Intermediary Liability Blog
The Evidence Hub for Policymakers

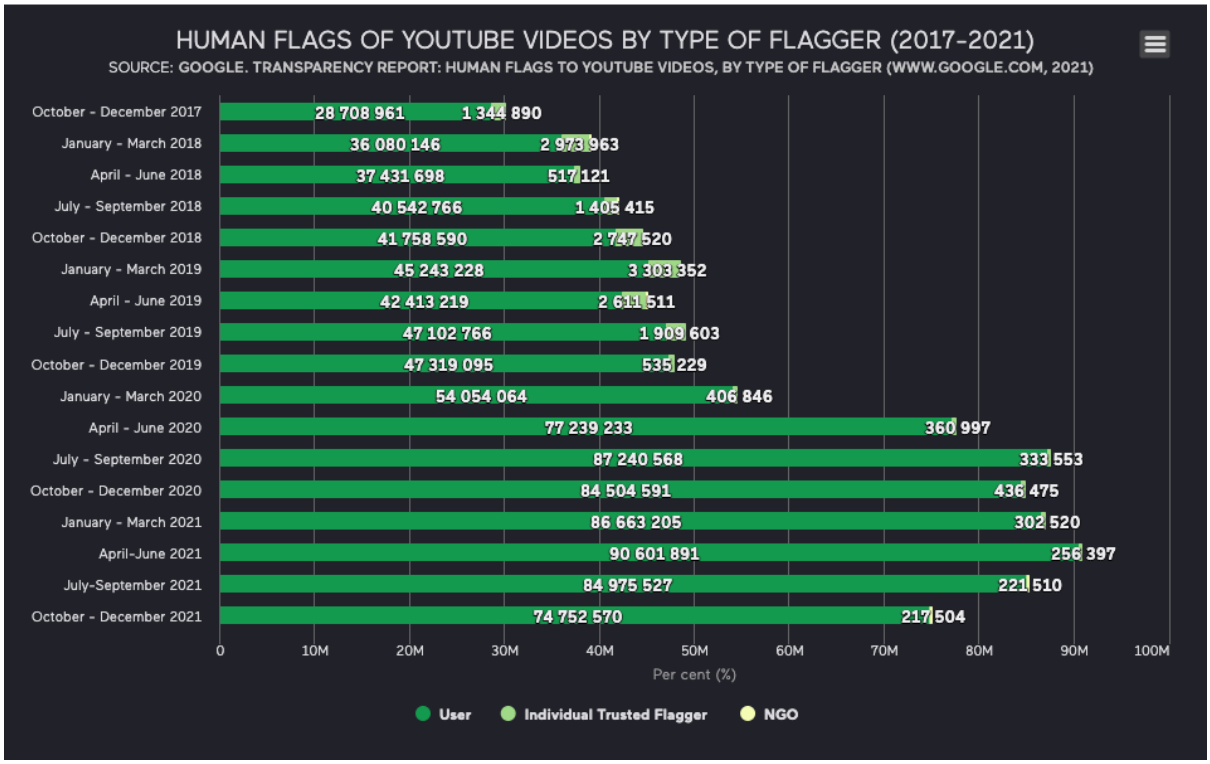
A Critique of Pure Friction: Does More Hassle Mean Additional Safety and Better Regulation?

