JOURNAL OF DIGITAL SOCIAL RESEARCH

YOUNG, SCRAPPY, AND HUNGRY
VOL 3, NO 1, 2021

JOURNAL OF DIGITAL SOCIAL RESEARCH

VOL. 3 : NO. 1 : 2021

JOURNAL METADATA

ISSN
2003–1998

DOI
http://doi.org/10.33621/jdsr

WEB
www.jdsr.io

ABOUT JDSR

JDSR is a interdisciplinary, online, open-access journal, focusing on the interaction between digital technologies and society. JDSR is published by DIGSUM, the Centre for Digital Social Research at Umeå University, Sweden.

CONTACT US

E-MAIL
editor@jdsr.se

JOURNAL OF DIGITAL SOCIAL RESEARCH

VOL. 3 : NO. 1 : 2021

JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 1, 2021, 1–38

DARK AND BRIGHT PATTERNS IN COOKIE CONSENT REQUESTS

Paul Graßl[1], Hanna Schraffenberger[1], Frederik Zuiderveen Borgesius[1, 2] and Moniek Buijzen[3, 4]

ABSTRACT

Dark patterns are (evil) design nudges that steer people's behaviour through persuasive interface design. Increasingly found in cookie consent requests, they possibly undermine principles of EU privacy law. In two preregistered online experiments we investigated the effects of three common design nudges (default, aesthetic manipulation, obstruction) on users' consent decisions and their perception of control over their personal data in these situations. In the first experiment (N = 228) we explored the effects of design nudges towards the privacy-unfriendly option (dark patterns). The experiment revealed that most participants agreed to all consent requests regardless of dark design nudges. Unexpectedly, despite generally low levels of perceived control, obstructing the privacy-friendly option led to more rather than less perceived control. In the second experiment (N = 255) we reversed the direction of the design nudges towards the privacy-friendly option, which we title "bright patterns". This time the obstruction and default nudges swayed people effectively towards the privacy-friendly option, while the result regarding perceived control stayed the same compared to Experiment 1. Overall, our findings suggest that many current implementations of cookie consent requests do not enable meaningful choices by internet users, and are thus not in line with the intention of the EU policymakers. We also explore how policymakers could address the problem.

Keywords: dark patterns; privacy; design nudges; cookie consent requests; GDPR; ePrivacy Regulation

1 iHub, Radboud University, Nijmegen, The Netherlands
2 Institute for Computing and Information Sciences (iCIS), Radboud University, Nijmegen, The Netherlands
3 Behavioural Science Institute, Radboud University, Nijmegen, The Netherlands
4 Erasmus School of Social and Behavioural Sciences, Erasmus University Rotterdam, Rotterdam, The Netherlands

1 INTRODUCTION

Whenever people are browsing the web they face privacy decisions in the form of cookie consent requests. The goal of cookie consent requests (under the EU's ePrivacy Directive) is a) to inform users about the goal of the cookies, and b) ask users for their consent. To give online users control over their personal data, the ePrivacy Directive only allows the use of tracking cookies (and similar tracking technologies) after the user has given his or her prior consent.

To ensure that users understand the decision they make with a consent request, consent (for tracking cookies) in the ePrivacy Directive must be interpreted in line with the strict criteria for valid consent in the General Data Protection Regulation (GDPR 2016); we refer to the two legal acts together as "EU privacy law". These criteria include that valid "consent" of the internet user (data subject) requires a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement" (GDPR, 2016, article 4(1)). In that, EU law appears to assume that people make deliberate and well-informed privacy choices. This assumption corresponds to a prominent model of privacy decision making, the privacy calculus theory, which presumes people's behaviour to be fundamentally rational and privacy decisions to be made through conscious weighing of the costs and benefits of each choice option (Laufer & Wolfe, 1977). But do people in practice perceive control over their personal data and show deliberative rational decision behaviour in the context of cookie consent requests?

This is questionable in light of a new trend of using "dark patterns" in cookie consent requests, which aim to influence users' privacy decisions (e.g., through pre-ticked boxes or highlighted options; Forbrukerrådet, 2018). Dark patterns are (evil) design nudges, which steer users against their best interest towards a certain choice through persuasive interface design (Brignull, n.d.; Gray, Kou, Battles, Hoggatt, & Toombs, 2018). Originally, nudging means influencing the decisions of individuals or groups towards good choices (as judged by themselves) through minor changes in the choice environment without compromising freedom of choice (a prominent example is a fly painted on a urinal in a public men's toilet to prevent urine spillage; Thaler & Sunstein, 2009).

The use of dark patterns can be problematic for legal as well as ethical reasons. While the GDPR (2016) does not explicitly ban all dark patterns, they do breach the spirit of the GDPR. Ethically, dark patterns (and nudges in general) may lead users to make choices that are not in their interest and deprive users of their control (Forbrukerrådet, 2018; Schubert, 2015). In fact, if a nudge is used for evil, Thaler (2018) refuses to call it "nudge", but rather "sludge". His colleague Sunstein (2016b) states two conditions to assess whether a manipulation is ethically objectionable: (1) when the goals of the manipulator are self-interested and (2) when the manipulation subverts the chooser's deliberative capacities. Dark patterns meet the first condition because they are used in the interest of the manipulator to collect

personal data. The second criterion, as we will argue in the next paragraphs, is met as well because dark patterns push users to make quick heuristic decisions rather than slow and deliberate ones.

EU privacy law and the privacy calculus theory assume that people make privacy decisions with what Kahneman (2011) calls System 2, that is the slow and consciously reasoning part of us. However, considering evidence from a multi-disciplinary literature assessment from Acquisti et al. (2017), it cannot be assumed that people behave purely rational in privacy decision situations. Rather, people apply heuristics - mental shortcuts in decision-making - and fall back to cognitive or behavioural biases, which work on the quick, heuristic System 1 (Sunstein, 2016a).

Cookie consent requests feature several characteristics that make people prone to applying heuristics. First, there is an information asymmetry between the user confronted with the consent request and the company asking for it. The user has access to less information regarding the purpose of data collection and possible future usage of it than the data controller. Second, consent requests often use ambiguous language (e.g., the data may be used for a certain cause) creating a decision under uncertainty for the user because not all possible outcomes are known. Acquisti et al. (2017) argue that these circumstances facilitate the application of heuristics, given that human rationality is limited to the available cognitive resources and the available time (based on the concept of bounded rationality; Simon, 1957). Third, people's privacy decisions are influenced by several cognitive biases, such as the status-quo-bias (individuals' preference for default choices) or the salience-bias (individuals' tendency to focus on prominent features). These three circumstances of cookie consent requests likely facilitate the mechanism of dark patterns, which targets mainly the intuitive, heuristic System 1 (Bösch, Erb, Kargl, Kopp, & Pfattheicher, 2016).

While there are many examples of the use of dark patterns in practice (see Brignull, n.d.; Fansher, Chivukula, & Gray, 2018; Forbrukerrådet, 2018), the field of privacy and data protection lacks research in this regard. The few studies that focused on the effects of dark patterns were conducted either with a non-representative sample (e.g., only students or young university-educated people; Machuletz & Böhme, 2019; Nouwens, Liccardi, Veale, Karger, & Kagal, 2020) or in a context that cannot be generalised easily (e.g., participants were told to have been automatically signed up for a costly identity-theft protection service; Luguri & Strahilevitz, 2019). Solely Utz, Degeling, Fahl, Schaub, and Holz (2019) demonstrated adequately that the use of dark patterns possibly influences a user's consent decisions, however, giving no clear answer on how to deal with the underlying problem of an overwhelming number of consent requests which may lead to indifference towards them over time.

Therefore, it is crucial to gain a better understanding of the effects of design nudges in cookie consent requests and to assess whether a) the understanding of privacy decision making in EU privacy law represents reality, and b) whether users

perceive control over their personal data through consent requests. We investigated these aims in two online experiments: Experiment 1 focused on the effects of dark patterns on people's consent decisions and their perception of control over their personal data. In a follow-up experiment (Experiment 2), we reversed the direction of the design nudges (i.e., towards the privacy-friendly option) to see how this affects people's consent behaviour and their perceived control compared to the first experiment (we titled such privacy-friendly design nudges "bright patterns"). Following, we will briefly introduce and outline the two experiments. After that, we focus in more detail first on Experiment 1 and then on Experiment 2. We end with a general discussion.

1.1 Experiment 1: Dark patterns in cookie consent requests

In our first experiment, the research questions were: given a cookie consent request with two choice options (privacy-friendly vs. privacy-unfriendly), do dark patterns lead users to choose the privacy-unfriendly option more often than the privacy-friendly option, even if the privacy-friendly option is rationally superior? And do dark patterns deprive users of their perceived control over their personal data? Specifically, we focused on the effects of three of the most common dark patterns, that is (1) default, (2) aesthetic manipulation and (3) obstruction (Fansher et al., 2018).

Default refers to any situation where one option is preselected prior to any action of the user, for example when the option to agree to a privacy policy is selected by default (Gray et al., 2018). Aesthetic manipulation refers to the act of giving "one option visual or interactive precedence over others", for example when one out of two choice buttons is coloured blue while the other one is simply grey (also called "false hierarchy"; Gray et al., 2018, p. 7). Obstruction means making an interaction more effortful than it needs to be to dissuade the user from a certain action or choice, for example when the option to opt out of online tracking is not presented together with the opt-in option but can only be reached by clicking through several submenus.

Following this design nudge (towards choosing the privacy-unfriendly option) can be considered a non-rational choice if the privacy-friendly option has more benefits (i.e., is rationally superior) than the privacy-unfriendly option (Archer, 2013). In Experiment 1, we presented the privacy-unfriendly option (i.e., allowing web tracking) in such a way that choosing this option could lead to losing control over one's personal data without providing any benefit (such as more relevant advertising). Hence privacy calculus theory would predict that people choose the privacy-friendly option (Smith, Dinev, & Xu, 2011). Deviations from this prediction indicate that people engage in privacy decisions (in the context of cookie consent requests) with the automatic, heuristic System 1, rather than with the rational, deliberate System 2.

We formulated the following hypotheses. In a cookie consent request situation with two choice options (privacy-friendly vs. privacy-unfriendly), where the privacy-friendly option is rationally superior,

Hypotheses 1a/b/c: participants will be more likely to choose the privacy-unfriendly option (compared to privacy-friendly) when the privacy-unfriendly option is (H1a) preselected, (H1b) visually more salient or (H1c) the alternative (privacy-friendly) option is obstructed.

Hypotheses 2a/b/c: participants report lower levels of perceived control over their personal data when the privacy-unfriendly option is (H2a) preselected, (H2b) visually more salient or (H2c) the alternative (privacy-friendly) option is obstructed.

Because little is known about the effects of dark patterns in cookie consent requests, the first study focused on their main effects rather than possible (and more speculative) interaction or moderation effects, in order to create a solid basis for further investigation. Nevertheless, we repeatedly highlighted that deliberating about a decision indicates System 2 behaviour. Little conscious deliberation, on the other hand, is associated with heuristic System 1 decision making (Albar & Jetter, 2009), which dark patterns seem to target. Therefore, we explored the possible moderating role of deliberation in the decision process. We hypothesised that more deliberation would reduce the effects of the dark patterns on the consent decisions and on the level of control that people perceive.

