Towards a European surveillance society? Combating copyright infringement through graduated response initiatives in France and the United Kingdom.
Meyer, Trisha; Van Audenhove, Leo

Published in:
EuroCPR: Policies for a digital Europe: lessons learned and challenges ahead

Publication date:
2010

Document Version:
Accepted author manuscript

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 07. May. 2020
Towards a European surveillance society? Combating copyright infringement through graduated response initiatives in France and the United Kingdom.

Trisha Meyer & Leo Van Audenhove

Abstract

This paper reflects on and frames graduated response in terms of theories on surveillance society & code. Graduated response is a warning & sanction mechanism aimed at fighting online piracy. Internet users caught infringing copyright are repeatedly warned about and ultimately sanctioned for their illegal actions. Graduated response is contested in Europe for reasons of proportionality, implementability and legal issues concerning Internet users and service providers. In this paper, however, we contend that many objections raised to graduated response have been reduced to issues concerning the procedure rather than the principle. We believe important societal questions concerning graduated response remain un(der)explored. Drawing from the literature on surveillance society & code, we offer three alternative critiques to graduated response and argue that graduated response portrays rights holders as being in a state of emergency, is a form of social sorting and has a technological bias. The paper consists of three parts. First, we discuss the literature on surveillance society & code, to then continue with an analysis of the EU debate concerning graduated response and an overview of the current initiatives in France and the United Kingdom (UK). Finally, we link our theoretical insights on surveillance society and code to graduated response.

1 Trisha Meyer is a doctoral researcher at the Institute for European Studies (IES) and is affiliated with the center for Studies on Media, Information and Telecommunication (IBBT-SMIT). Her Ph.D concerns copyright enforcement policies in EU member states. Leo Van Audenhove is a professor for International Communication at the Vrije Universiteit Brussel (VUB) and a senior researcher at IBBT-SMIT. The authors can be contacted at Trisha.Meyer@vub.ac.be and Leo.Van.Audenhove@vub.ac.be.
1. Introduction

The Internet has made control over the distribution and reproduction of creative content much more difficult. In 2008 an estimated 95% of music downloads were illicit.² This massive sharing and downloading of copyrighted content on the Internet is a significant worry to rights holders, who try to fight copyright infringement both through deterrents - law(suits), educational campaigns, technological protection measures, and incentives - legal offers. The newest deterrent is graduated response, a mechanism through which Internet users caught infringing copyright are repeatedly warned about and ultimately sanctioned for their illegal actions. Graduated response is contested in Europe for reasons of proportionality, implementability and legal issues concerning Internet users and service providers.

This paper reflects on and frames graduated response in terms of theories on surveillance society and code. First, we begin by delving into the literature on surveillance society & code. All information societies are surveillance societies, and all surveillance can be used for either care or control. Surveillance is a type of social sorting, as it prioritizes the rights and interests of one over another. Additionally, code is a significant new means of regulation on the Internet, but its potential for perfect enforcement, opaqueness and automatization is disconcerting. Then, our discussion on surveillance society and code is followed by an analysis of the EU debate concerning graduated response and an overview of the current initiatives in France and the United Kingdom (UK). France and the UK are the two EU member states who are the furthest advanced in developing warning and sanction mechanisms. Both initiatives promote graduated response as a means of deterring copyright infringement, but in comparing the two initiatives we notice that while France emphasizes the suspension of Internet access as a sanction, the UK seems to prefer technical measures, such as Internet filtering. Moreover, while the French proposal is mainly government-driven, the British opt for co-regulation. Finally, we conclude by linking our theoretical insights on surveillance society and code to graduated response. Graduated response entails surveillance and regulation of Internet activities through technology. We offer three alternative critiques to graduated response and argue that graduated response portrays rights holders as being in a state of emergency, is a form of social sorting and has a technological bias. Most importantly, graduated response has significant societal consequences which currently remain un(der)explored.