07 March 2022 | Estimated reading time: 07 minutes

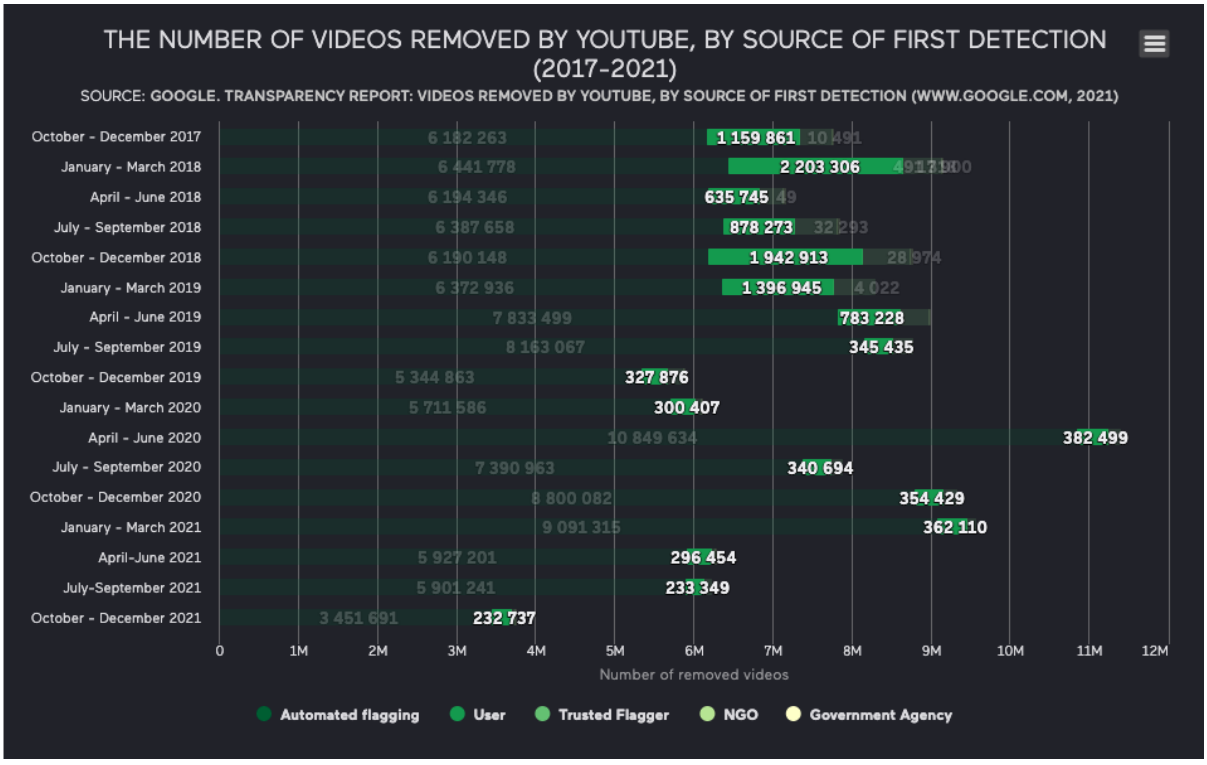
The recent spate of digital regulation initiatives in Europe have one thing in common: they introduce new procedures that create friction in the system, such as consent forms, *ex ante* impact and risk assessment, reporting, rights of appeal. Built-in hurdles like these can be found in a lot of existing European Union legislation, such as the general data protection regulation and the platform to business regulation. And the more recent European Commission proposals – the digital services act (DSA), the digital markets act (DMA) and the artificial intelligence act – would go a long way towards embedding the idea that the more fussiness we can bring to the Internet experience, the better the consumer will be protected and the greater the threats we will have successfully evaded.

But when it comes to friction, more is not necessarily better. Too little friction can make the car lose control, but too much friction will make it stop entirely. And detailed case-by-case or *ex ante* procedures have one other significant drawback: they are largely ineffective at dealing with the massive scale and unpredictable human behaviour that takes place on social media. They can even slow down and hamper efforts to keep consumers genuinely protected in the online sphere or to respond in real time to genuine threats that exist on the Internet.

The ongoing negotiations over the DSA and the DMA – the complex legislative packages that must be agreed by the Council of the European Union, the European Parliament and the European Commission to become law – have become a battle field where the EU's big legislative guns are trained on each other to see who can add more and more friction to the system. For instance, Council of the European Union negotiators propose to grant a "right-to-appeal" in the DSA to anyone who flags a posted item – which is essentially a message to the platform that the viewer thinks the post is inappropriate and should be removed – if the post was examined but found to be in conformity with community guidelines. In other words, a viewer can flag a post for whatever reason, and, if the service provider does not take down the content, the flagger has a right to challenge the decision. To understand the implications, bear in mind that YouTube received a staggering 74,752,570 flags in the last quarter of 2021 – meaning had the new rule been in effect millions of YouTube users would have received detailed explanations in Q4 of how their comment flag was processed along with a right to launch proceedings to have that flagging decision overturned.