1.2 Experiment 2: Bright patterns in cookie consent requests

In the follow-up experiment, we reversed the direction of the design nudges (i.e., towards the privacy-friendly option) to see how this affects people's consent decisions and their perception of control over their personal data. We formulated the follow-up research questions based on the results from Experiment 1, where most people agreed to all consent requests in a default manner. The two research questions were thus: given a cookie consent request situation with two options (privacy-friendly vs. privacy-unfriendly), do bright patterns lead users to choose the privacy-friendly option more often than the privacy-unfriendly option (despite the previously observed default behaviour towards the privacy-unfriendly option)? And do bright patterns deprive users of their perceived control over their personal data in a similar way as dark patterns (given that any form of System 1 nudge compromises one's perception of control to some extent; Schubert, 2015; Sunstein, 2016a)?

We hypothesised that in a cookie consent request situation with two choice options (privacy-friendly vs. privacy-unfriendly),

Hypotheses 3a/b/c: participants will be more likely to choose the privacy-friendly option (compared to privacy-unfriendly) when the privacy-friendly option is (H3a) preselected, (H3b) visually more salient or (H3c) the alternative (privacy-unfriendly) option is obstructed.

Hypotheses 4a/b/c: participants report lower levels of perceived control over their personal data when the privacy-friendly option is (H4a) preselected, (H4b) visually more salient or (H4c) the alternative (privacy-unfriendly) option is obstructed.

In addition to the design nudges, other factors may influence whether a person acts in a rather fast and heuristic or more deliberate manner on privacy decisions. Based on evidence from previous research (Awad & Krishnan, 2006; Lai & Hui, 2006; Malhotra, Kim, & Agarwal, 2004) we controlled for general privacy concerns in both experiments. Additionally, we investigated in Experiment 2 whether controlling for privacy fatigue, as proposed by Choi, Park, and Jung (2018), instead of privacy concerns leads to different results.

2 EXPERIMENT 1

2.1 Method

Before running Experiment 1, we preregistered our sample size estimation, hypotheses and statistical analysis. The preregistration, the code of the study application, all used materials, data, and analysis scripts are available on the Open Science Framework (https://osf.io/c7qza/). Information about the used R version and all packages can be found in Appendix A.

2.1.1 Procedure and Design

The online experiment followed a within-subjects design where participants were asked to review eight news websites (shown in random order) and report on their first impression of the visual design of each news website. We used this cover story to create a realistic setting for the presentation of cookie consent requests and disguise the true purpose of the study. Each news website displayed an overlaying cookie consent request when being visited (while the rest of the website was dimmed at first), offering two choice possibilities: allow the website and other third parties to collect data and to track user's web behaviour (privacy-unfriendly), versus not allowing such data collection and web tracking (privacy-friendly).

After the participant made a choice, the overlaying consent request disappeared and the news website was shown (no matter which option the participant had selected), but only for three seconds to fit the cover story about first impressions. Regardless of the participants' choice, we did not track their behaviour nor collected more data than that necessary for the experiment (i.e., we only

recorded the consent decision). Each news website visit was followed by three questions about the participant's first impression of the design of the news website (for the sake of the cover story). After reviewing all news websites (which corresponds to part 1 of the experiment), we presented the eight consent requests again (one by one in the form of screenshots), and asked participants how much control they felt each consent request gave them over their personal data and how much they had deliberated on their decision. Additionally, for each consent request (presented as a screenshot), we asked manipulation check questions about whether participants had read the consent information and could recall the option they had chosen. Lastly, we assessed each participant's general privacy concerns and asked control questions about individual browser setup and device type. At the end of the study, we debriefed participants about the cover story and the true purpose of the experiment.

2.1.2 Web application and Materials

2.1.2.1 Web application

To run our online experiment, we set up a web application using the Python framework Flask (Lord, Mönnich, Ronacher, & Unterwaditzer, 2010). The application was hosted on a university server. We conducted a preliminary pilot study to test the credibility of our cover story. Four bachelor students were asked to do the study while thinking aloud, showing that the cover story worked as intended. We used eight different news website templates, which are licensed under the Creative Commons Attribution 3.0 (Colorbib, 2019). The news websites were called Avision, Megazine, Motivemag, Quitelight, Techmag, Technews, Viral and Webmag. We adjusted the templates partly in functionality (e.g., hyperlinks were disabled), content (e.g., exchange placeholder text such as "lorem ipsum" with plausible news content) and design to fit the purpose of our study. To achieve additionally required functionality for the online experiment, such as building multi-step consent requests (i.e., obstruction manipulation) or detecting when participants clicked on the back button, we used code solutions from An (2019) and Brooke (2011), respectively, which are available under the MIT license. Two examples of the used websites can be found in Appendix B, while the rest can be found on the Open Science Framework.

2.1.2.2 Consent requests

For each news website, we created a cookie consent request, which appeared as an overlay when a participant was directed to the news website. The general layout and text of the consent requests were inspired by a corpus consisting of consent requests of several popular news websites and big tech companies (corpus available on the Open Science Framework). The aim was to create cookie consent requests that resemble many of such consent requests used in practice. Whereas we kept the main

characteristics (e.g., the content of the provided text) of the consent requests constant across all conditions, we changed minor design details (e.g., font type, order of the sentences in the text, colour of the consent box edges etc.) of each consent request, to make them look slightly different from each other and to support the cover story about eight independent, external news websites. To have an indication of non-rational behaviour, the consent requests provided no information about any benefit of choosing the privacy-unfriendly option "Agree" (e.g., better-targeted advertising), which only left the cost of potentially losing control over ones' personal data when agreeing to the policy (i.e., allowing web tracking). Hence, choosing the privacy-unfriendly option "Agree" can be considered a non-rational choice (an example consent request text can be found in Appendix C).

Whereas the general layout of the consent requests was consistent, each request contained one out of eight possible combinations of the three dark patterns (1) default, (2) aesthetic manipulation and (3) obstruction. The statistical model we used (mixed-effects model) required the inclusion of all possible combinations of the independent variables (i.e., the dark patterns) to accurately estimate the effect of each predictor. Default was represented by a preselected "Agree" radio button on the websites Quitelight, Techmag, Technews and Webmag (Figure 1 shows one example consent request; screenshots of all consent requests can be found on the Open Science Framework). Aesthetic manipulation was represented by a blue coloured "Agree" button on the websites Megazine, Techmag, Viral and Webmag. Obstruction was represented by the option "Manage options" instead of "Do Not Agree" on the websites Motivemag, Technews, Viral and Webmag. Participants could only choose "Do Not Agree" after selecting "Manage options". The consent request of the website Avision represented the baseline condition with none of the three design nudges included (see figure in Appendix B1).

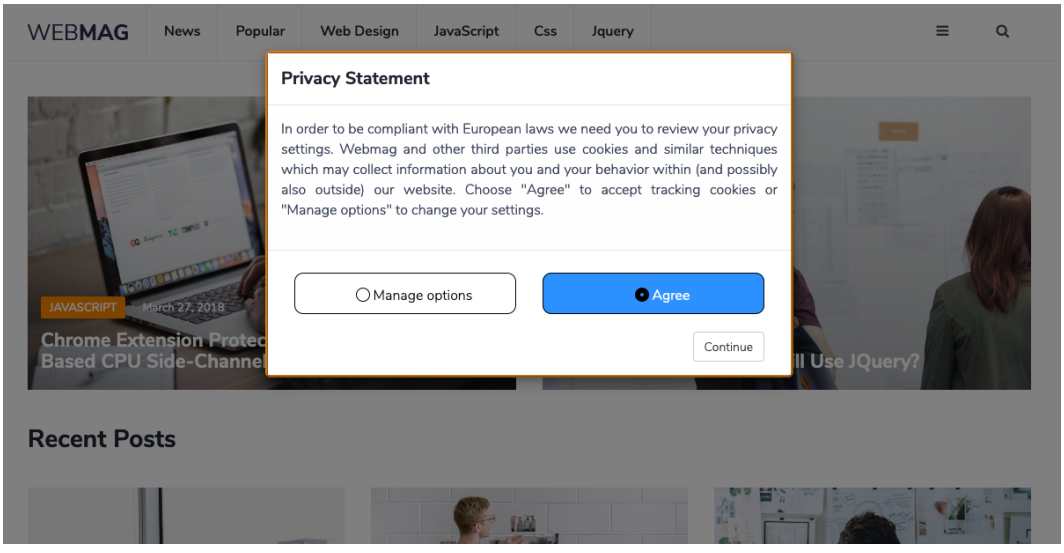

Figure 1. Example consent request featuring all three dark patterns default, aesthetic manipulation and obstruction. Website: Webmag

2.1.2.3 Measures

For each consent request, we recorded a participant's consent decision and assessed his or her level of perceived control, level of deliberation and several control questions regarding his or her attentiveness during the decision process. Further, we asked participants to report on their general privacy concerns and personal browser setup.

To measure how much control participants felt each consent request gave them over their personal data we built on the Perceived Control scale from Xu (2007). We adjusted the formulation of the items to fit the purpose of the study (see Table 1). Participants could indicate their perceived level of control over their personal data on a slider ranging from *Not at all* to *Complete* (higher values indicate more perceived control). We used the average of all five items as the final outcome variable perceived control in the statistical analysis (range: 0 - 100, M = 31.80, SD = 28.54). Further, the perceived control measure showed very good internal consistency with a raw Cronbach's α = 0.99 (none of the individual items increased the overall α if being dropped).

We assessed how much participants deliberated about their decision by asking "How much did you think about your decision before clicking on one option?" (formulation of the item was adapted for the present study; Dijksterhuis, Bos, Nordgren, & van Baaren, 2006). Participants could indicate the level of deliberation on a slider ranging from *Not at all* to *A great deal* (range: 0 - 100, M = 20.99, SD = 25.33). Lastly, we used the Global Information Privacy Concern scale from Malhotra et al. (2004) to assess general privacy concerns (on a seven-point scale ranging from *Strongly disagree* to *Strongly agree*, range: 1 - 7, M = 4.13, SD = 1.24). For the statistical analysis, we used the average score of the three items, which formed the scale. The measure General Privacy Concerns showed good internal consistency with a raw Cronbach's α = 0.79 (again none of the individual items increased the overall α if being dropped).

We included several manipulation checks and control questions to get a better understanding of the participants' behaviour during the study. When reviewing each consent request (in the form of a screenshot), we asked whether the participant had read the consent information (in 10.1% of the cases "Read it completely", 49.6% "Skimmed it", 40.3% "Did not read it at all") before clicking on an option and whether they remembered which option ("Agree", "Do Not Agree") they had chosen (2.6% of all consent decisions could not be remembered correctly). Further, we asked whether participants had installed a browser plugin, which handles or deletes cookies (31.1% "Yes", 68.9% "No").

Table 1. Perceived control questionnaire items

Number	Question
1	How much control did you feel the consent form gave you over the amount of your personal information collected by the company?
2	How much control did you feel the consent form gave you over who can get access to your personal information?
3	How much control did you feel the consent form gave you over your personal information that has been released?
4	How much control did you feel the consent form gave you over how your personal information is being used by the company?
5	Overall, how much did the consent form made you feel in control over your personal information provided to the company?