2. Surveillance society & code

In this first section, we reflect on the ideas of an information society as a surveillance society and technology (code) as a regulator. On the one hand, we situate surveillance within its sociological context and emphasize that surveillance is a manifestation of society's desire to manage and control. On the other hand, we highlight some issues of regulation through code.

2.1 Surveillance society

David Lyon, a leading scholar in surveillance studies, contends that "all societies that are dependent on communication and information technologies for administrative and control processes are surveillance societies"³. Surveillance is "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered"⁴. As such, surveillance is "a

---

⁴ IDEM, p. 2.
key feature of modern life, upon which we depend for the efficiency and convenience of many ordinary transactions and interactions\(^5\). Surveillance is necessary in an information society, and thus is certainly not inherently bad.

Surveillance has two faces, care and control, and thus can either enable or constrain. Indeed, the verbs “surveiller” in French or “to watch over” in English can be interpreted either positively or negatively.\(^6\) A practical and current example is the use of Internet filtering on YouTube, which allows the identification of copyrighted content on the popular video-sharing site. Upon notification of detection of copyrighted content, rights holders can decide to either allow further use (enable) or order the take down (constrain) of the video containing their content. Put differently, surveillance is a means of managing risks. Risk calculation and speculation, concepts commonly used in the field of financial markets and investment, have gradually spread to other areas, such as security but also culture. Didier Bigo argues that 9/11 has brought a normalization of emergence, a feeling of insecurity which allows governments to take extreme measures to monitor and control.\(^7\) The current discourse in security emphasizes threats and calls for increased control.

Surveillance also needs to be understood in its wider political economic context. Lyon believes our surveillance society has an "impetus to coordinate and control"\(^8\), a "cultural obsession with omniperception"\(^9\). Although most of the time people comply with the system, surveillance is about power and social sorting. It is used to manage, categorize and control persons and populations.\(^10\) Surveillance technology can either enable or constrain practices of certain groups. Consequently those deciding the data and the criteria for monitoring are in a powerful position. In contemporary society, surveillance is mainly kept in check by privacy and data protection legislation. Surveillance scholars argue, however, that privacy cannot provide adequate resistance to surveillance, because it fails to address the underlying issue of social justice.\(^11\) Surveillance intensifies power relations and places the interests and rights of one over another.

### 2.2. Code

Further, surveillance has shifted away from humans. Rather than human beings, the targets of surveillance are data and the agents of surveillance are technology (code). Maria Los believes it is important to understand which role surveillance technology plays in postmodern society. Quoting William Staples, she argues that surveillance and social control (which are "pervasive, rational and predictable") are used to compensate for the fragmentation and uncertainty present in postmodern society (due to the "radical questioning of the validity of common-sense, pre-given rationality criteria and the objective search for truth").\(^12\) Thus quite paradoxically, our relativistic society has led to "surveillant positivism" (a bias towards technology), as "human involvement introduces inherently risk interference because of its subjectivity and arbitrariness".\(^13\)

---


\(^6\) IDEM, p. 3.


\(^9\) IDEM, p. 124.

\(^10\) IDEM, p. 3.

\(^11\) IDEM, p. 130.


\(^13\) IDEM, p. 90.
Lawrence Lessig agrees that technology is a significant new means of regulation in the digital environment. Code is increasingly used to complement other regulatory instruments, which Lessig identifies in his model as law, market and social norms. He makes a distinction between West Coast Code, the Rule of Technology, and East Coast Code, the Rule of Law (which comprises of the traditional means of regulation). Lessig and others (such as Zittrain, Brownsword, McIntyre & Scott) express concern about West Coast Code, because it nears perfect enforcement, tends to be less transparent and can be automatized. Roger Brownsword phrases the apprehensiveness as follows, "[o]n the East Coast, legalism at least lets regulatees now where they stand. By contrast, on the West Coast, those who are controlled stand only where their regulated environment allows them."16

