A TRULY DIGITAL SINGLE MARKET?

June 2015

INTRODUCTION

THE TIME IS RIGHT

It is undoubtedly a positive development that the Commission has launched the Digital Single Market Communication. For far too long, we have found ourselves in the ridiculous situation where "progress" has been translated into the inability to do things with new technologies which were previously unproblematic, such as selling or lending books. For far too long have European citizens and businesses been tripping over the chaos of the million-plus options given to Member States for the implementation of copyright exceptions and limitations. For far too long have citizens been faced with "not available in your country" when trying to access cultural content.

It is also undoubtedly positive that the new structure of the European Commission allows a level of coordination and accountability that was previously impossible. Take internet provider liability and voluntary law enforcement measures, for example. Previously, this was the independent responsibility of the Home Affairs, Internal Market, Communications Networks, Content and Technology, Trade and Consumer Directorates and Secretariat General of the European Commission. Now, Commission Vice-President Andrus Ansip leads the Digital Single Market project team, providing accountability and structure.

LACKING AMBITION

If a Commission is going to be bold and ambitious, it is at the start of its mandate. However, instead of boldness and ambition, the Digital Single Market Communication displays the damage of sustained lobbying campaigns that have already driven the Commission off track. Unfortunately, while the Commission is completely correct about the need to engender trust in the online space, the Communication's efforts to accommodate all of the demands of all lobby groups leads to policies which will unquestionably fail to achieve this trust.

The most serious example of this is the approach to intermediaries. Responding to pressure from telecoms operators, the Communication expresses worries that online intermediaries are too powerful.[1] This is not an invalid argument. However, in the very next section,[2] the Commission argues, responding to pressure from copyright holders,

1 Cf. Section 3.3.1. "Role of online platforms" of the DSM Communication
2 Section 3.3.2.

that online intermediaries should be given even more power, in order to undertake *ad hoc* policing activities. In the absence of any analytical information showing that this would be necessary or legal, the Commission's "evidence" document that accompanied the Communication descended into a chaotic analysis of this policy area, mixing unauthorised online content, illegal online content and legal but potentially harmful and treating this all as one issue. The dangers of this unsophisticated approach are very clear.

The same lobbying damage can be found in the proposals on personal data. While producing typically ambitious figures about the economic value of "big data", the Communication offers no particular ambition for strengthening the e-Privacy Directive, no words to describe the lack of progress of the proposed Directive on protection of personal data being processed for law enforcement purposes and no leadership on the ongoing destruction of the proposed General Data Protection Regulation.

Finally, it is worth noting the "once only" approach to e-government – which means that personal data will flow around government departments, potentially also across borders, reducing citizens' control over their personal data. Cost efficient solutions that also develop citizens trust can be nurtured, designed and implemented, but this will only happen when the challenges are recognised and privacy by design and default are priorities and not afterthoughts. The approach to this policy issue contradicts the Commission's established approach and needs serious rethinking.

COPYRIGHT

Having announced the copyright reform for autumn 2015, the Digital Single Market Communication and the Commission's Staff Working Document (the Commission's "Evidence" document) touch on a number of topics related to copyright which are under discussion in the European Parliament. The main points of concern raised in the DSM texts are:

ACTA II – PRIVATISED LAW ENFORCEMENT

The Commission considers in section 3.3 of the DSM Communication the use of the so-called 'voluntary measures' (cf. "*due diligence*" and "*duty of care*") to address "Intellectual Property Rights" (IPR) infringements (p. 12).

There are clear reasons to worry about the imposition of sanctions by intermediaries outside the rule of law and the extent to which it undermines the presumption of innocence, the right to due process of the law and, depending on the specific measures put in place, also the right to privacy and freedom of communication.[1] We welcome that, in the text, this reference to "self-regulatory" schemes includes concern that the measures must be taken with care and that the European Commission has taken on board the risks to fundamental rights when enforcing IP rights. However, there are no clues in the Communication as to what this recognition will mean in practice. The need for counterbalancing measures to protect fundamental rights, particularly in the light of the ruling of the European Court of Justice in the Telekabel case[2], is becoming ever more pronounced.