Note. M = 31.80, SD = 28.54, range: 0 - 100, Cronbach's α = 0.99 (raw)

2.1.3 Participants

We recruited a total of N = 228 participants for Experiment 1 via the crowdsourcing platform Prolific Academic. This sample size was initially determined for a frequentist regression analysis as preregistered for Experiment 1 (detailed information about the power estimation can be found via the Open Science Framework link provided above).

Inclusion criteria for study participation were an age between 18 and 65 years (to represent a broad range of society) and a current living location in the United Kingdom (to minimise noise in the data because of cultural differences we restricted the study to the biggest participant pool within Prolific Academic). Participants were compensated with 1.70GBP for the successful completion of the study, which was estimated to take around 12 minutes (8.50GBP/h). On average it took participants 9.79 minutes (SD = 4.02) to complete the study. We left 33 participants out of this calculation because they showed very long completion times, indicating that they divided the study over several days. Yet, their consent behaviour did not seem to differ from the rest of the sample and thus they were kept for analysis. Additionally, we found that only 5 participants had completed the experiment in less than 5 minutes (but not under 3 minutes). Because of that low number, we kept them in the sample. We excluded participants who could not finish the study due to technical problems.

The total sample population consisted of 137 females (60.1%), 91 males (39.9%) and had a mean age of 36.02 years (SD = 11.62). Of all 228 participants who took part in the experiment, 35 dropped out in the second part of the study (i.e., after reviewing the eight news websites). Because none of the dropouts

happened during the completion of a questionnaire (only in between) and no prevalent pattern of missingness was detected (e.g., the consent behaviour did not differ between participants with complete cases and those who would drop out later on), we found all participants' data eligible for analysis.

2.1.4 Data Analyses

As mentioned earlier, we initially conducted a frequentist regression analysis for Experiment 1. However, we decided later to use a Bayesian framework for Experiment 2 for two reasons: Firstly, Bayesian model results fit better with how people think about and interpret parameter estimates compared to frequentist models (Morey, Hoekstra, Rouder, Lee, & Wagenmakers, 2016). Secondly, Bayesian regression models turn out often to be superior to frequentist models when it comes to multilevel structured data (Browne & Draper, 2006; Bryan & Jenkins, 2016). Therefore, we reran the analysis of Experiment 1 for consistency purposes using Bayesian modelling (the pattern of results did not differ between the frequentist and the Bayesian approach). All reported statistics refer to the Bayesian models.

Instead of classic significance testing, we used 95% credible intervals (CrI) to decide whether a given parameter has a substantial impact on the outcome. Credible intervals indicate a range within which the parameter of interest lies with a probability of X% (we used 95%), given the data. If the credible interval of a parameter does not include zero (zero would mean no effect) we assume a substantial effect of the corresponding variable on the outcome. Credible intervals are different from frequentist confidence intervals, however, the latter gets often incorrectly interpreted as the former (Morey et al., 2016). The analysis was conducted using Stan (Carpenter et al., 2017) called via the package brms (Bürkner, 2017) within the R environment (R Core Team, 2020).

For each of the two dependent variables (consent decision and level of perceived control), we fit separate models with a maximal random-effects structure, following the advice of Barr, Levy, Scheepers, and Tily (2013). Thus, each main model included a per-participant random adjustment to the fixed intercept and a per-participant random adjustment to the slope of each within-subject variable (default, aesthetic manipulation and obstruction). Further, main models included general privacy concerns as a control variable.

To fit exploratory models, we added deliberation as a moderator to the aforementioned design of the main models. Specifically, deliberation was present as a fixed effect and part of an interaction with each of the three main predictor variables. Additionally, exploratory models added a per-participant random adjustment to the slope of the main effect of deliberation and each interaction term with it.

We used the $Bernoulli$ distribution as the model family for all models with consent decision as the dependent variable. The estimated models had thus the form of:

$$\begin{aligned} y_i &\sim Bernoulli(p_i) \\ logit(p_i) &= \alpha_{j[i]} + \beta_{j[i]} x_i \\ \alpha_{j[i]} &\sim Normal(\alpha, \sigma_\alpha) \\ \beta_{j[i]} &\sim Normal(\beta, \sigma_\beta) \\ \alpha &\sim Normal(0, 10) \\ \beta &\sim Normal(0, 5) \\ \sigma_\alpha &\sim Cauchy(0, 2.5) \\ \sigma_\beta &\sim Cauchy(0, 2.5) \end{aligned}$$

In this mixed-effects model, i refers to each element of y (i.e., the observed consent decisions), and j denotes the grouping factor, the participant. For models with perceived control as the dependent variable, we chose the $Beta$ distribution as the model family to mirror the continuous but interval restricted nature (0,1) of the outcome best (following Ferrari & Cribari-Neto, 2004). We estimated the models in the following manner:

$$\begin{aligned} y_i &\sim Beta(\mu_i, \phi) \\ logit(\mu_i) &= \alpha_{j[i]} + \beta_{j[i]} x_i \\ \alpha_{j[i]} &\sim Normal(\alpha, \sigma_\alpha) \\ \beta_{j[i]} &\sim Normal(\beta, \sigma_\beta) \\ \alpha &\sim Normal(0, 10) \\ \beta &\sim Normal(0, 5) \\ \sigma_\alpha &\sim Cauchy(0, 2.5) \\ \sigma_\beta &\sim Cauchy(0, 2.5) \\ \phi &\sim Gamma(0.01, 0.01) \end{aligned}$$

Due to a lack of previous literature to build on in terms of expected effect sizes, we applied only weakly informative priors on parameter estimates in all models.

2.2 Results

2.2.1 Main Analyses

To investigate our first set of hypotheses 1a/b/c (stating that dark patterns will sway people towards the "Agree" option) we first visualise the recorded consent decisions for each news website (see Figure 2). We observed that in the majority of cases (93.8%) people chose to agree to the consent requests. Moreover, most people chose

always the same consent option for each news website, suggesting that nudging did not seem to matter for their decision (only 4.0% of all participants changed their consent behaviour between conditions).

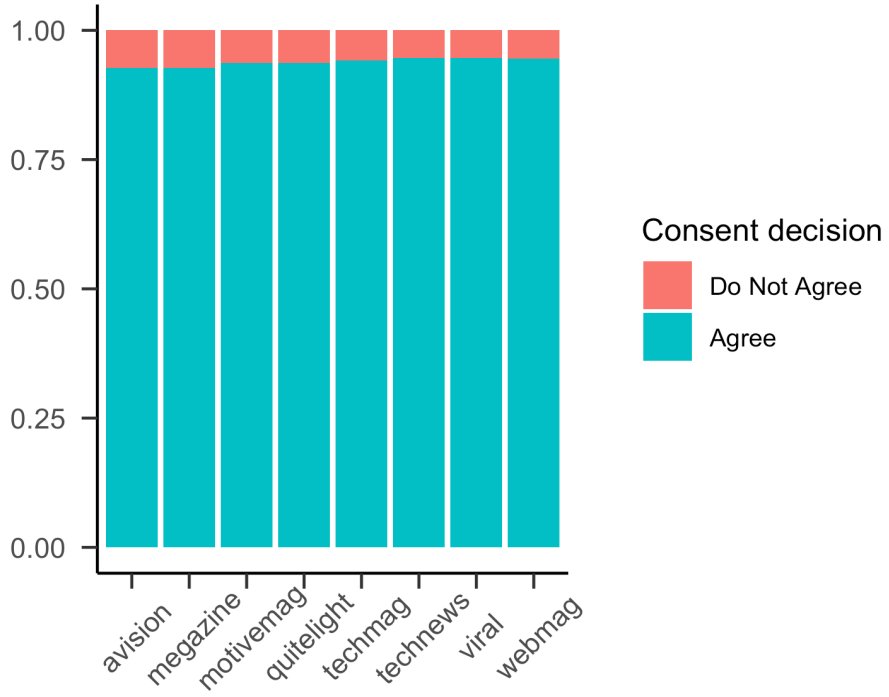

Figure 3. Consent decisions (proportional) by condition (different news websites)

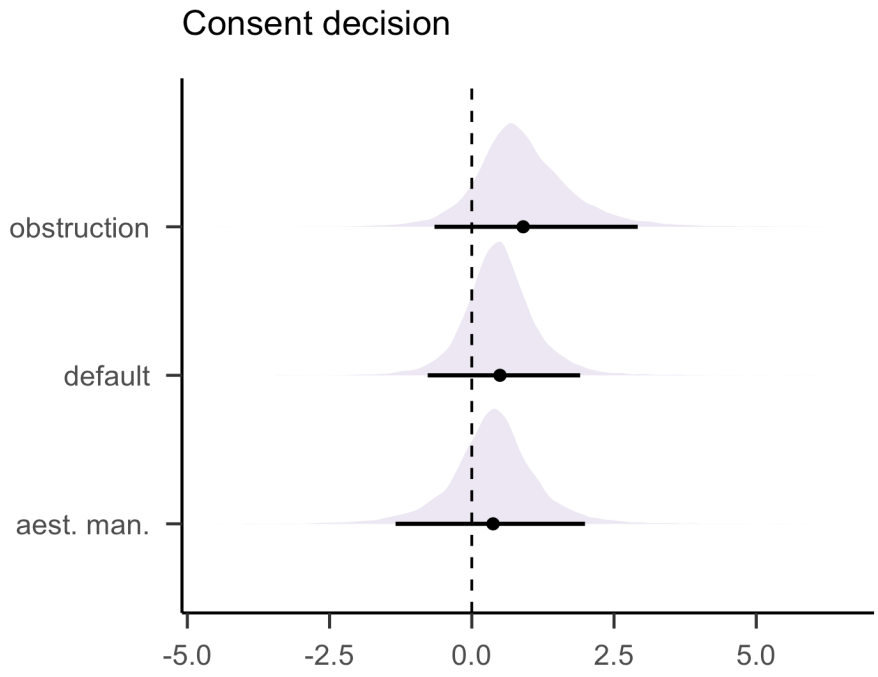

Figure 2. Posterior distributions with mean and 95% credible interval for the predictors obstruction, default and aesthetic manipulation (outcome consent decision)

Our results confirm this suggestion as we did not find support for our hypotheses H1a, H1b and H1c, meaning that there was no substantial effect of default, β = 0.50 (0.66), CrI 95% [-0.78, 1.90], OR = 1.64, aesthetic manipulation, β = 0.37 (0.80), CrI 95% [-1.34, 1.99], OR = 1.45, or obstruction, β = 0.90 (0.87), CrI 95% [-0.66, 2.92], OR = 2.47, on the outcome consent decision (see Figure 3). The pattern of results did not change when additionally accounting for the previous consent decision of a participant (although this was a good predictor of each consent decision given that most people did not vary their consent behaviour between conditions) or whether a participant had a browser plugin installed that handles or deletes cookies.Regarding our second set of hypotheses 2a/b/c, we did not find that the dark patterns made people perceive less control over their personal data. To our surprise, however, we found the design nudge obstruction to have the opposite effect: people reported more rather than less perceived control over their personal data when the "Do Not Agree" option was obstructed by "Manage options".

