foundation. https://www.eff.org/https-everywhere.
• Privacy Badger: The Electronic Frontier Foundation provides this web browser add-on that blocks spying ads and invisible trackers.\textsuperscript{126}

• PANOPTICCLICK—Is your browser safe against tracking?: The Electronic Frontier Foundation provides an online tool that analyzes the susceptibility of your web browser’s configurations to online identification and invasive tracking.\textsuperscript{127}

Coordination with your information technology security professionals should help to prevent these and other threats. To efficiently detect such threats, repair vulnerabilities, and secure networked desktop, laptop, mobile and server computers, consider endpoint security/management solutions like IBM BigFix.\textsuperscript{128}

• Possible search leakage to data subjects or other third parties through unencrypted online searching: Eavesdropping by third parties is a vulnerability that could compromise confidentiality. Make sure that your internet searches are secure through encryption. For example, note the “s” for “Secure Sockets Layer” or “SSL” encryption in the https://www.google.com web address.\textsuperscript{129} An encrypted search engine should be used when doing online confidential research to support AML/CTF investigations. For Google, Secure Sockets Layer (SSL) encrypts the connection between Google and the visitor. This should prevent third parties from seeing visitor search results and login information. SSL does not provide complete security. It does not always hide the fact that you visited Google.com or search terms types. For example, when visiting another website from the Google search results page, that website may be able to track what site you came from or search terms used. As an alternative, DuckDuckGo is a privacy-oriented encrypted search engine that refrains from recording IP addresses, monitoring searches and using cookies.\textsuperscript{130}

• Localization and personalization of searches: If two search engine users were to perform separate search queries on “John Doe” by name, they would likely come up with different search result links to choose from. Search results would likely be different based on localization and personalization from search engine algorithms.\textsuperscript{131} Different results could lead search engine users to overlook significant details that support or militate against the filing of a SAR.

Localization can affect search results by taking into account your computer’s settings and IP address. If using Google, location can be changed reportedly by using versions for particular countries or by changing location to a different city or zip code when using Google.com. To turn off Google’s automatic localization when traveling, the “No Country Redirect” command of www.google.com/ncr will take you back to Google.com in English and without local search results.\textsuperscript{132}

\textsuperscript{126} Privacy Badger. Electronic Frontier Foundation. https://www.eff.org/privacybadger.


\textsuperscript{128} The endpoint platform for organizations of every size, IBM BigFix. http://www-03.ibm.com/security/bigfix/.


Personalization can affect search results by taking into account earlier search and click history, among several factors. If using Google, “personalized web search” can be turned off reportedly either by adding “&pws=0” at the end of Google’s search URL or by using the Chrome incognito version. Alternatively, DuckDuckGo presents itself as a privacy-driven, location-agnostic alternative to Google on issues such as localization and personalization.

- Watch out for contrived search results: Checking one’s references with a healthy skepticism makes sense when reviewing search results, given some unscrupulous online reputation management practices, such as:
  - Fake bad reviews or complaints about individuals or businesses to manufacture demand for online reputation management software and services
  - Positive information being withheld from public view
  - Individuals overshadowing unwanted search results by mimicking an industry thought leader with online publication of ghost-written articles
  - Scammers extorting payment(s) to remove or suppress unwanted content or search results

For AML/CTF investigations, both derogatory and favorable search results about individuals or businesses should be corroborated for accuracy, completeness and relevance to specific individuals or businesses in question.

8) Conclusion and Next Steps

Momentum for an online “right to be forgotten” is growing steadily, now that Google’s delisting program has been operationalized to cover 33 European countries, at least 17 additional countries have reportedly implemented, or are expected to implement, versions of the “right to be forgotten,” and the possibility of an online “right to be forgotten” is being actively discussed in the U.S. and other countries.

Consistent with this growing momentum, three interrelated exigencies are timely with respect to AML/CTF investigations:

- Verify the practicality of your firm’s AML/CTF investigative standards, procedures and practices, mindful of current and potential investigative blind spots prompted by an online “right to be forgotten.”

---

especially important if your firm is a U.S.-based financial institution that has a global reach (affiliates or correspondent relationships) and/or has customers or employees who are residents of countries with a “right to be forgotten.” For example, should your firm’s investigative standards be restated in more general terms? Should related investigative procedures be restated more flexibly to cover variables such as the possible search engine delisting or suppression of information on customers or employees, red flag indicators, the use of metasearch engines versus search engines, or the localization and personalization settings on computers used by AML/CTF investigators? Are actual investigative practices inadvertently introducing unintended consequences and security risks that should be mitigated?