Another related term mentioned in the DSM documents that raises concerns is the reference to "*due diligence*" What due diligence might mean, especially in the online environment, is not self-explanatory and it is not described in the texts. The only thing that it logically cannot mean is the "diligence" referred to in the CJEU L'Oreal/eBay case[3], as this is already part of the European legal framework. The tenor of the Communication suggests that it is unlikely to mean less diligence, while it could hardly mean more effort on the part of the intermediaries, as this would push the balance beyond what was considered reasonable in the above-mentioned ruling.

Astonishingly, the Commission attempts to reinforce its case by mixing, in one paragraph, ISPs' responsibilities for unauthorised content, criminal content and

1 See https://edri.org/papers/human-rights-privatised-law-enforcement/

2 CJEU, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, C-314/12, 27 March 2014. See an analysis of the Telekabel case here (https://edri.org/austria-intransparent-web-blocking-scheme/) and here (https://edri.org/web-blocking-austria-law-with-the-law-taken-out/)

3 CJEU, L'Oréal and Others v eBay , C-324/09, 12 July 2011, C 324/09/. See an analysis of the L'Oreal/eBay case here: https://edri.org/edrigramnumber9-14ebay-loreal-case-ecj/

harmful content, making no effort whatsoever to analyse whether it is appropriate or even counterproductive to suggest dealing with criminal and legal content in the same way – outside a predictable legal or evidence-based framework.

In a document aimed at strengthening Europe's online competitiveness and harmonising the market, the Commission suggests weakening protection for European online companies via-a-vis their US counterparts and forcing them to introduce ad hoc, arbitrary policing schemes that will add new barriers.

"FOLLOW THE MONEY" AND "COMMERCIAL SCALE INFRINGEMENTS"

Two terms which are often been used in different documents related to copyright and IPR are also deployed in the DSM texts: the "*follow the money approach*" and "*commercial scale infringements*". Readers are not told which one(s) of the existent schemes has been put in place and where, and which results they have obtained. The USA already uses Google, Visa and others to impose US law globally – is that what the Commission understands as "follow the money"? Is it something else? What are the results of the US approach that are so positive that we can import that model or invent our own? We don't know and the Commission doesn't tell us.

Finally, regarding the concept of "*commercial scale infringements*", we need to remember that the Commission itself has indicated that it needs to be better defined, but yet appears to have no ambitions to produce this better definition. In September 2012, in its "roadmap" for a revision of the IPR Enforcement Directive, the Commission explained that it "would also require a clearer definition of "commercial scale", so as to make sure that professional counterfeiters rather than individual consumers are targeted".[4] Has something happened in the meantime that means that this analysis is no longer valid? We don't know, because the Commission hasn't told us.

TEXT AND DATA MINING

The documents include a positive reference to the need for a EU legal framework on text and data mining.

In section 3.5 of the "vidence" document, the Commission says that "text and data mining has also emerged as an area where legal uncertainty as regards EU copyright law and divergent approaches at national level could hamper European research, including cross-border research collaboration." (p. 30) If the European Commission moves

4 http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2011_markt_006_review_enforcement_directive_ipr_en.pdf

towards achieving "legal certainty" allowing the effective exercise of these techniques, the European Commission will take a big step forward in the digital agenda for Europe.

HARMONISING THE COPYRIGHT REGIME (BUT JUST A BIT)

Regarding the chaotic system of exceptions and limitations in EU copyright law, the Commission calls for the harmonisation of exceptions and limitations in the "evidence" document. However, despite the fact that existing exceptions and limitations could only have been included in the main piece of EU copyright law (the so-called InfoSoc Directive (2001/29/EC)) because of their compliance with the 3-step test, the harmonisation proposed by the Commission is addressed only to "certain exceptions". We fail to see why existing and uncontroverisal exceptions that "*do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder*" (in the terms described in the Article 5.5 of the InfoSoc Directive) should not all be mandatory and, sadly, the Commission does not tell us.