More specifically, obstruction showed a small positive effect, β = 0.11 (0.03), CrI 95% [0.05, 0.17], OR = 1.11 (see Figure 4). Hence H2c was not supported. Further, we did not find support for hypotheses H2a and H2b concerning the effects of default, β = 0.01 (0.01), CrI 95% [-0.02, 0.04], OR = 1.01, and aesthetic manipulation, β = 0.01 (0.02), CrI 95% [-0.03, 0.05], OR = 1.01.

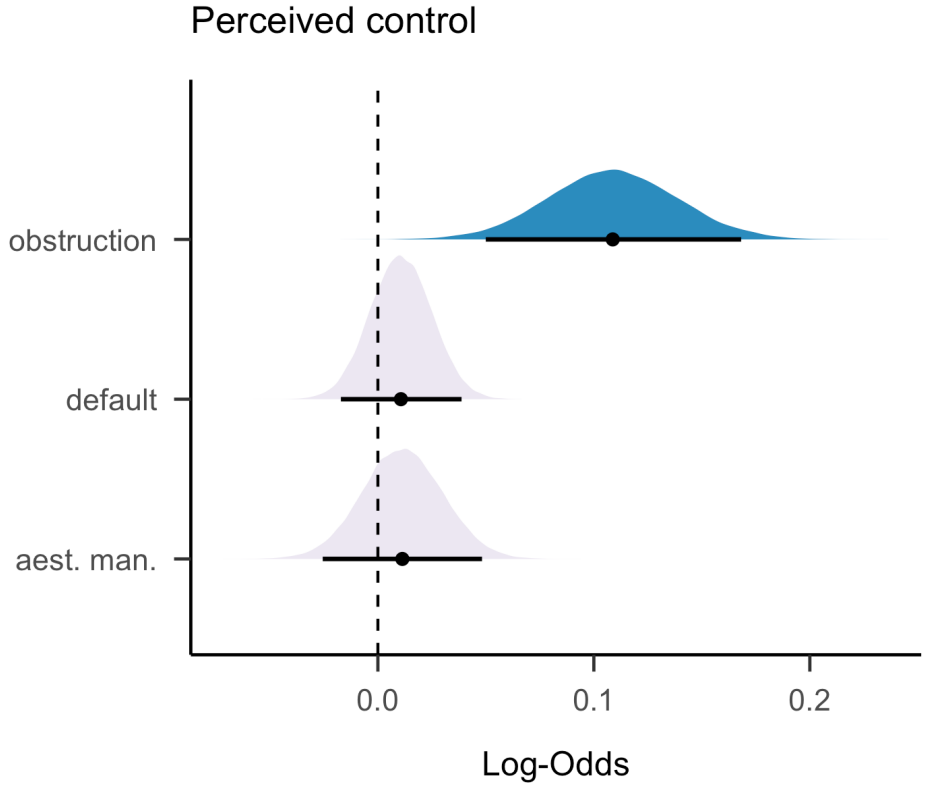

Figure 4. Posterior distributions with mean and 95% credible interval for the predictors obstruction, default and aesthetic manipulation (outcome perceived control)

The analysis of perceived control levels had to deal with a floor effect, meaning that a high number of observations gathered at the lower boundary of our measurement scale. This was probably partially due to how this variable was measured (i.e., slider's default position being *Not at all*), which may have led people to report generally low levels of perceived control (M = 31.80, SD = 28.54, Figure 5). Furthermore, we checked again whether accounting for a browser plugin installation that handles or deletes cookies changed the pattern of results, however, this was not the case.

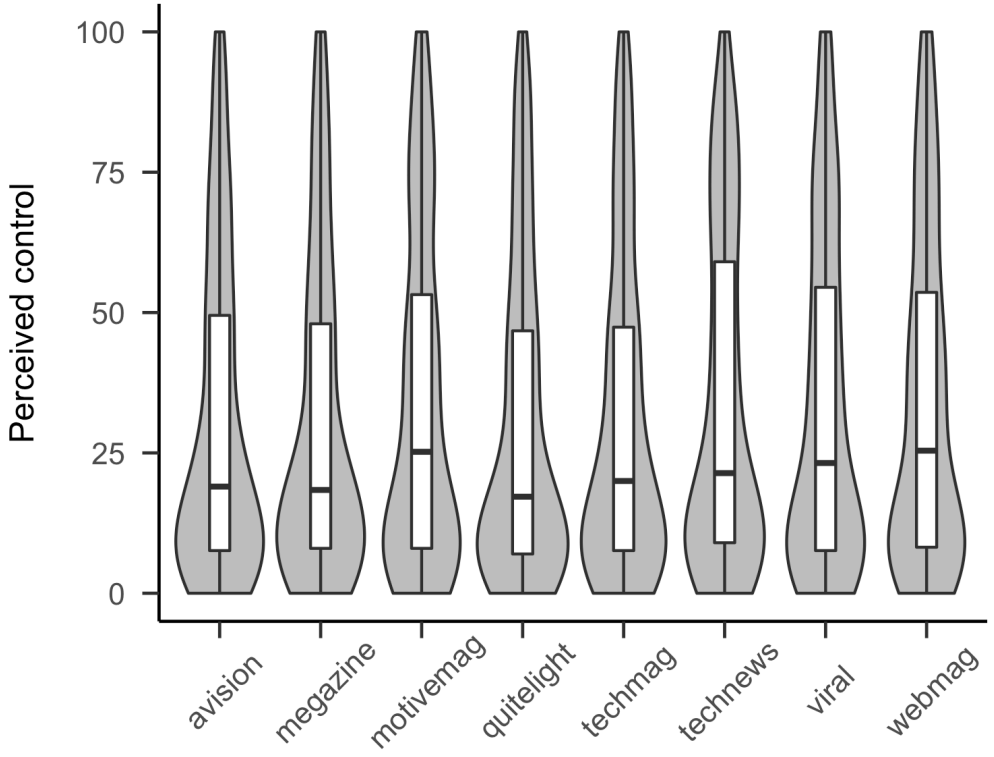

Figure 5. Violin plots showing levels of perceived control by condition (different news websites). Grey shapes visualise the distribution of the variable, white bars represent box plots

2.2.2 Exploratory Analyses

We ran two additional mixed-effects models to investigate whether the effects of the three dark patterns (default, aesthetic manipulation and obstruction) on participants' consent decisions and their perception of control depend on how much participants deliberated about their choice.

Our findings suggest that the extent to which participants deliberated about their choices did not substantially influence the effects of the three dark patterns on participants' consent decisions: default, β = 0.19 (0.74), CrI 95% [-1.29, 1.69], OR = 1.21, aesthetic manipulation, β = -0.31 (0.94), CrI 95% [-2.13, 1.59], OR = 0.74, and obstruction, β = 0.79 (1.05), CrI 95% [-1.23, 3.02], OR = 2.20. Neither did the extent to which participants deliberated about their choices substantially

influence the effects of the three dark patterns on participants' perceived control: default, β = -0.02 (0.02), CrI 95% [-0.06, 0.02], OR = 0.98, aesthetic manipulation, β = -0.01 (0.02), CrI 95% [-0.04, 0.03], OR = 0.99, and obstruction, β = -0.01 (0.03), CrI 95% [-0.06, 0.04], OR = 0.99. This finding may be due to the fact that participants reported generally low levels of deliberation (M = 20.99, SD = 25.33). Similar to the perceived control measurement, absolute values of deliberation should be interpreted cautiously due to the assessment procedure (i.e., slider's default position being *Not at all*).

2.3 Discussion

The goal of Experiment 1 was to investigate whether dark patterns in cookie consent requests lead users to choose the privacy-unfriendly option more often than the privacy-friendly one and whether such dark patterns make people perceive less control over their personal data. Although we could show that the majority of participants always chose the privacy-unfriendly option and reported a lack of control over their personal data, we did not find clear support for those effects being due to the dark patterns. Unexpectedly, we found that obstruction led people to perceive more rather than less control over their personal data. Given the generally low levels of perceived control, which we observed across all conditions (as shown in Figure 5), more evidence is needed before making interpretations about this association.

Apart from specific effect structures, the data provided substantial ground for further insights into how people perceive consent requests and how they act on them. Most participants reported that they did not read the consent requests properly and did not think much about their decision before choosing one option. Still, the majority of participants agreed to all consent requests, seemingly in a default manner. This consent behaviour suggests that legal consent requirements for tracking cookies do not work as intended by law. At least, this conclusion applies to the way how cookie consent requests are often presented in practice. People do not seem to engage with privacy decisions in a rational and deliberate manner, as assumed by the privacy-calculus theory and, partly, by EU privacy law (GDPR, 2016, recital 7).

One reason for this observed default behaviour may be that people are conditioned to agree to consent request from their everyday life. Many websites do not even provide the opportunity to choose between different options, but make access to the site conditional on accepting tracking cookies with so-called "tracking walls" (called "forced action" by Gray et al., 2018; Zuiderveen Borgesius et al., 2017a). Hence, people often have to consent to access the content of a website or other service. It might be that the conditioned behaviour from reviewing consent requests on a daily basis overwrote the effects of the dark patterns in Experiment 1. This would be in line with the finding that people did not think much about their

decision, but possibly followed the heuristic approach of choosing the option they normally choose.

To see how the design nudges relate to the observed (and possibly conditioned) default behaviour and to further investigate the unexpected effect of obstruction increasing perceived control, we conducted Experiment 2. In this follow-up experiment, we reversed the direction of the design nudges (i.e., towards the privacy-friendly option). By applying the design nudges in this "unconventional" way we aimed to see whether this would change the behaviour observed in Experiment 1. Further discussion of Experiment 1 will follow in the general discussion after Experiment 2.

3 EXPERIMENT 2

3.1 Method

As for the first experiment, we preregistered our sample size estimation, hypotheses and statistical analysis before running Experiment 2. The preregistration, the code of the study application, all used materials, data, and analysis scripts are again available on the Open Science Framework (https://osf.io/bfdvy/). Information about the used R version and all packages can be found in Appendix A. Following, we will only describe the differences between the original Experiment 1 and the follow-up Experiment 2 to avoid repetition.

3.1.1 Procedure and Design

Whereas the general procedure and design stayed the same in the follow-up experiment, we asked participants additionally about their privacy fatigue. This questionnaire was added to the second part of the study, just before we assessed general privacy concerns.

3.1.2 Web application and Materials

3.1.2.1 Consent requests

To reverse the direction of the design nudges, the focus was now on the "Do Not Agree" (to tracking) option instead of the "Agree" option. Hence, default was represented by a preselected "Do Not Agree" radio button on the websites Quitelight, Techmag, Technews and Webmag (Figure 6 shows one example consent request; screenshots of all consent requests can be found on the Open Science Framework). Aesthetic manipulation was represented by a blue coloured "Do Not Agree" button on the websites Megazine, Techmag, Viral and Webmag. Obstruction was represented by the option "Manage options" instead of "Agree" on the websites Motivemag, Technews, Viral and Webmag. Participants could only choose "Agree" after selecting "Manage options". The consent request of the

website Avision represented, as in Experiment 1, the baseline condition with none of the three design nudges included.