More than any other regulatory instrument, code can indirectly influence Internet behavior by enabling or constraining certain actions. Even though we have yet to see perfect enforcement, the danger lies in the potential. The insecurity felt after 9/11 allowed the adoption of extreme measures. Lessig believes a serious threat on the Internet (such as malware) could incite radical change. Just because so far the Internet has been relatively open and generative, does not mean it can't change. Considering technology is not neutral and "code codifies values", who frames the discourse and has control over the code really matters - especially when code entails a loss of transparency. Lessig explains that code can either be programmed as open or closed. Two characteristics of closed code are that "users cannot easily modify the control that the code comes packaged with" and that its functionality is opaque. If the criteria for surveillance and filtering are not known, there is little assurance that a balance between interests and rights will be held. Add automatization to perfect enforcement and opaqueness, and West Coast Code becomes particularly disconcerting. TJ McIntyre and Colin Scott object to automatized enforcement, because although it may reduce biased enforcement, a complete ruling out human discretion is undesirable. McIntyre & Scott argue that "software is a very efficient mechanism for implementing rules, but not so good when it comes to standards." An Internet filter can detect copyrighted content, but cannot distinguish between legal and illegal use. Additionally, automatization of regulation through code limits the possibility of feedback. Opposing certain technological measures can be more difficult than opposing its bureaucratic counterparts, as "bureaucratic enforcers can cater for harsh or unintended effects through the exercise of discretion". A last general, but nevertheless important objection to code as regulator, raised by Los, McIntyre & Scott, concerns the loss of responsibility for one's actions. Surveillance is meant to instill self-discipline. However, "[i]f [through code] actions outside the acceptable range are simply impossible, then we need no longer engage in moral choice, since our actions will, of necessity be acceptable." Thus a possible and dangerous side effect of technological solutions (such as graduated response and Internet filtering) is the erosion of users' sense of responsibility on the Internet, because what ever is possible will be acceptable.

---

15 IDEM, pp. 72-74.
19 IDEM, p. 78.
20 IDEM, p. 139.
21 IDEM, p. 151.
23 IDEM, p. 117.
24 IDEM, p. 123.
3. Graduated response: EU, France & UK

Having discussed surveillance society and code, in this second section, we dig deeper into the opinions of EU stakeholders towards graduated response and Internet filtering. We also look at the graduated response approach adopted in France and the UK to understand the mechanism better and highlight similarities and differences between the two initiatives. The aim is to offer a critical analysis of the European discussion and developments concerning graduated response.

In the French Memorandum of Understanding between government, rights holders and Internet service providers concerning “the development and protection of cultural works and programs on the new networks” (Accord Olivennes), graduated response is defined as “a warning and sanction mechanism aimed at deterring infringements of intellectual property rights on digital networks”25. Internet users caught infringing copyright are sent two warning letters and then risk receiving a sanction. The general procedure of graduated response involves identifying the infringement, identifying the infringer (based on an IP address), warning repeatedly about the infringement and ultimately sanctioning the infringer (most notably through the suspension of Internet access).

3.1 European Union

In January 2008, the European Commission published a communication and held a public consultation on the topic of "creative content online in the single market".26 The objective of the Commission was to address certain challenges identified as central to the uptake of online content services in Europe: digital rights management, multi-territory rights licensing, and legal offers and piracy. At IBBT-SMIT, we made a stakeholder and content analysis of all non-citizen contributions (239) to the consultation. In this paper we focus on the answers to the two last questions, which concerned graduated response and Internet filtering.27

Graduated response & Internet filtering

Question 10 - Do you consider the Memorandum of Understanding, recently adopted in France, as an example to followed?28

In the 2008 consultation, the opinions of stakeholders towards graduated response were quite split: 34% expressed a positive view, 29% expressed a negative view, and 33% expressed a nuanced view. Only 4% expressed an alternative view. Many answers found in the category "nuanced" stated that the French policy initiative was at too early of a stage to evaluate. The low number of respondents with an alternative view was most likely due to the framing of the question. The European Commission made a specific reference to the French initiative and placed the question within a discussion on copyright protection and enforcement.

