HOW MALIGN FORCES LEVERAGE DEFAMATION LAWS AND DATA PRIVACY LEGISLATION TO UNDERMINE DEMOCRACY

Privacy experts, consumer advocates and consumers themselves would be the first to say that privacy legislation, principally the gold standard – the EU GDPR (General Data Protection Regulation), is a welcome development. Agreed, but there was at least one arguably unintended consequence of the EU GDPR, which is being exploited to the detriment of investigative journalists, human rights defenders and other activists, writers and publishers who speak out or publish material on matters of public interest. In short, those wishing to shut down research or publicity on such matters have an additional weapon at their disposal, namely the ability to obtain information about themselves, and bring lawsuits, under data protection rules. I focus below on the use of this weapon principally in British courts.

Background and Context

The increasing use of data protection laws to silence critics needs to be seen in the context of a broader effort to silence journalists, civil society researchers and others reporting on kleptocracy, corruption, illicit finance and other malign activities. That broader landscape is littered with costly, meritless lawsuits brought by powerful figures to intimidate, distract, potentially bankrupt and ultimately silence critics. In the process, free speech and public debate are chilled. These lawsuits are known as strategic litigation against public participation ("SLAPPs").[1]

As many have reported (*see, e.g.*, " An anti-SLAPP law is essential to the health of UK democracy" and "The Use of SLAPPs to Silence Journalists, NGOs and Civil Society"), the threat of SLAPPs has prompted many media outlets and others to self-censor legitimate reporting on corruption, illicit finance, political wrongdoing and more, while others may find it necessary to "correct" the record or even apologize for statements simply to avoid the cost and other significant burdens of responding to, let alone defending against, meritless legal challenges.

---

[1] The term "strategic litigation against public participation" was coined by two professors at the University of Denver, George W. Pring and Penelope Canan. In their 1996 book, SLAPPs: Getting Sued for Speaking Out, the Pring and Canan largely focused on suits targeting environmental activists. In the United States, even the Racketeering Influenced and Corrupt Organizations (RICO) Act has been deployed to chill the speech of civil society activists. According to reporting by the Reporters Committee for Freedom of the Press, as of September 2023, 33 states and the District of Columbia have anti-SLAPP statutes (which, admittedly, vary significantly as to coverage, from state to state).

For a comprehensive review of British-based SLAPPs (including use of GDPR claims, *see* Foreign Policy Center Project Director Susan Coughtrie's report, "London Calling: The issue of legal intimidation and SLAPPs against media emanating from the United Kingdom." The scourge of SLAPPs is by no means limited to Britain. *See e.g.,* Freedom House analysts Jessica White and Alexandra Karppi, "European Journalism on the Docket Thanks to Bogus Lawsuits" (October 2023), as well as the report issued by the Coalition Against SLAPPs in Europe (CASE) "Shutting out Criticism: How SLAPPs Threaten European Democracy" (March 2022) and the report prepared for the European Parliament "The European Media Freedom Act: media freedom, freedom of expression and pluralism" (July 2023). *See also* the article written by Melinda Rucz in the Journal of Media Law ("SLAPPed by the GDPR: protecting public interest journalism in the face of GDPR-based strategic litigation against public participation").

Essentially, SLAPPs shift discourse and debate that rightly belongs in the political sphere into the legal arena. The legal outcome of these lawsuits is not what matters; what matters is that the process typically is sufficient to drain capacity, morale and financial resources of the targets. The process also has an effect that goes beyond the direct targets of these legal actions, serving as a warning to others to remain silent.[2]

Never mind highly effective disinformation or misinformation campaigns. The ultimate goal of these legal processes is to silence criticism and change the subject. Unleashing these processes deprive citizens of the ability to form an opinion as to, or even to be aware of, matters of significant public interest, which is why they pose such a threat to democracy.

Expansion to Data Protection Actions

While defamation law historically has been the most common path for abusive lawsuits, in recent years data protection has provided to be fertile ground as well. As Oliver Bullough, author of "Butler to the World," set out in his May 2022 article in The Economist, "Why oligarchs love European data protection laws," when the GDPR was enacted, many thought that the "data" meant to be protected were limited to "the algorithmic index of our habits, interests and families stored" by social media companies. But data can mean almost any information (specifically, "any information relating to an identified or identifiable living individual"), and moreover, the GDPR enshrined a second protection in its Article 5, namely that personal data stored by "data controllers"[3] must be secure, lawfully processed and accurate.