- **Increase data privacy/protection and cyber security education relevant to AML/CTF investigations.** Education within the AML/CTF community should be encouraged on how an online “right to be forgotten” can affect financial crime investigations. This should be extended not only to AML/CTF investigators involved with transaction monitoring and know your customer groups, but also to other stakeholders such as business controls, auditors, independent monitors, law enforcement, and AML/CTF and data privacy/protection law makers and regulators in the U.S., Europe and other countries that are following Europe’s lead. Such information sharing with law makers and regulators could facilitate regulatory and operational harmonization of AML/CTF and data privacy/protection laws in Europe and other jurisdictions.

- **Encourage information sharing between internet search and metasearch engines and the AML/CTF community.** Google’s Advisory Council on the “right to be forgotten” panel and meetings evidence the relative lack of executive and operational input from various sectors impacted by AML/CTF investigative blind spots—banking; government, securities broker/dealers and money services businesses; insurance; accounting and law firms; gaming organizations; entities that monitor and combat human trafficking; credit, debit and prepaid card companies; real estate agencies; jewelry and precious metals dealers; and law enforcement. Perhaps ACAMS could be the AML/CTF community’s focal point for bridging this information gap with internet search and metasearch engines.

The importance of these three interrelated points cannot be overlooked. Addressing them directly and proactively should elucidate further how an online “right to be forgotten,” and related AML/CTF investigative blind spots, might impact global transaction monitoring going forward.