There was a strong polarization between (but actually also within) stakeholder groups. Rights holders (except publishers) supported graduated response, while citizen & digital rights groups and Internet service providers (except when having a stake in the content industry) opposed the measure. On the one hand, the supporters of graduated response considered sanctioning necessary to deter online piracy. On the other hand, opponents believed sanctioning through the suspension of Internet access was disproportionate. They also foresaw practical and legal issues with Internet users and service providers. In our analysis, we were surprised at the level of support for graduated response, especially considering the reference to the French proposal. However, as the question was framed within a discourse on copyright, it did not easily allow wider interpretations on the issue.

**Question 11 - Do you consider that applying filtering measures would be an effective way to prevent online copyright infringements?**

Comparable to question 10 on graduated response, the opinions of stakeholders towards the Internet filtering were also quite split: 33% expressed a positive view, 34% expressed a negative view, and 27% expressed a nuanced view. Only 6% expressed an alternative view.

Quantitatively, question 11 on Internet filtering was similar to question 10 on graduated response. The profiles of supporters and opponents were also corresponding. On the one hand, rights holders argued that Internet filtering was an effective and beneficial way to prevent online copyright infringement. On the other hand, citizen & digital rights groups and Internet service providers contended that Internet filtering was an ineffective way that would cause legal issues with Internet users and service providers. Qualitatively, however, question 11 was different from question 10, as the positive answers were less pronounced, while the negative answers were quite strong. All stakeholders agreed that Internet filtering is not a panacea for online copyright infringement and several stakeholders also advocated applying filtering measures to monitor data for the development of new legal offers. Linking back to our previous theoretical discussion, the stakeholders were in fact acknowledging certain limitations of code as a regulator and promoting the application of surveillance and filtering technology to enable alternative uses.

**Further developments**

Since the “creative content online” consultation in 2008, there has been a clear shift in the Commission's focus towards extended collective and multi-territory rights licensing. Indeed, the final report on the content online platform, published in May 2009, stated that, on the matter of online copyright infringement, “no consensus on remedies” was found and it appeared “difficult at this point in time to strike the right balance between all interests involved”. Back in February 2009, EurActiv had already reported that the Commission had “shelved plans to curb online piracy”, because the topic was too controversial and the debate had been radicalized. Online piracy is still dealt with through the directives on copyright and IPR enforcement, in the newly created European observatory on counterfeiting and piracy, and also in the negotiations for an anti-counterfeiting trade agreement (ACTA) between a.o. the EU, US, Switzerland, and Japan. In fact graduated response may even be discussed within the context of the ACTA negotiations. Nevertheless, at the EU level, graduated response currently seems too contested for policy action. Meanwhile, two leading European economies, France and the United Kingdom, continue with their graduated response initiatives. As will be explained below, France and the UK argue that online piracy needs to be countered before new legal offers

---


30 EUROPEAN COMMISSION. Final report on the content online platform. May 2009, p. 4.

can be launched. We believe this raises important questions about the current EU approach towards online content and the role of the EU in copyright enforcement.

3.2 France

Having looked at EU stakeholders’ opinions towards graduated response and Internet filtering, we now turn to two initiatives in EU member states. France was the first member state to propose graduated response as a means of fighting online piracy. Despite contestation about the proportionality of a graduated response mechanism, the French government brokered a memorandum of understanding (Accord Olivennes32) and passed two laws (Hadopi I - Loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet33, Hadopi II - Loi du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet34) spelling out the warning and sanction mechanism. The implementation of the two laws is currently held up by the French data protection authority (CNIL - Commission Nationale de l'Informatique et des Libertés), who expressed concern about the processing of users’ data in the newly created administrative high authority (HADOPI - Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet).