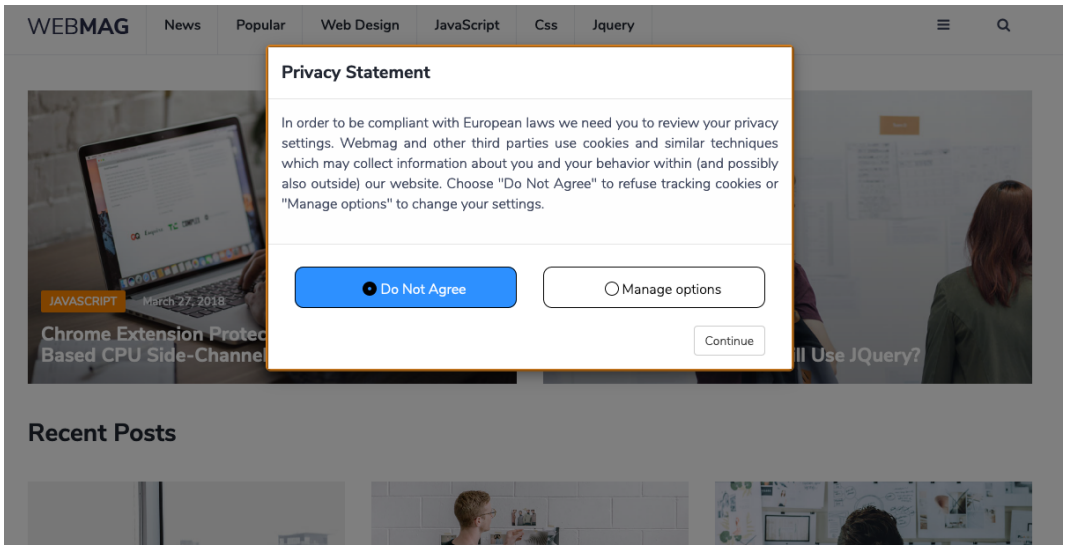

Figure 6. Example consent request featuring all three bright patterns default, aesthetic manipulation and obstruction. Website: Webmag

3.1.2.2 Measures

All measures of Experiment 1 were also in place in Experiment 2. As in the first study, perceived control (range: 0 - 100, M = 39.55, SD = 28.90) showed very good internal consistency with a raw Cronbach's α = 0.98. Observed deliberation levels had a range of 0 - 100, M = 26.97 and SD = 28.61. General privacy concerns, with a range of 1.33 - 7, M = 4.23 and SD = 1.15, showed acceptable to good internal consistency with a raw Cronbach's α = 0.77.

Manipulation checks included again the question for each consent request whether the participant had read the consent information (in 11.8% of the cases "Read it completely", 48.2% "Skimmed it", 40.0% "Did not read it at all") before clicking on one option and whether they remembered which option ("Agree", "Do Not Agree") they had chosen (15.3% of all consent decisions could not be remembered correctly). Further, participants provided information on whether they had installed a browser plugin, which handles or deletes cookies (19.8% "Yes", 80.2% "No").

Additionally to all measures of Experiment 1, we added a questionnaire about privacy fatigue, developed by Choi et al. (2018), to the follow-up experiment. We did not include items that Choi et al. (2018) deleted due to cross-loading (or other reasons). Privacy fatigue, measured on a seven-point scale ranging from *Strongly disagree* to *Strongly agree*, with a range of 1.50 - 7, M = 4.40 and SD = 1.01, showed acceptable internal consistency with a raw Cronbach's α = 0.71. Although dropping questionnaire item one would increase the overall α-level by 0.02 we refrained from

doing so because the increase was too marginal to question the theoretical structure of the scale. We used the average of all six items in the statistical analysis to form the control variable privacy fatigue.

3.1.3 Participants

We recruited a total of $N = 255$ participants for Experiment 2 via the crowdsourcing platform Prolific Academic. This sample size was based on the sample size of Experiment 1 and followed the same inclusion criteria.

On average it took participants 10.60 minutes ($SD = 5.28$) to complete the study. We left 54 participants out of this calculation because they showed very long completion times, indicating that they divided the study over several days. Yet, their consent behaviour did not seem to differ from the rest of the sample and thus they were kept for analysis. Similar as in Experiment 1, only 7 participants completed the experiment in less than 5 minutes (but not under 3 minutes). Because of the low number we kept them in the sample. We excluded participants who could not finish the study due to technical problems.

The total sample population consisted of 175 females (68.6%), 79 males (31.0%), 1 person identifying as "Other" (0.4%) and had a mean age of 35.20 years ($SD = 10.97$). Of all 255 participants who took part in the experiment, 58 dropped out in the second part of the study (i.e., after reviewing the eight news websites). Again, none of the dropouts happened during the completion of a questionnaire (only in between) and we detected no prevalent pattern of missingness (e.g., the consent behaviour did not differ between participants with complete cases and those who would drop out later on). Hence, we found all participants' data eligible for analysis.

3.1.4 Data Analyses

Experiment 2 followed the same analysis approach (including the same model structures) as Experiment 1 to ensure valid one-to-one result comparison. The only addition in Experiment 2 were two extra exploratory models (following the structure of the main models) with privacy fatigue instead of privacy concerns as the control variable, to see whether this would change the pattern of results.

3.2 Results

3.2.1 Main Analyses

To investigate our third set of hypotheses 3a/b/c (stating that bright patterns will sway people towards the "Do Not Agree" option) we again first visualise the recorded consent decisions for each news website (see Figure 7). We observed that in Experiment 2 only in slightly more than half of the cases (53.2%) people chose to agree to the consent requests, representing a reduction of 40.7% compared to

Experiment 1. This time, more than one-third of the participants (36.1%) changed their consent behaviour between conditions. This trend is reflected by our results, which showed that two of the three tested design nudges swayed participants effectively towards the "Do Not Agree" option.

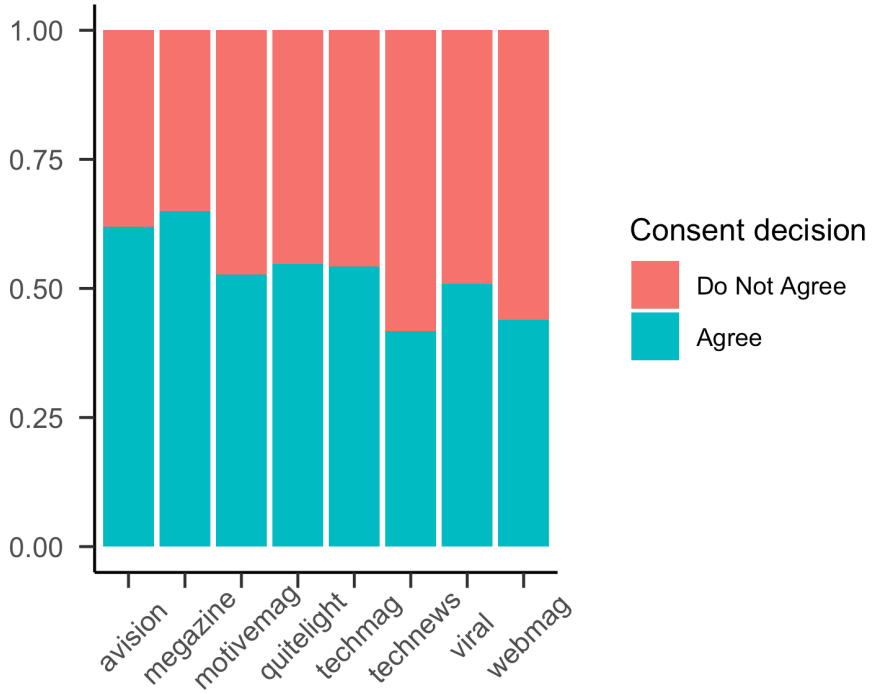

Figure 7. Consent decisions (proportional) by condition (different news websites)

Specifically, we found a substantial main effect of default, β = -0.75 (0.13), CrI 95% [-1.01, -0.51], OR = 0.47, and obstruction, β = -0.97 (0.20), CrI 95% [-1.39, -0.60], OR = 0.38, on the outcome consent decision (see Figure 8), supporting our hypotheses H3a and H3c respectively. Given that we kept the outcome consent decision coded as in the original study (0 = "Do Not Agree", 1 = "Agree"), a negative effect estimate means an increased likelihood of selecting "Do Not Agree". To interpret odds ratios which are smaller than 1 in a meaningful way we will inverse them (1/OR). Hence, if the option "Do Not Agree" was selected by default, the odds of participants choosing this option were two times higher than if the option had not been preselected. Similarly, if the "Agree" option was obstructed the odds of participants choosing the "Do Not Agree" option were two and a half times higher than if the "Agree" option had not been obstructed. We did not find support for Hypothesis H3b however, as there was no notable effect of aesthetic manipulation, β = 0.06 (0.14), CrI 95% [-0.21, 0.34], OR = 1.06. The pattern of results did not change when additionally accounting for a participant's previous consent decision or whether the participant had a browser plugin installed that handles or deletes cookies.

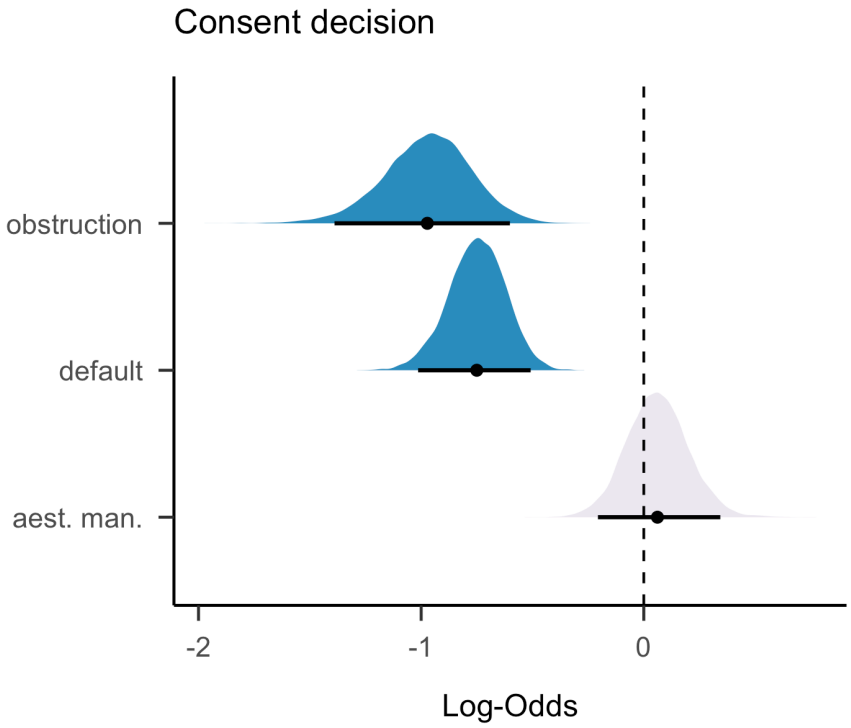

Figure 8. Posterior distributions with mean and 95% credible interval for the predictors default, aesthetic manipulation and obstruction (outcome consent decision)

Testing our fourth set of hypotheses 4a/b/c, we did not find that (bright) design nudges made people perceive less control over their personal data. Rather, we replicated the result pattern of Experiment 1, including the finding that obstructing one choice option led participants to report more rather than less perceived control.