But the majority of flags are little more than low-effort ways of expressing aversion and throwing a bit of mud towards something or someone a viewer dislikes. In fact, when looking at removal statistics, YouTube reports that only 232,737 videos were taken down in Q4 because of flags, i.e., one video for every 300 flagged. And the most flagged person in the world? Justin Bieber. You may or may not like his music or his style, but little of it poses a harm which could justify its removal from social media on community-guideline grounds (at least to this author's ears and eyes). Incidentally, Tim O'Reilly and others have written insightfully about this. Interactivity, in his view, is based on an "architecture of participation." Flagging posts or liking comments is good and fun and interesting. But is it really a form of commentary on a par with free speech?



The European Parliament has also been eager to tack on more friction, flexing its legislative muscle with a host of proposed add-ons to the existing proposal. Among the many European Parliament amendments:

1. Extend the requirements for notifying users when their posted content is "demoted" or made less visible in search results or sharing and not just when it is actually removed as is the practice now.
2. Require e-commerce platforms to gather and verify data from traders such as contact details, goods certification, trade registry certificates and payment details before allowing those companies to sell over the platform.
3. Extend the requirement for a full risk assessment by very large platforms from a yearly basis to every time a new service is released.
4. Require large platforms to ask for GDPR-like consent when they combine data from different services (such as iCloud and Apple Music which are already bundled on many people's Mac).

These proposals are exactly that: proposals. They will now be discussed and possibly corrected or dismissed. But they reveal an underlying way of thinking by policymakers that remains: the idea that increasing friction in the system will make users safer and the Internet more secure. The requirement to notify users every time content is demoted, for one, would lead to an explosion of notifications regarding a routine function of the Internet – one that is largely data-driven and built to deliver content relevance and meaningful user experiences to the 3.5 billion people who use the Internet. The e-commerce requirements, too, while well intentioned, are an ocean away from the very real problem of counterfeit goods, which takes place mostly in large, container-driven businesses; though the proposal would radically increase the amount of paperwork – and the number of compliance thresholds – on small businesses that use platforms to sell. And the proposal that platforms be required to publish full risk assessments before a new service is rolled out is the most dangerous of all. Today, in the era of agile, iterative development and permanent beta, services are released and updated almost on a daily basis, making the task impossible. And imagine if such a requirement had been in place when the WannaCry Ransomware attack was underway. Sometimes platforms need to act quickly. Sometimes we really want them to.

To be clear, adding friction can be a very good idea in some situations. There are, for example, lengthy, time-eating requirements in place before a person or couple can sign a mortgage or a new drug be widely distributed to the population. But when applied indiscriminately, friction can penalise (by accident or on purpose) the weakest part of society, such as minorities and small businesses. In at least one country, multiple identity checks and forms have been designed and used to disenfranchise voting rights of minorities. In other places, unclear and lengthy importing procedures are a well-known kind of non-tariff barrier which harms big and small businesses alike. The European Commission itself has raised a flag on this practice, noting in its action plan for better implementation and enforcement of single market rules that "SMEs are the first to be penalised by administrative burdens and complexity."

A good example of the unintended cons of adding too much friction to the system is the general data protection regulation (GDPR). I am not referring to the cumbersome user experience due to pop-up proliferation, which is a deliberate achievement because it raises the awareness of users about how personal data is treated. But when it comes to its economic impact, small businesses and new startups have been excessively penalised by the indirect effects of the regulation as much recent

scholarship has shown. Stricter privacy controls reduced competition in advertising markets and increased market concentration as cookie consent rates are smaller for small players. Younger and early-stage ventures are also more affected than established companies. And ad-blockers reduce product and brand discovery. This does not mean that GDPR failed, but it does mean that even a measure considered successful must deal carefully with direct and indirect effects and the consequences are often different from the expectations. In this context, continuously adding new friction is unlikely to work when it is applied too brusquely – or given tasks to perform that it is singularly ill-equipped to deliver. And it can even add to the information and other asymmetries that it is intended to correct. Jura Liaukonyte, professor of applied economics and management at Cornell University, put it succinctly in a recent twitter thread: "Evidence is rapidly accumulating, suggesting that stricter privacy controls exacerbate inequality between large and small businesses."