Procedure35

The French graduated response mechanism leaves the identification of the infringement up to rights holders. Indeed, the high authority (HADOPI) acts on request of professional associations combating piracy, collective rights management societies, the national cinematographic center (CNC - Centre National de la Cinématographie) or the public prosecutor. The identification of the infringer is based on information from Internet accounts, which is compiled by HADOPI from Internet service providers. In France, the holder of an Internet account is responsible for activity on his account, meaning he will be considered the infringer. HADOPI sends two notifications to the account holder (first by email, then by registered letter), warning about the infringement, and informing about online legal offers, means of securing the Internet account, as well as the danger of online piracy for artistic creation. If the infringements persist after two warnings, a judicial authority can impose a sanction on the account holder through a simplified legal procedure. The sanctions provided by law are a fine, imprisonment or (since Hadopi II) suspension of Internet access (up to one year). An account holder who (willfully) neglects to secure his Internet account, risks the suspension of access (up to one month), and Internet service providers who do not suspend access upon notification, risk a fine. During the suspension period, an account holder is not allowed to open a new account.

Scope

The French government views graduated response as a mainly educational measure, because infringers are given repeated chances to alter their illicit behavior before being sanctioned. They also contend that a strong

legal framework enforcing copyright is necessary for the further development of legal offers. Therefore, the French initiative is twofold - a warning and sanction mechanism and commitments to promote the availability of legal content on the Internet, but with the fulfillment of the commitments hinging on the success of the warning and sanction mechanism. In this manner, the French discourse on graduated response evokes a sense of emergency and emphasizes strong intervention. Further, rights holders, software developers and Internet service providers have also committed to experiment with Internet filtering, thus in fact showing interest in regulation through not only surveillance, but also filtering technology. HADOPI will evaluate and report on these experiments.

As mentioned above, the French graduated response mechanism is contested. Both within and outside France the initiative has been opposed, mostly on grounds of disproportionality of the suspension measure. At the national level, the Constitutional Council overruled the first government bill, which allowed HADOPI to impose sanctions, stating the need for a judicial ruling. At the European level, the Council of Europe passed a resolution on "Internet governance and Internet resources", emphasizing that “fundamental rights and Council of Europe standards and values apply to online information and communication services as much as they do to the offline world". What’s more, the European Parliament showed disfavor towards graduated response on multiple occasions. Most notably, the Telecoms Reform Package, an effort to update the EU legal framework for regulating telecommunications services, was held up over an amendment stipulating the need for prior judicial ruling when suspending Internet accounts. In November 2009, the Telecoms Package was passed, with the compromised text reading: "[a] prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to an effective and timely judicial review shall be guaranteed."

3.3 United Kingdom

The United Kingdom was the second member state to propose graduated response as a means of fighting online piracy. In November 2009, a government bill was introduced in the British House of Lords (Digital Economy bill). This bill was preceded by a memorandum of understanding between government, rights holders and Internet service providers (memorandum of understanding on "an approach to reduce unlawful file-sharing") as well as multiple consultations and reports (such as the consultation on "legislative options to address illicit peer-to-peer (P2P) file-sharing" and the Digital Britain interim report), all reflecting on ways to deter online piracy. In June 2009, the Digital Britain final report was published, which gave the details of graduated response as proposed in the current government bill.

---


40 BRITISH DEPARTMENT FOR BUSINESS, ENTERPRISE AND REGULATORY REFORM. Consultation on legislative options to address illicit peer-to-peer (P2P) file-sharing. July 24th, 2008, 66 p.


Procedure

In the British proposal for a graduated response mechanism, the identification of the infringement is done by rights holders. Based on a copyright infringement report submitted by rights holders, Internet service providers proceed with the identification of the infringer (linking of the IP address with the account holder). The Digital Economy bill proposes to oblige Internet service providers to send a notification (warning) to the account holder's electronic or postal address, informing him about the infringement and copyright, and advising on legal offers and means of protecting the Internet account. Internet service providers can also be obliged to provide a "serious infringers list" to rights holders, which would not reveal the identity of the account holder, but disclose which copyright infringement reports relate to the account holder. This would enable rights holders to start proceedings against the account holder. Finally, the responsible Secretary of State (Department for Business, Innovation and Skills) can oblige Internet service providers to limit or suspend the Internet access of the account holder (sanction).