GEO-BLOCKING

Another topic which is under discussion is geo-blocking. As stated by the Commission itself, "Consumers expect to be able to access content anywhere and from everywhere".[5]

The European Commission says in the "evidence" document that "*addressing the problem of territorial restrictions in e-commerce could bring increased price transparency, more competition in cross-border e-commerce and greater availability and choice of products for consumers*" (p.24). The text also adds that 19% of citizens are interested in watching or listening to content from another EU country and that "*27% of citizens said they would be interested in watching or listening to audiovisual content or music transmitted from their home country when moving temporarily abroad, for example for holidays or for business*" (p. 26).

The Commission admits that the territoriality of the copyright regime is one of the basis for these restrictions. However, although the intention to tackle the problem of geo-blocking is positive, the approach misses the point of including non-commercial uses such as it occurs for example when YouTube shows the "*this video is not available in your country*" sign.

Along with the access to cultural content using freely accessible platforms (such as the YouTube example commented above), another element to which the DSM documents remain silent is about the framework regulating the access to the content originated from public broadcasters in different Member States.[6] The stated purpose of copyright is to defend cultural creativity, not to lock European culture away from European citizens.

5 Page 25 of the "evidence" document.

6 http://blogs.lse.ac.uk/mediapolicyproject/2015/05/06/the-ecs-digital-single-market-strategy-implications-for-territorial-licensing-of-audio-visual-rights-geo-blocking-and-public-broadcasting/

DATA PROTECTION, PRIVACY AND DATA FLOWS

The Digital Single Market documents raise a number of concerning points regarding data protection and privacy.

TO START WITH, THE TEXT HIGHLIGHTS THAT:

- Only 22% of Europeans have full trust in companies, such as search engines, social networking sites and e-mail services.
- 72% of Internet users in Europe still worry that they are being asked for too much personal data online.

The "evidence" document says that *"(a) clear and consistent approach should be pursued in all initiatives related to data stored and accessed over the Internet, be it for data protection purposes or for accessing evidence, thereby enabling effective criminal investigations and prosecutions."* (p. 51) The Commission, however, does not propose measures to finally bring an end to illegal data retention obligations that are imposed by a variety of EU Member States.

In the same vein, the Commission touches on another topic especially worrying in the field of the right to privacy: **Big Data**. The "evidence" document uses typically over-ambitious and unclear projections on its value, arguing that: *"(...) (I)f the top 100 European manufacturers could start from scratch by incorporating systematically the results of their big data analytics in their business processes, they would save EUR 160 billion"* (p. 62). However, especially given the current weak "progress" on the adoption of the new General Data Protection Regulation, the calls for any exploitation of data should be framed within a system of safeguards for an effective protection of privacy rights. The Commission's approach on this issue is out of tune with the rest of the DSM Communication, which stresses the need for trust in the development of the Digital Single Market.

The DSM Communication alsocalls for a **free flow of data** strategy: *"Member States are [not] able to inhibit the free movement of personal data on grounds of privacy and personal data protection, but may do so for other reasons. Any unnecessary restrictions regarding the location of data within the EU should both be removed and prevented"* (pp. 14-15). While proposing no steps to ensure that any national data self-defence measures should

be unnecessary, the Commission prefers to put all its faith in the adequacy of the future General Data Protection Regulation, and fails to mention its struggling proposal for a Directive on data protection in the law enforcement area. It is doing this, despite the fact that it the draft Regulation is being watered down past any degree of credibility in current negotiations in the EU Council.

One has to worry about the closeness of the Commission to certain lobbies, when the telecoms lobby website calls "on legislators to ensure a global level playing field for all actors processing personal data"[1] and the Commission's Communication then calls for a "*level playing field for all market players*" (p.13). Now that the online providers have almost succeeded in turning a fairly strong draft Regulation into something resembling a homeopathic remedy, it seems unlikely that the playing field will be levelled by raising standards for all, the risk is that the field will be levelled downwards — to the further detriment of privacy, security and freedom of communication.

1 https://www.etno.eu/home/working-groups/data-protection-trust-security

THE "ONCE-ONLY" PRINCIPLE FOR E-GOVERNMENT

Section 4.3 of the DSM Communication, dealing with "An inclusive e-society", promotes the "once-only" principle for public administration. It is claimed that the EU can save 5bn EUR per year implementing this principle.