Specifically, obstruction showed a small but notable main effect, β = 0.06 (0.03), CrI 95% [0.00, 0.12], OR = 1.06, on the outcome perceived control (see Figure 9). Hence, hypothesis H4c was not supported. Further, we did not find support for hypotheses H4a and H4b concerning the effects of default, β = -0.01 (0.01), CrI 95% [-0.04, 0.02], OR = 0.99, and aesthetic manipulation, β = -0.02 (0.02), CrI 95% [-0.07, 0.02], OR = 0.98. We checked again whether accounting for a browser plugin installation that handles or deletes cookies changed the pattern of results, but this was not the case.

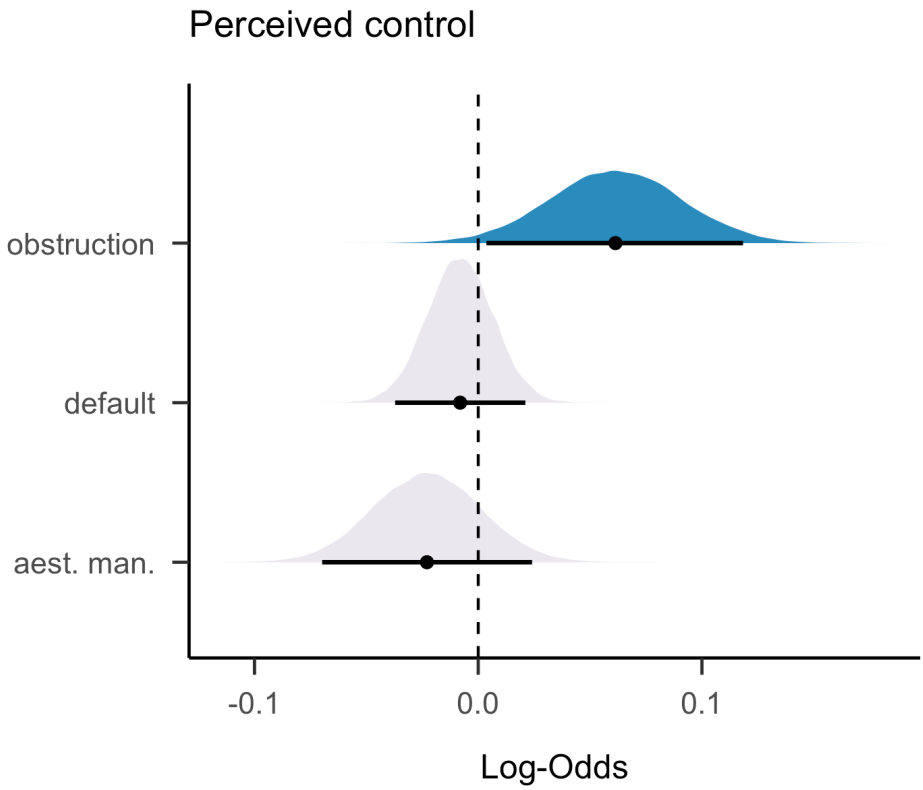

Figure 9. Posterior distributions with mean and 95% credible interval for the predictors default, aesthetic manipulation and obstruction (outcome perceived control)

3.2.2 Exploratory Analyses

Apart from investigating possible moderation effects of deliberation (as in Experiment 1), we ran two additional mixed-effects models with privacy fatigue instead of privacy concerns as a control variable to see whether this would change our results.

As in the original study, the extent to which participants deliberated about their choices did not substantially influence the effects of the three bright patterns on participants' consent decisions: default, β = 0.05 (0.16), CrI 95% [-0.27, 0.36], OR = 1.05, aesthetic manipulation, β = 0.02 (0.17), CrI 95% [-0.32, 0.36], OR = 1.02, and obstruction, β = 0.22 (0.21), CrI 95% [-0.20, 0.65], OR = 1.25. Neither did the extent to which participants deliberated about their choices substantially influence the effects of the three bright patterns on participants' perceived control: default, β = 0.00 (0.02), CrI 95% [-0.03, 0.04], OR = 1.00, aesthetic manipulation, β = 0.01 (0.02), CrI 95% [-0.03, 0.06], OR = 1.01, and obstruction, β = -0.01 (0.03), CrI 95% [-0.06, 0.04], OR = 0.99. This finding may be due to the fact that participants reported again generally low levels of deliberation (M = 20.99, SD = 25.33).

Replacing privacy concerns with privacy fatigue as the control variable showed that privacy fatigue acted across all models in the opposite direction as privacy

concerns. While higher levels of privacy concerns were associated with being less likely to agree to the consent requests, higher levels of privacy fatigue were associated with being more likely to choose "Agree". However, the pattern of results did not differ whether privacy concerns or privacy fatigue was used as a control variable.

3.3 Discussion

The follow-up experiment aimed to explore how design nudges towards the privacy-friendly option (i.e., bright patterns) would influence people's consent choices and their perception of control compared to what we found in Experiment 1.

The first finding was that people did not agree to every cookie consent statement in a default manner anymore (as many had done in Experiment 1). Compared to Experiment 1, about ten times more people changed their consent behaviour between conditions in Experiment 2. Given that all we changed between Experiment 1 and Experiment 2 was the direction of the design nudges, the results illustrate that these seemingly small tweaks in the interface can heavily influence people's privacy choices. The results also support the suspicion that the effects of the dark patterns in Experiment 1 were obscured, because people may be conditioned to always agree to cookie consent requests. People might have developed such automatic behaviour by reviewing thousands of ambiguous cookie consent requests, or even take-it-or-leave-it choices. Specifically, we found that people were substantially more likely to choose "Do Not Agree" if this option was preselected or the alternative "Agree" option obstructed.

The result pattern regarding perceived control over one's personal data was very similar between the two experiments. In each experiment, people reported that they perceived little control over their personal data. However, we could not find that the design nudges had led to this low level of perceived control. Surprisingly, in both cases, obstructing one choice option led people to perceive more rather than less control over their personal data. One possible explanation could be that the phrase "Manage options", which obstructed either the "Agree" (Experiment 1) or "Dot Not Agree" (Experiment 2) option, conveyed somehow the feeling of control. Further discussion of these findings follows in the subsequent general discussion.

4 GENERAL DISCUSSION

In the last part of this paper, we first summarise our findings and discuss how they fit into the existing literature and the theoretical framework of privacy decision making (in the context of design nudges). In a second step, we shift towards practical approaches to address the problems of the current consent system. Specifically, we explore how policymakers could address problems with the legal

consent requirement for tracking cookies. Lastly, we will address limitations of our experiments and give suggestions for future work.

4.1 Summary and theoretical implications

Overall, our findings were in line with previous research (Machuletz & Böhme, 2019; Utz et al., 2019) and form additional evidence supporting the persuasive power of design nudges on users consent choices. In Experiment 1 (featuring dark patterns that people are used to) it did not seem to differ for participants' consent behaviour whether design nudges were used or not. However, in Experiment 2 (featuring bright patterns), two out of the three tested design nudges substantially affected people's consent choices in the hypothesised direction. As the only difference between the two experiments was the direction of the design nudges, it appears that such nudges influence privacy choices after all.

Why did we observe this discrepancy between the results of the two experiments? Nudges are often thought of as manipulations of the choice environment which only elicit their potential effect while being in place (i.e., no long-term effect). However, it may be that this changes when nudges (specifically System 1 nudges) are used for longer periods of time (e.g., seeing consent requests with dark patterns for years). A form of conditioning may happen, ultimately leading people to behave in a certain way even in absence of the nudge (e.g., participants agreeing to the consent request in the baseline condition without any design nudges present). Hertwig and Grüne-Yanoff (2017) refer to this process of "effect survival" after the removal of the nudge as the development of behavioural routines. Of course, design nudges are probably not the only reason for this conditioning to happen, but they certainly have the potential to play an important role.

Concerning the influence of the design nudges on participants' perception of control over their personal data, our results were stable across both experiments but did not support our assumptions. Although participants had (theoretically) full control over each decision in our study (i.e., for each consent request there was the possibility to choose "Do Not Agree"), they did not seem to perceive it that way, possibly because they are used to ambiguous real-life consent requests, which do not always offer a meaningful choice. Surprisingly, people perceived more rather than less control if one choice option was hidden behind "Manage options". As mentioned in the discussion of Experiment 2 the formulation "Manage options" may have somehow (unjustified) conveyed the feeling of control, highlighting the manipulative effect of design nudges. This is in line with what Forbrukerrådet (2018) describe as the "illusion of control". Further considerations and suggestions for future work are discussed at the end of the paper.

4.2 Practical implications

Taking these findings into account, the question arises how problems of the current consent system for tracking cookies could be addressed so that online privacy self-management works in a meaningful way. We believe that there are two ways to tackle the issue: Focusing on users or on companies. First, we discuss approaches that focus on the user.

By focusing on the user, we mean any attempt to change the behaviour or competences of the user. Following Hertwig and Grüne-Yanoff (2017), we differentiate between nudging approaches, which try to change behaviour by altering the choice architecture, and boosting approaches, which focus on competence building to enable a certain behaviour. Non-educative nudges, such as bright patterns, could be used to nudge users towards the privacy-friendly option, as in Experiment 2. These bright patterns do not require any motivation from the user but may lead to similar problems as their dark counterparts, such as unreflective default behaviour and users' perception of a lack of control.

Further, there are educative nudges (after Sunstein, 2016b) such as reminders or warnings, which build a middle ground between nudging and boosting, because they require some level of motivation to foster a context-specific competence (called short-term boosts by Hertwig & Grüne-Yanoff, 2017). In the context of cookie consent requests, an example of an educative nudge could be feedback about possible consequences of a choice. However, the company that asks for consent would have to implement this educative nudge. As many companies have incentives to nudge internet users towards the privacy-unfriendly option (e.g., to collect data for targeted advertising), the practical feasibility of such nudges is questionable. After all, if policymakers require companies to implement pro privacy nudges, the companies can sabotage those nudges (Willis, 2014).

Lastly, there are long-term boosts, which aim at a permanent change of skills and decision tools. In theory, boosts, which aim at building procedural rules such as "When I see a consent request I read the provided information before making a choice" could be used in the context of cookie consent requests. Such boosts, in theory, could be suitable to break people out of automatic behaviour and to help them deliberate before making a choice. However, long-term boosts are often costlier than nudges (e.g., changing a default requires less time and effort than creating an intervention to form procedural rules). In addition, boosts only work if people are motivated to acquire new skills.

Presumably, people's motivation to deliberate about cookie consent requests is low. If somebody wants to visit a website, having to think about a consent request is an unwelcome hurdle. If people lack the motivation to build certain competences, Hertwig (2017) advises to use nudging rather than boosting approaches. This brings us back to bright patterns, which do not require motivation from the user. However, as noted, many companies using dark patterns have an interest in tracking people's online behaviour, so it does not seem plausible that such companies will

implement effective pro-privacy nudges. Consequently, user-focused approaches seem unrealistic for the context of cookie consent requests.