Scope

The Digital Britain initiative is an example of "Industrial Activism", where the British government stimulates key areas of growth that in turn can strengthen the UK's economic position in the future. In the Digital Britain report, the British government share that "commercially-led solutions remain by far the preferred approach", but that legislation could "provide an underpinning for these market models and to create an enforcement climate that will focus consumers on legal sources of content rather than unlawful ones". The proposal in the Digital Economy bill is co-regulatory, as rights holders and Internet service providers are permitted to draft their own code of practice stipulating the details of the warning procedure. Ofcom, the British regulator for communications industries, would be responsible for approving (or in absence of an agreement, drafting) such a code. Linking back to our theoretical discussion, the British government here effectively grants the private industry a position of power over users, as they are mandated to monitor and warn about illegal Internet actions.

Further, the Digital Economy bill allows the Secretary of State to direct Ofcom to assess and prepare a code concerning technical obligations for Internet service providers (sanction procedure, including Internet filtering). In the explanatory notes to the bill, it is emphasized that technical measures to limit Internet access would only be used against "serious repeat infringers". In August 2009, the Digital Britain report and related consultation were supplemented with a government statement, in which the suspension of Internet access was added to the list of technical measures, for the following reasons: "some stakeholders have argued strongly that none of those technical measures is powerful enough to have a significant deterrent effect on infringing behaviour. Also we cannot know how P2P technology might develop in the short to medium term, and we want to ensure that Ofcom has a full tool-kit from which to select the most appropriate measure should technical measures be deemed necessary."

We believe this quote is illustrative of the British government's bias towards technological regulation. They advocate the use of multiple technical measures to regulate Internet actions, unfortunately without taking the societal consequences of their use into account.

---

3.4 Comparison

When comparing graduated response in France and the UK, it is clear that the French initiative is in a further stage of development than the British. Two laws have been passed in France, while a government bill has only recently been introduced in the UK. However, currently neither graduated response mechanism has been implemented.

Procedure

The French and British proposals to deter online copyright infringement both contain a warning and sanction procedure. A main difference between the proposals lies in the role of the administrative authority HADOPI in France compared to the obligations imposed on Internet service providers in the UK. While the French government emphasizes suspension of Internet access as a sanction after having received two warnings, the British government proposes technical measures to limit or suspend Internet access for “serious repeat infringers”. In the course of events, it has been particularly remarkable to observe how the French proposal for sanctions has been weakened, while the British proposal has been strengthened. France's original proposal, which allowed HADOPI to implement sanctions, received much criticism and was eventually shot down by its own Constitutional Court. The UK's current proposal suggests giving Ofcom (not a judge!) the power to impose technical measures if the warning procedure fails.

Scope

The French proposal is more government-driven, which is reflected in the setup of HADOPI. The UK prefers co-regulation, encouraging rights holders and Internet service providers to draft their own code concerning the warning procedure. The British government bill also calls for a person "sufficiently independent" of rights holders, Internet service providers and Ofcom to resolve copyright infringement disputes and account holder appeals. Further, both France and the UK stress the need for a strong legal framework for the further development of online legal offers. In the Hadopi I law and the Digital Britain report, commitments are made to promote legal content on the Internet. The fulfillment of these commitments, however, are dependent on the success of the warning and sanction mechanism. It is notable that the Digital Britain initiative seems more in line with the European approach. The proposal is part of a wider discussion on reforming the content industry. Similarly, the European Union is currently focusing on multi-territory rights licensing and legal offers. Interestingly, although the British policy initiative has a more outward focus, thus far the French initiative (due to the suspension aspect) has attracted more international attention.