What's more, the European obsession with introducing friction as a form of regulation reflects a fundamental misalignment with the nature of digital services and, more generally, with today's complex society. *Ex ante* assessments can work in specific cases but they are not effective tools to resolve the complex, non-linear problems generated by human use of digital technologies at massive scale. As Daphne Keller, director of the platform regulation programme at Stanford Cyber Policy Centre, puts it, such measures "seem built on the hope that with enough rules and procedures in place, governance of messy, organic human behaviour can become systematised, calculable and predictable." The proliferation of *ex ante* measures is particularly ironic in this context because the distinguishing feature of digital services is their iterative nature driven by the fundamental fact that human behaviour is difficult to predict outside of a context that is agile and data-driven.

Let me be clear. I don't advocate a deregulatory, frictionless approach based on free speech and "innovation without permission." And even less do I endorse the idea that adding friction makes better regulation. In fact, we do not have to choose between the two. We have examples of different approaches in government, bridging the gap between cultures of *ex post* result-oriented decisions (typical of digital services) and *ex ante* process-oriented rulings (typical of traditional government).

Recent regulatory trends point to new approaches such as sandboxes and so-called "agile regulation," a toolkit for effectively regulating fast-moving digital markets through data analytics and iteration. And we find signs of these fast-emerging approaches in the DSA and other recent proposals. For one, the DSA's strict reporting requirements go in the direction of fostering a more responsive, data-driven regulatory system – one based more on actual than expected behaviour. But the data troves that these new reporting requirements produce will need to be strategically designed to avoid inconsistencies and to make the data easier to understand and act upon. As is, too much performance data – much of it generated through self-reporting and the code-of-conduct approach – is buried across widely dispersed European Commission initiatives or in single-company reports. To be genuinely useful, the metrics should be carefully designed, standardised across different policy instruments possibly at the global level, published in open data formats and made accessible through synthesis reports with interactive visualisation. If that could be achieved, the results could be more widely used and ultimately more effective in regulating a fast-moving phenomenon that is difficult to nail *ex ante* even under the best of circumstances.

In other words, *ex-ante* risk assessments, to the extent that they are used, should be targeted, limited in number, carefully designed and consistently followed up through

iterative monitoring. Regulators must ask, is the expected impact taking place? And if not, what are the reasons behind that? Otherwise, the rules will be at best little more than cumbersome regulatory requirements and at worst box-ticking exercises that give the illusion of control and allow responsibilities to be evaded.

Last but not least, when it comes to overseeing moderation at such a massive scale, an approach based on notification rights and a case-by-case appeal process seems less effective than a risk-based approach based on well designed and transparent sampling. There is a trade-off between quantity and quality of moderation, not just for the moderators, but also for those like policymakers who intend to regulate this moderation. Providing every user, commenter and flagger with the right to monitor and appeal will not lead to a fairer system and could be easily abused by those most able to play the game.

Regulating digital technologies is one of the profound challenges of this generation. It will have a deep impact on our democracies and way of life. We need to gather data, share knowledge and discuss openly to understand what works – and what doesn't. And we need to see how that knowledge can be used to generate new ideas and more effective approaches. But it is also important to quickly drop ideas that do not work. The overreliance on friction is one of them.

DAVID OSIMO
David Osimo is director of research at the Lisbon Council.

This blog post appeared on the Digital Services Evidence Hub, an interactive website managed by The Lisbon Council, a Brussels-based think tank, to gather available evidence and data points on the issue of intermediary liability. Its website is https://evidencehub.net/.