"Once-only" is the principle according to which public authorities should never ask citizens and businesses for information that is already in the possession of another public authority in that country. Instead, they should reuse previously collected information. Some EU Member States implemented or are implementing this principle.

Page 74 of the Commission working document "DSM: Analysis and Evidence", contains some information on the issue. The Commission cites one of its own reports, from April 2014, which claims that the EU can save 5 billion EUR per year if the Danish approach to the "once-only" principle is implemented across Europe. The e-Government proposal seems to have been heavily inspired by Danish practices.

THE "ONCE-ONLY" PRINCIPLE FROM A DIGITAL RIGHTS PERSPECTIVE

According to the Commission, public sector data infrastructure must be able to facilitate the "once-only" principle, since this is intended to apply across different institutions (data controllers), and maybe even across different Member States. This idea can work only if databases of different public institutions are linked together, for example through a common citizen ID number that is used in every system. This is exactly how the Danish public sector is structured: a single citizen ID is used everywhere from tax management to health care.

This has a number of disadvantages from a privacy, data protection and IT-security ("cybersecurity") perspective:

1. Citizens are often not aware about what kind of data a specific public authority (data controller) processes about them since it could be that they did not provide the data to that institution. Moreover, requiring consent from the citizen in order for public authority A to fetch data from the database of public authority B will not always solve this problem, since consent statements are often too vague.
2. When public sector databases are linked with a common ID, it is much easier for the

government to circumvent purpose limitations and use personal data for different purposes (this is also "once-only", just without any citizen involvement). For example, in Denmark, the public interest exemption in the Data Protection Directive is frequently used to justify these practices. Among other things, this leads to more profiling of citizens, for example for welfare fraud.

3. When public sector databases are directly linkable with a common citizen ID, they are more attractive targets for IT-criminals ("cybercriminals"). Identity theft perpetrators want to build a profile of their victims in order to steal their identity. Indeed this becomes easier if various data pieces obtained from separate systems can be linked together. The value of system decentralisation is diminished if databases can be linked together and this increases the costs of data protection.
4. There is an inherent conflict between the "once-only" principle and new privacy and security by design requirements in the proposed General Data Protection Regulation.
5. Linkable databases would make it easier for the public sector to provide complete personal data profiles to third parties. Often this data is claimed to be anonymised, so that citizen consent is not needed, but the risk of re-identification is not adequately considered.

IN SUMMARY:

What the Commission proposes:

Section 4.3 of the DSM Strategy promotes the "once-only" principle for public administration, claiming it will make EU save a lot of money;

the "once-only" principle is the principle according to which the "public administrations reuse information about the citizen or companies that is already in their possession without asking again" (page 16, Official communication document)[1]

Applying the "once-only" across different institutions and possibly across Member States would mean linking databases of different public institutions. A centralized system, probably built around a common citizen ID number, would have different consequences:

- It will affect the consistency of citizens' consent statements;
- It would be easier for governments to use personal data for new and different purposes once they are collected;
- It would make databases more attractive for cybercrimes such as identity theft;
- It would affect citizens privacy and right to have some data anonymized by public administrations.

1 Leaked draft Communication define the "once-only" principle as "the principle according to which information is collected from citizens and business only once"

CONCLUSION

There are numerous positive aspects in the Communication. Its very existence is a recognition of the problems that need to be addressed and resolved. The Commission has identified a number of key issues that are central to the creation of a Digital Single Market. However, it is important for policy-makers to remember that the lack of progress over the past ten years is not an inexplicable anomaly – it comes from a lack of leadership and heavy pressure from vested interests that profit from inertia. If the Commission can realise this, resolve the concerns raised in this analysis and can show leadership and vision, the Digital Single Market can be a huge success. It is time to hoist the sails, re-set the rudder and set a course for a unified digital Europe.[1]

1 Published originally as part of the article http://www.friendsofeurope.org/smarter-europe/new-digital-single-market-strategy-lacks-ambition/

PROTECTING DIGITAL FREEDOM

European Digital Rights
Rue Belliard 20, 1040 Brussels
www.edri.org
@edri
tel. +32 (0) 2 274 25 70