4. Conclusion

From the discussion above, it should be clear that graduated response is a contested means of deterring online copyright infringement. In the 2008 EU consultation concerning creative content online, proponents of graduated response asserted that new sanctions, preferably limiting or suspending Internet access, were needed in the fight against online piracy. Opponents contended that suspending Internet access was a disproportionate reaction to the problem of online piracy. We argue that many objections raised to graduated response have been reduced to issues concerning the procedure rather than the principle. The hesitation of both the French Constitutional Council and the European Parliament towards the graduated response dealt with the way of sanctioning, and the current concern of the French data protection authority (CNIL) focuses on the processing of data in the new administrative authority HADOPI. We believe important societal questions concerning graduated response remain un(der)explored. Drawing from the literature on surveillance society & code, we would like to offer three alternative critiques to graduated response.
First, graduated response fits within a particular discourse on threats to copyright. Rights holders seek to manage risks on the Internet by emphasizing the dire consequences of online piracy and advocating deterrents to this illegal use (controlling and restraining) rather than incentives to legal use (caring and enabling). The current discourse on online piracy portrays rights holders as residing in a state of emergency, requiring exceptional measures such as graduated response, and steadily avoids discussions on alternative forms of renumeration that could disturb the status quo of (big) rights holders. Indeed graduated response in France and the UK focuses on creating an enforcement climate rather than developing legal online offers. Similarly, during the EU creative content online consultation in 2008, the questions on graduated response and Internet filtering were framed within a discourse on copyright and prevention of copyright infringement. Interestingly, since the 2008 consultation, the EU has shifted its approach to extended collective and multi-territory rights licensing. Graduated response with its focus on deterrents is in conflict with this approach emphasizing incentives.

Second, graduated response is a form of social sorting, prioritizing the rights and interests of one over another. It allows widespread surveillance and regulation of Internet activities for the protection of copyright and consequently those deciding the data and the criteria for monitoring are in a powerful position. Graduated response is a co-regulation of government and private industry (especially in the British proposal). Within the limits of privacy and data protection legislation, whom, what and how is surveilled is left up to their discretion. However, surveillance scholars argue that privacy cannot provide adequate resistance to surveillance, because it fails to address the underlying issue of social justice. As the graduated response mechanism leaves the identification of infringements up to rights holders, the dividing line between those with and without the capacity to track down the Internet for infringing content is reinforced. This could result in the enforcement of copyright of only big rights holders. Moreover, the dividing line between those with and without Internet skills is equally reinforced, as the technologically competent users could more easily circumvent control. Graduated response effectively favors the interests of big rights holders over small rights holders and Internet users, and deepens the digital divide.

Third, graduated response has a bias towards code (technology), but regulation through code has certain characteristics (perfect enforcement, automatization and opaqueness) that (especially when combined) endanger society and the Internet. In the 2008 EU consultation, stakeholders expressed certain concerns about technical issues and side effects of graduated response and Internet filtering. Indeed in graduated response, perfect enforcement is circumventable with surveillance technology, but more difficult with filtering technology, as this tends to be automatized. Additionally, graduated response uses closed code, meaning the functionalities of the surveillance and filtering technology are opaque and cannot easily be modified. Technological regulation makes resistance and feedback more difficult. This close monitoring and control of actions on the Internet, which graduated response requires, has important side effects. It can lead to a loss of responsibility in society, as illegal content is technologically kept out of reach, and a loss of generativity on the Internet, as basic Internet principles, such as openness, transparency and limited control, are forgone.

Graduated response is much more than a means of deterring copyright infringement, and consequently requires a wider discussion on its political economy and societal consequences. Graduated response is about surveilling and controlling persons and populations. It manages, categorizes and either enables or constrains practices of certain groups. We would argue that graduated response is one of the first cases in which government is mandating surveillance of Internet actions, possibly followed by legal sanctions, by private industry. The widespread, systematic and private nature of the monitoring is disconcerting. Further, graduated response is also about regulating the Internet. Especially when combined with Internet filtering, graduated response is an example of regulation of the Internet through technology, (almost completely) sidestepping human deliberation. Therefore graduated response is a symbolic case. Decisions taken here could have an important impact on the direction of the future regulation of society and the Internet.
Bibliography


EUROPEAN COMMISSION. Final report on the content online platform. May 2009, 6 p.