While British defamation laws were tightened by, among other things, requiring a showing that a putative claimant had suffered "serious harm," claimants have found favorable judicial reception to claims under the GDPR (while the GDPR is EU law, it applies in Britain[4]). Claimants ("data subjects," meaning any person whose personal data has been collected or stored) can demand copies of any information any controller of data may have about them – so called "data subject access requests" ("DSARs"), and if that information turns out to be inaccurate, can sue that controller.

DSARs impose two burdens on data controllers. First, the data controller is required by law to respond within 30 days, meaning it must trawl through emails and texts for any relevant information. Second, a lawsuit can brought against the data controller even if the information

---

[2] It has been widely reported that, at the time she was murdered, Maltese journalist Daphne Caruana Galizia faced 47 civil and criminal defamation lawsuits from politicians and businesspeople.

[3] The EU GDPR defines a data controller is a person, entity or body who determines "determines the purposes and means of the processing of personal data." "Processing" means any action taken in respect of personal data, including among others collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use or disclosure. While the e-commerce website that collects your data (whether you inputted it or it is scrapped by virtue of browsing) is an obvious data controller, in the SLAPPs world, anyone who collected data is covered.

[4] The EU GDPR was incorporated into UK law at the end of the Brexit transition period under the European Union (Withdrawal) Act 2018 (EUWA) and modified by the Data Protection, Privacy and Electronic Communication (Amendments etc) (EU Exit) Regulations 2019 under the power in section 8 EUWA 2018 to create the UK GDPR. Data protection in the United Kingdom is also covered by the Data Protection Act 2018.

in question has not been published, regardless of where that data controller may physically be located, regardless of the level of diligence undertaken in compiling the information, and regardless of whether the information has caused serious harm – the relevant test is whether the information turns out to be inaccurate.

Thus far, subject data access claims in British courts have ensnared:

- Orbis Business Intelligence (co-founded by former intelligence officer Christopher Steele) twice (the first involving claims brought by three Russia oligarchs under predecessor legislation, and the second involving claims brought by Donald Trump, in each case involving information collected by Steele and leaked by Buzzfeed);
- Financial Times journalist and author of "Putin's People: How the KGB Took Back Russian and Then Took on the West" Catherine Belton and her publisher HarperCollins, who were named in a flurry of libel or data protection lawsuits by four Russian oligarchs and the state-owned energy conglomerate, Rosneft;
- Financial Times journalist and author of "Kleptopia: How Dirty Money is Conquering the World") Tom Burgis and his publisher, who were sued by Kazakh mining group Eurasian Natural Resources Corporation; and
- former Member of Parliament (MP) Charlotte Leslie, who ran an organization called the Conservative Middle East Council and who flagged donations to the Conservative Party by a major donor (in essence as part of diligence on the donor, apparently on the basis of open-source checks), who issued a DSAR against her seeking access to details of confidential conversations she had, and brought a data protection claim (actually two), which the donor ultimately discontinued, as well as a defamation claim, which ultimately was struck out.

Various MPs, citing the Belton, Burgis, Leslie and Steele cases, have called attention on the floor of the Commons to the SDAR issue and the broader assault on press freedom and civil society reporting via SLAPPs. Note that while all of the foregoing examples involve British citizens, the UK Court of Appeal allowed a UK-based British-Israeli businessman to bring a data protection claim, together with claims of defamation and misuse of private data, against a US-based news website (Forensic News) and four-US based journalists relating to reporting on the claimant, who had been summoned to testify before Congress. Jurisdiction by the British court reportedly was based on three subscriptions in sterling and three subscriptions in euros to the Forensic News website. No claims were brought in California, where Forensic News in based, presumably because California has an anti-SLAPP law.