A second strategy focuses not on the user, but on changing the behaviour of companies. Amending legal requirements can influence company behaviour. Our consent requests were designed in a way that they resemble many of those requests used in practice under the ePrivacy Directive. Thus, the results of our experiments illustrate that consent requests often do not lead to genuinely "informed" consent, considering that most participants did not read the consent information, and reported a lack of control over their personal data. Dark patterns may play a role in that, but based on our study findings it cannot be concluded that stricter design regulations for consent requests alone (i.e., banning dark patterns from consent requests) would resolve the problem. After all, most participants also agreed to web tracking in the baseline condition of Experiment 1 without any design nudge present. Overall, this study contributes to a body of research that questions the effectiveness of legal informed consent requirements as a privacy protection tool (Acquisti et al., 2017; Zuiderveen Borgesius, 2015a). How should policymakers react?

Could enforcement of current law push companies to use bright patterns? As noted, the ePrivacy Directive (2009) requires consent for tracking cookies and similar tracking techniques; the GDPR's strict conditions for valid consent apply. But these two instruments do not explicitly ban dark patterns in consent requests, let alone require bright patterns. Dark patterns do violate the spirit of the GDPR, for two reasons. First, the GDPR requires that personal data are only collected "fairly and in a transparent manner in relation to the data subject" (article 5(1)(a)). Many dark patterns could be regarded as unfair. However, the fairness requirement is rather vague, and therefore difficult to enforce.

Second, an argument could be made that the GDPR generally discourages the use of dark patterns, because the GDPR bans certain types of dark patterns. For instance, the GDPR bans opt-out systems (that assume consent if people fail to object), pre-selected "I consent" options, and certain types of tracking walls and similar take-it-or-leave-it choices (article 4(11) and article 7). The GDPR also states that a consent "request must be clear, concise and not unnecessarily disruptive" (recital 32), and must use "plain language and (…) should not contain unfair terms" (recital 42). Some dark patterns may violate those requirements. Moreover, European regulators note that "dark patterns (…) are contrary to the spirit of Article 25" of the GDPR, which requires privacy by design (European Data Protection Board, 2020).

All in all, the extent to which the GDPR bans dark patterns must become clear in case law and enforcement actions by Data Protection Authorities. In 2018, seven consumer organisation filed complaints with national Data Protection Authorities regarding location tracking by Google. The organisations also complain about dark patterns (BEUC, 2020). However, Data Protection Authorities did not

finish their investigations yet. More generally, it may take a long time before there is enough case law to push companies towards abandoning dark patterns.

Amendments to the law could be useful. The European Commission (2017) published a proposal to replace the ePrivacy Directive with an ePrivacy Regulation. The proposal for the ePrivacy Regulation contains promising ideas, especially after the European Parliament (2017) amended it. For instance, under the ePrivacy Regulation, it would be obligatory for any company to respect "Do Not Track" and similar signals (European Parliament, 2017). With "Do Not Track" or a similar system, an internet user can choose a setting on their device once, which communicates to all websites and tracking companies that the user does not want to be tracked. Such a "Do Not Track"-like solution could limit the number of times that people are asked to consent to tracking (Zuiderveen Borgesius et al., 2017).

Perhaps additional rules are needed to ensure that companies refrain from asking people to make an exception to their "do not track me" setting. The ePrivacy proposal also bans companies from using "tracking walls", a barrier that visitors can only pass if they consent to tracking by third parties (European Parliament, 2017). However, at the moment it is unclear whether and in what form the ePrivacy proposal will be adopted (Legislative Train Schedule, 2020).

4.3 Limitations and suggestions for future research

The first limitation of our study that future research should address is the location of the presented choice options. Known as Fitts's law, which is a predictive model of human movement, one can assume that it is easier and faster to hit larger targets closer to you than smaller targets further away from you (MacKenzie, 1992). In our design of the consent requests the "Agree" option was on the right-hand side and thus closer to the "Continue" button (which was also on the right-hand side) than the "Do Not Agree" option, which was on the left-hand side. This setup was inspired by what we saw in real-life practice but might have acted as an additional design nudge. It could be interesting to include eye-tracking measurements to follow participants visual attention while they encounter cookie consent requests.

A second limitation relates to our conceptualisation of rational choice. We base ourselves on the privacy calculus theory to weigh the privacy risks against the privacy benefits of each choice in the consent request. Not included in this calculation are factors such as little time differences between choosing one option versus the other, which arise for instance when one option is obstructed (e.g., choosing one option requires more mouse clicks than the other). These factors, however, are often the mechanistic core of a design nudge and thus hard to "strip away".

Third, we had to compromise between ecological validity and a controlled experimental setting for the design of our consent requests. To include all three design nudges at the same time, we had to choose a consent request setup, which deviated slightly from most real-life consent requests. Namely, we presented the

available choice possibilities in the form of radio buttons (which can be ticked) instead of clickable buttons, because regular buttons cannot be preselected (which is needed for the design nudge default).

Fourth, we had to tweak some aspects of the design of each consent request (see Appendix B or the Open Science Framework) to match the design of the corresponding news website and make the cover story of eight independent external news websites plausible. While these changes may seem arbitrary, we paid close attention to not change any parts close to the choice options in which our manipulations where applied.

Fifth, our design complicated the reliable measurement of participants' perceived control over their personal data, which was assessed with a time delay to the actual consent decisions (i.e., after all eight news websites had been reviewed). This was due to our study design involving the cover story about the first impression of the design of news websites, which would have been compromised when drawing attention on the consent requests during part 1 of the experiment (i.e., while reviewing the news websites). In addition, the slider with which people could indicate how much control they perceived had a default setting of *Not at all*. We chose this setting because it resembled in our opinion the most neutral and intuitively understandable starting position (compared to the middle between *Not at all* and *Complete control*). However, this setting may have partially caused the previously discussed floor effect (see results section of Experiment 1). Future studies should reconsider the scale's default position and its possible consequences for measurement. Nonetheless, we hope to have created a starting point for future research to assess perceived control specifically in the context of consent requests. Further, it may be valuable to investigate the concept of perceived control additionally through a qualitative approach to shed light onto the possible shortcomings of the quantitative approach which was used so far.

Lastly, future research should investigate whether and under what circumstances conditioning and behavioural routines develop regarding informed consent procedures. In a second step, it could be examined how these behavioural routines may be disrupted, for instance by applying friction to the decision process to stimulate deliberation (Terpstra, Schouten, Rooij, & Leenes, 2019; Zuiderveen Borgesius, 2015).

4.4 Conclusion

Overall, this project shed light on some of the mechanisms of design nudges in cookie consent requests. Our research findings demonstrate some of the shortcomings of legal consent requirements for cookies and similar rules that expect people to make many informed choices about their privacy. We explored possible solutions to face these shortcomings. For instance, the upcoming ePrivacy Regulation of the EU should limit the number of cookie consent requests people are confronted with. Policymakers should not put unreasonable burdens on people's

shoulders and avoid responsibilisation. Responsibilisation describes "the process whereby subjects are rendered individually responsible for a task which previously would have been the duty of another – usually a state agency – or would not have been recognized as a responsibility at all" (Wakefield & Fleming, 2009, p. 276; see also Gürses, 2014). In conclusion, the concept of informed consent is not obsolete in the digital era but should be used wisely and sparingly (see also Böhme and Köpsell, 2010). In the case of web tracking and personalisation, this could mean, for instance, a global option in the browser which has to be set only once.

FUNDING STATEMENT

This project is primarily funded by the Behavioural Science Institut (BSI) and partly by the Dutch Research Council (NWO), for the research program 'SocialMovez' with project number VI.C.181.045

ACKNOWLEDGEMENTS

We would like to thank the reviewers for their valuable comments to improve the manuscript. Further, we thank Franc Grootjen and Ayke van Laethem for their technical advice; Franc especially for providing a university server.

REFERENCES

Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., … Schaub, F. (2017). Nudges for privacy and security. ACM Computing Surveys, 50(3), 1–41. https://doi.org/10.1145/3054926

Albar, F. M., & Jetter, A. J. (2009). Heuristics in decision making. In PICMET '09 - 2009 Portland International Conference on Management of Engineering & Technology (pp. 578–584). IEEE. https://doi.org/10.1109/PICMET.2009.5262123

An, N. Z. (2019). Multi-step modals for Bootstrap. Retrieved from https://github.com/ngzhian/multi-step-modal

Archer, M. S. (2013). Rational choice theory. Routledge. https://doi.org/10.4324/9780203133897

Auguie, B. (2017). GridExtra: Miscellaneous functions for "grid" graphics. Retrieved from https://CRAN.R-project.org/package=gridExtra

Aust, F., & Barth, M. (2020). papaja: Create APA manuscripts with R Markdown. Retrieved from https://github.com/crsh/papaja

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly, 1328.

Barr, D. J., Levy, R., Scheepers, C., & Tily, H. J. (2013). Random effects structure for confirmatory hypothesis testing: Keep it maximal. Journal of

Memory and Language, 68(3), 255–278. https://doi.org/10.1016/j.jml.2012.11.001

BEUC. (2020). The long and winding road. Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective. Retrieved from https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf

Böhme, R., & Köpsell, S. (2010). Trained to accept?: A field experiment on consent dialogs. In Proceedings of the 28th international conference on Human factors in computing systems - CHI '10 (p. 2403). Atlanta, Georgia, USA: ACM Press. https://doi.org/10.1145/1753326.1753689

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies, 2016(4), 237–254. https://doi.org/10.1515/popets-2016-0038

Brignull, H. (n.d.). Dark patterns. Retrieved from https://darkpatterns.org/

Brooke, B. (2011). Browser back button detection. Retrieved from http://www.bajb.net/2010/02/browser-back-button-detection/

Browne, W. J., & Draper, D. (2006). A comparison of Bayesian and likelihood-based methods for fitting multilevel models. Bayesian Analysis, 1(3), 473–514. https://doi.org/10.1214/06-BA117

Bryan, M. L., & Jenkins, S. P. (2016). Multilevel modelling of country effects: A cautionary tale. European Sociological Review, 32(1), 3–22. https://doi.org/10.1093/esr/jcv059

Bürkner, P.-C. (2017). brms: An R package for Bayesian multilevel models using Stan. Journal of Statistical Software, 80(1), 1–28. https://doi.org/10.18637/jss.v080.i01

Bürkner, P.-C. (2018). Advanced Bayesian multilevel modeling with the R package brms. The R Journal, 10(1), 395–411. https://doi.org/10.32614/RJ-2018-017

Carpenter, B., Gelman, A., Hoffman, M., Lee, D., Goodrich, B., Betancourt, M., … Riddell, A. (2017). Stan: A probabilistic programming language. Journal of Statistical Software, Articles, 76(1), 1–32. https://doi.org/10.18637/jss.v076.i01

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Colorbib. (2019). 28 best free news website templates 2019. Colorlib. Retrieved from https://colorlib.com/wp/free-news-website-templates/

Dijksterhuis, A., Bos, M. W., Nordgren, L. F., & van Baaren, R. B. (2006). On making the right choice: The deliberation-without-attention effect. Science, 311(5763), 1005–1007. https://doi.org/10.1126/science.1121629