9) **Sources Cited**

<table>
<thead>
<tr>
<th>Source</th>
<th>Details</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicant</td>
<td>Arrested for money laundering.</td>
</tr>
<tr>
<td>Ardamis</td>
<td>BrandYourself.com is a good idea with only fair execution, Ardamis. <a href="https://ardamis.com/2012/03/20/brandyourself-good-idea-fair-execution/">https://ardamis.com/2012/03/20/brandyourself-good-idea-fair-execution/</a>.</td>
</tr>
<tr>
<td>Bing</td>
<td>Request to Block Bing Search Results In Europe. <a href="https://www.bing.com/webmaster/tools/eu-privacy-request">https://www.bing.com/webmaster/tools/eu-privacy-request</a>.</td>
</tr>
<tr>
<td>China Copyright and Media</td>
<td>National People’s Congress Standing Committee Decision concerning Strengthening Network Information Protection, China Copyright and Media, dated December 28, 2012.</td>
</tr>
<tr>
<td>Disconnect.me</td>
<td>- Disconnect. <a href="https://search.disconnect.me">https://search.disconnect.me</a>.</td>
</tr>
<tr>
<td>DuckDuckGo</td>
<td>- DuckDuckGo: We don't collect or share personal information.</td>
</tr>
<tr>
<td>Source</td>
<td>Resource Details</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Source</td>
<td>Articles</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Forbes                        | • How Brazil and the EU Are Breaking the Internet, Forbes, dated May 19, 2014.  
|                               | • The Dark Side Of Reputation Management: How It Affects Your Business, Forbes, dated May 9, 2013.  
|                               | • Want To Live In Europe? "Buy" A Residency Permit, Forbes, dated September 29, 2013.  
| Forget.me                     | • Frequently Asked Questions - The Right To Be Forgotten, Forget.me.  https://forget.me/faq.  
| France – government documents | • CNIL orders Google to apply delisting on all domain names of the search engine, dated June 12, 2015.  
|                               | • Right to delisting: Google informal appeal rejected, dated September 21, 2015.  
| Free Internet Project (The)   | • Google appeals Mexico’s right to be forgotten decision in favor of Carlos Sánchez de la Peña related to family business dealings, The Free Internet Project.  
|                               | http://thefreeinternetproject.org/blog/google-appeals-mexicos-right-be-forgotten-decision-favor-carlos-sanchez-de-la-pena-related.  
| Freedom House                 | • Mexico 2015, Freedom on the Net.  
| GoDaddy                       | • GoDaddy.com Whois search results for Hiddenfromgoogle.com.  
|                               | • Top Golden Visa Applicant Countries, La Vida.  
| Google                        | • Adapting our approach to the European right to be forgotten, Google Europe Blog, dated March 4, 2016.  
|                               | http://googlepolicyeurope.blogspot.co.uk/2016/03/adapting-our-approach-to-european-right.html.  
|                               | • Google Legal Help - Search removal request under data protection law in Europe.  
|                               | https://support.google.com/legal/contact/lr_eudpa?product=webs
<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Advisory Council to Google on the Right to be Forgotten, dated February 6, 2015.</td>
<td><a href="https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjivV0hNbDA/view?pli=1">https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjivV0hNbDA/view?pli=1</a></td>
</tr>
<tr>
<td>The Advisory Council to Google on the Right to be Forgotten, Google.</td>
<td><a href="https://www.google.com/advisorycouncil/">https://www.google.com/advisorycouncil/</a></td>
</tr>
<tr>
<td>HiddenFromGoogle</td>
<td>HiddenFromGoogle.com. <a href="http://hiddenfromgoogle.com">http://hiddenfromgoogle.com</a></td>
</tr>
<tr>
<td></td>
<td>Social Engineering Attackers Deploy Fake Social Media Profiles, IBM Security Intelligence, dated November 6, 2015. <a href="https://securityintelligence.com/social-engineering-attackers">https://securityintelligence.com/social-engineering-attackers</a></td>
</tr>
<tr>
<td><strong>IFEX (formerly the International Freedom of Expression Exchange)</strong></td>
<td>What are the implications of the right to be forgotten in the Americas?, IFEX. <a href="https://www.ifex.org/americas/2015/09/22/derecho_olvido/">https://www.ifex.org/americas/2015/09/22/derecho_olvido/</a>.</td>
</tr>
<tr>
<td>Intelligence² Debates</td>
<td>The U.S. Should Adopt The 'Right To Be Forgotten' Online, IntelligenceSquared Debates, dated March 15, 2015. <a href="https://www.youtube.com/watch?v=yvDzW-2q1ZQ&amp;ebc=ANyPxKo3yp-3Y6wAlwWcLMCOAo0NSfCOJo-XivLyYufMV6nSqGqp6t6693GNgqPwLyZwlu03E7">https://www.youtube.com/watch?v=yvDzW-2q1ZQ&amp;ebc=ANyPxKo3yp-3Y6wAlwWcLMCOAo0NSfCOJo-XivLyYufMV6nSqGqp6t6693GNgqPwLyZwlu03E7</a>.</td>
</tr>
<tr>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Japan Times (The)                           | Right to be forgotten' on the Internet gains traction in Japan, The Japan Times, dated December 9, 2014.  
| La Razón de México                          | Google litiga contra el IFAI por el "derecho al olvido," La Razon de Mexico, dated April 28, 2015.  
| Lifehacker                                  | Avoid Getting Redirected to Country-Specific Versions of Google, Lifehacker, dated August 9, 2015.  
| Los Angeles Times                           | FBI chief: San Bernardino shooters did not publicly promote jihad on social media, Los Angeles Times, dated December 15, 2015.  
| Mashable                                    | Global Malware Hackers Use Social Media to Escape Cyber Sleuths, Mashable, dated April 23, 2013.  
| McAfee                                      | The 2015 Most Dangerous Celebrity is Putting Devices in a State of Trance, McAfee Blog Central, dated September 28, 2015.  
   Responsable: Google Mexico, S. de R.L. de C.V. Expediente: PPD.0094/14, Instituto Federal de Acceso a la Informacion y |
<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reddit</td>
<td>- “Syed Farook” - Some results may have been removed under data protection law in Europe, Reddit, dated December 3, 2015.  <a href="https://www.reddit.com/r/european/comments/3v9d6k/syed_farook_some_results_may_haveBeen_removed/">https://www.reddit.com/r/european/comments/3v9d6k/syed_farook_some_results_may_haveBeen_removed/</a>?.</td>
</tr>
<tr>
<td>Riviera Estate Spain</td>
<td>- 4 signs that the Spanish property market is bottoming out, Riviera Estate Spain, dated December 6, 2014.  <a href="http://rivieraestatespain.net/2014/12/06/4-signs-that-the-spanish-property-market-is-bottoming-out/">http://rivieraestatespain.net/2014/12/06/4-signs-that-the-spanish-property-market-is-bottoming-out/</a>.</td>
</tr>
<tr>
<td>SEO Blog</td>
<td>- Ten things you need to know about the EU’s decision on the ‘right to be forgotten’ on Google, SEO Blog, dated June 2, 2014.  <a href="http://www.searchengineoptimizations.co/2014/06/02/ten-things-need-know-eus-decision-right-forgotten-google/">http://www.searchengineoptimizations.co/2014/06/02/ten-things-need-know-eus-decision-right-forgotten-google/</a>.</td>
</tr>
<tr>
<td>Source</td>
<td>Details</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>12 C.F.R. § 563.180 (U.S. Office of Thrift Supervision)</td>
</tr>
<tr>
<td></td>
<td>12 C.F.R. §§ 353.1–353.3 (U.S. Federal Deposit Insurance Corporation)</td>
</tr>
<tr>
<td></td>
<td>31 C.F.R. § 103.18 (U.S. Treasury Department)</td>
</tr>
<tr>
<td></td>
<td>31 U.S.C. § 5318(g)</td>
</tr>
<tr>
<td></td>
<td>Fraud Alert – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud, Internet Crime Complaint Center, dated September 17, 2012.</td>
</tr>
</tbody>
</table>


| Wikimedia Foundation (The) | - Notices received from search engines, The Wikimedia Foundation. [https://wikimediafoundation.org/wiki/Notices_received_from_search_engines](https://wikimediafoundation.org/wiki/Notices_received_from_search_engines).