The statute of limitations for defamation is one year, while under the GDPR claimants have six years. As Arabella Pike, publishing director of HarperCollins, testified before the House of Commons Foreign Affairs Committee in March 2022, claimants are using GDPR "to essentially disguise what is a defamation claim" to get "around the [one-year] statute of limitations." GDPR claims are increasingly wrapped into threats of legal action under defamation law, and as Burgis testified, it allows claimants to go after source material on the ground that such material is confidential property of the claimants.

According to Bullough, close to 300 DSAR cases were brought in British courts in 2021, alone. This number was far greater than the number of defamation cases brought. While media organizations have an exemption under the GDPR, they must nonetheless respond to a DSAR before they can claim the exemption. These internal searches can take time and cost

money; large organizations can do these searches easily, while individuals and smaller organizations will have far more difficulty doing so.

Bullough cites the risk that these requests could potentially expose confidential sources of information, and extend to business intelligence firms or law firms conducting due diligence in the ordinary course of business. In her Commons testimony, Belton cites hearing of SDARs to force the release of information on sources triggered by internal investigations that concluded that bank accounts should not be opened due to corruption.

In March 2023, the newly created Department of Science, Innovation and Technology introduced the Data Protection and Digital Information (No. 2) Bill to streamline data protection in Britain. Among other provision, the proposed legislation (new Article 12A) would replace the current "manifestly unfounded or excessive" threshold for refusing DSARs with a lesser standard, "vexatious or excessive." The proposed legislation provides the following examples of requests that may be vexatious: requests that are intended to cause distress, are not made in good faith or are an abuse of process. As commentators have noted, this may not shift the types of requests that can be rejected; much will depend on guidance from, and application by, the newly established Information Commission (which would replace the current office of the Information Commissioner).

And just as SLAPPs are a Europe-wide issue, so too is the use of GDPR to attack press and other freedoms of expression. For example, in 2021, a Greek media outlet and one of its journalists were successfully sued under the GDPR by a mining executive for reporting that the mining executive and one of his colleagues (naming them) had been convicted for environmental degradation (which was accurate). The basis of the lawsuit was breach of privacy (*see* "Weaponizing GDPR: How EU data protection threatens press freedom in Greece").

Anti-SLAPPs Legislation

The European Union is focused on reining in SLAPPs via a directive that currently is the "trilogues" negotiation phase (*see* EU Parliament briefing). However, as Melinda Rucz notes, while the EU anti-SLAPP effort is a promising first step, it is not "optimally attuned to GDPR-based SLAPPs."

Britain has long had a reputation as the capital of libel tourism and a hub for illicit finance (the National Crime Agency, in a 2022 sanctions report, estimated that more than £100 billion of money laundering impacts the UK economy annually through abuse of UK financial institutions, UK company structures, markets and property. The UK Economic Crime and Transparency Act 2023, which received Royal Assent this week, contains anti-SLAPP provisions, but, as the UK Anti-SLAPP coalition noted in its press release, the provisions are limited to protecting only those who speak out on "economic crimes," which falls short of the universal protections that are so needed. Observers believe that progress was made on anti-SLAPP legislation in Britain largely as a result of the Russian invasion of Ukraine.

The UK Anti-SLAPP Coalition has published a Model anti-SLAPP law intended to guide policymakers in drawing up more robust protections. The British government has indicated it is considering future legislative options to introduce more comprehensive anti-SLAPP protections. The Solicitors Regulatory Authority, in November 2022, issued a "warning notice" on SLAPPs aimed at the legal community that it regulates.

Concluding Thoughts

As Melinda Rucz argued, as anti-SLAPP initiatives are rolled out, it is important that the abuse of the data protection regime be recognized as an emerging form of SLAPP, and addressed. It is equally important that there be greater attention paid in the context of national implementation of the GDPR to the protection of freedom of expression and to the role of national data protection authorities in facilitating SLAPPs.

My overall message is that lawmakers should recognize that well-intentioned legislative efforts can be exploited for malign purposes if they fail to consider the unintended consequences of their legislation. Lawmakers assume that any loopholes they unwittingly create will in fact be exploited to the detriment of democracy. Failing proactive focus on the front-end before protections are enacted, corrective action should be taken to close unintended loopholes.

* * *

Mark S. Bergman
7Pillars Global Insights, LLC
Washington, D.C.
October 28, 2023