Eddelbuettel, D., & Balamuta, J. J. (2017). Extending extitR with extitC++: A Brief Introduction to extitRcpp. PeerJ Preprints, 5, e3188v1. https://doi.org/10.7287/peerj.preprints.3188v1

Eddelbuettel, D., & François, R. (2011). Rcpp: Seamless R and C++ integration. Journal of Statistical Software, 40(8), 1–18. https://doi.org/10.18637/jss.v040.i08

ePrivacy Directive. (2009). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications), last amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 337 11). Retrieved from https://eur-lex.europa.eu/eli/dir/2002/58/2009-12-19

European Commission. (2017). Proposal for a regulation of the European Parliament and of the Council, concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (No. COM/2017/010 final - 2017/03 (COD)). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017PC0010

European Data Protection Board. (2020). Guidelines 4/2019 on Article 25 data protection by design and by default version 2.0, adopted on 20 October 2020. Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

European Parliament. (2017). Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (No. COM(2017)0010 C8-0009/2017 2017/0003(COD)). Retrieved from https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html

Fansher, M., Chivukula, S. S., & Gray, C. M. (2018). #Darkpatterns. In R. Mandryk, M. Hancock, M. Perry, & A. Cox (Eds.), Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18 (pp. 1–6). New York, New York, USA: ACM Press. https://doi.org/10.1145/3170427.3188553

Ferrari, S., & Cribari-Neto, F. (2004). Beta regression for modelling rates and proportions. Journal of Applied Statistics, 31(7), 799–815. https://doi.org/10.1080/0266476042000214501

Forbrukerrådet. (2018). Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy. Retrieved

from https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

GDPR. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal L, 119, 1–88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In R. Mandryk, M. Hancock, M. Perry, & A. Cox (Eds.), Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18 (pp. 1–14). New York, New York, USA: ACM Press. https://doi.org/10.1145/3173574.3174108

Grosjean, P., & Ibanez, F. (2018). Pastecs: Package for analysis of space-time ecological series. Retrieved from https://CRAN.R-project.org/package=pastecs

Gürses, S. (2014). Attitudes towards "Spiny CACTOS". Retrieved from https://vous-etes-ici.net/next-week-spiny-cactos-at-usec-2014/

Hertwig, R. (2017). When to consider boosting: Some rules for policy-makers. Behavioural Public Policy, 1(02), 143–161. https://doi.org/10.1017/bpp.2016.14

Hertwig, R., & Grüne-Yanoff, T. (2017). Nudging and boosting: Steering or empowering good decisions. Perspectives on Psychological Science : A Journal of the Association for Psychological Science, 12(6), 973–986. https://doi.org/10.1177/1745691617702496

Kahneman, D. (2011). Thinking, fast and slow (1st ed). New York: Farrar, Straus and Giroux.

Kay, M. (2020). tidybayes: Tidy data and geoms for Bayesian models. https://doi.org/10.5281/zenodo.1308151

Kowarik, A., & Templ, M. (2016). Imputation with the R package VIM. Journal of Statistical Software, 74(7), 1–16. https://doi.org/10.18637/jss.v074.i07

Lai, Y.-L., & Hui, K.-L. (2006). Internet opt-in and opt-out: Investigating the roles of frames, defaults and privacy concerns. In Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research Forty four years of computer personnel research: Achievements, challenges & the future - SIGMIS CPR '06 (p. 253). Claremont, California, USA: ACM Press. https://doi.org/10.1145/1125170.1125230

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of Social Issues, 33(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Legislative Train Schedule. (2020). Proposal for a regulation on privacy and electronic communications. Retrieved from

https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform

Lord, D., Mönnich, A., Ronacher, A., & Unterwaditzer, M. (2010). Flask (a Python microframework). Retrieved from http://flask.pocoo.org/

Luguri, J., & Strahilevitz, L. (2019). Shining a light on dark patterns. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3431205

Machuletz, D., & Böhme, R. (2019). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. arXiv:1908.10048 [Cs]. Retrieved from http://arxiv.org/abs/1908.10048

MacKenzie, I. S. (1992). Fitts' Law as a research and design tool in Human-Computer Interaction. HumanComputer Interaction, 7(1), 91–139. https://doi.org/10.1207/s15327051hci0701_3

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Morey, R. D., Hoekstra, R., Rouder, J. N., Lee, M. D., & Wagenmakers, E.-J. (2016). The fallacy of placing confidence in confidence intervals. Psychonomic Bulletin & Review, 23(1), 103–123. https://doi.org/10.3758/s13423-015-0947-8

Mullen, L. A., Benoit, K., Keyes, O., Selivanov, D., & Arnold, J. (2018). Fast, consistent tokenization of natural language text. Journal of Open Source Software, 3(23), 655. https://doi.org/10.21105/joss.00655

Müller, K. (2017). Here: A simpler way to find your files. Retrieved from https://CRAN.R-project.org/package=here

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. arXiv:2001.02479 [Cs]. https://doi.org/10.1145/3313831.3376321

R Core Team. (2020). R: A language and environment for statistical computing. Vienna, Austria: R Foundation for Statistical Computing. Retrieved from https://www.R-project.org/

Revelle, W. (2019). Psych: Procedures for psychological, psychometric, and personality research. Evanston, Illinois: Northwestern University. Retrieved from https://CRAN.R-project.org/package=psych

Schubert, C. (2015). On the ethics of public nudging: Autonomy and agency. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2672970

Simon, H. A. (1957). Models of man, social and rational: Mathematical essays on rational human behavior in a social setting. New York, NY, USA: Wiley.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. MIS Quarterly, 35(4), 989–1015.

Stauffer, R., Mayr, G. J., Dabernig, M., & Zeileis, A. (2009). Somewhere over the rainbow: How to make effective use of colors in meteorological

visualizations. Bulletin of the American Meteorological Society, 96(2), 203–216. https://doi.org/10.1175/BAMS-D-13-00155.1

Sunstein, C. R. (2016a). People prefer system 2 nudges (kind of). SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2731868

Sunstein, C. R. (2016b). The ethics of influence: Government in the age of behavioral science. Cambridge University Press.

Terpstra, A., Schouten, A. P., Rooij, A. de, & Leenes, R. E. (2019). Improving privacy choice through design: How designing for reflection could support privacy self-management. First Monday, 24(7). https://doi.org/10.5210/fm.v24i7.9358

Thaler, R. H. (2018). Nudge, not sludge. Science, 361(6401), 431–431. https://doi.org/10.1126/science.aau9241

Thaler, R. H., & Sunstein, C. R. (2009). Nudge: Improving decisions about health, wealth, and happiness (Rev. and expanded ed). New York: Penguin Books.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)Informed consent: Studying GDPR consent notices in the field. In ACM SIGSAC Conference on Computer and CommunicationsSecurity (CCS '19) (p. 18). London, United Kingdom. Retrieved from https://arxiv.org/pdf/1909.02638.pdf

Wakefield, A., & Fleming, J. (2009). The Sage dictionary of policing. Los Angeles; London: SAGE. Retrieved from http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9781446207017

Wickham, H. (2011). The split-apply-combine strategy for data analysis. Journal of Statistical Software, 40(1), 1–29. Retrieved from http://www.jstatsoft.org/v40/i01/

Wickham, H. (2016). Ggplot2: Elegant graphics for data analysis. Springer-Verlag New York. Retrieved from https://ggplot2.tidyverse.org

Wickham, H. (2019). Stringr: Simple, consistent wrappers for common string operations. Retrieved from https://CRAN.R-project.org/package=stringr

Wickham, H., François, R., Henry, L., & Müller, K. (2020). Dplyr: A grammar of data manipulation. Retrieved from https://CRAN.R-project.org/package=dplyr

Wickham, H., & Henry, L. (2020). Tidyr: Tidy messy data. Retrieved from https://CRAN.R-project.org/package=tidyr

Willis, L. E. (2014). Why not privacy by default. Berkeley Technology Law Journal, 29, 61. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/berktech29\&id=71\&div=\&collection=

Xie, Y. (2015). Dynamic documents with R and knitr (2nd ed.). Boca Raton, Florida: Chapman; Hall/CRC. Retrieved from https://yihui.org/knitr/

Xie, Y., Allaire, J. J., & Grolemund, G. (2018). R markdown: The definitive guide. Boca Raton, Florida: Chapman; Hall/CRC. Retrieved from https://bookdown.org/yihui/rmarkdown

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. ICIS 2007 Proceedings, 1–14.

Zeileis, A., Hornik, K., & Murrell, P. (2009). Escaping RGBland: Selecting colors for statistical graphics. Computational Statistics & Data Analysis, 53(9), 3259–3270. https://doi.org/10.1016/j.csda.2008.11.033

Zhu, H. (2019). KableExtra: Construct complex table with 'kable' and pipe syntax. Retrieved from https://CRAN.R-project.org/package=kableExtra

Zuiderveen Borgesius, F. (2015). Behavioural sciences and the regulation of privacy on the internet. OxfordHart. Retrieved from https://dare.uva.nl/search?identifier=b0052c52-9815-4782-b4b0-b1cabb3624d0

Zuiderveen Borgesius, F. (2015a). Improving privacy protection in the area of behavioural targeting. Kluwer Law International. Retrieved from https://hdl.handle.net/11245/1.434236

Zuiderveen Borgesius, F., Hoboken, J. van, Fahy, R., Irion, K., Rozendaal, M., (2017). An assessment of the Commission's proposal on privacy and electronic communications: Study. European Parliament, Committee on Civil Liberties Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

Zuiderveen Borgesius, F., Kruikemeier, S., Boerman, S. C., & Helberger, N. (2017a). Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy Regulation. European Data Protection Law Review, 3. https://doi.org/10.21552/edpl/2017/3/9

APPENDIX A

R language and packages

We used R (Version 4.0.2; R Core Team, 2020) and the R-packages brms (Version 2.13.5; Bürkner, 2017, 2018), colorspace (Version 1.4.1; Zeileis, Hornik, & Murrell, 2009; Stauffer, Mayr, Dabernig, & Zeileis, 2009), dplyr (Version 1.0.1; Wickham et al., 2020), ggplot2 (Version 3.3.2; Wickham, 2016), gridExtra (Version 2.3; Auguie, 2017), here (Version 0.1; Müller, 2017), kableExtra (Version 1.1.0; Zhu, 2019), knitr (Version 1.29; Xie, 2015), papaja (Version 0.1.0.9942; Aust & Barth, 2020), pastecs (Version 1.3.21; Grosjean & Ibanez, 2018), plyr (Version 1.8.6; Wickham et al., 2020; Wickham, 2011), psych (Version 2.0.7; Revelle, 2019), Rcpp (Version 1.0.5; Eddelbuettel & François, 2011; Eddelbuettel & Balamuta, 2017), rmarkdown (Version 2.3; Xie, Allaire, & Grolemund, 2018), stringr (Version 1.4.0; Wickham, 2019), tidybayes (Version 2.1.1; Kay, 2020), tidyr (Version 1.1.1; Wickham & Henry, 2020), tokenizers (Version 0.2.1; Mullen, Benoit, Keyes, Selivanov, & Arnold, 2018), and VIM (Version 6.0.0; Kowarik & Templ, 2016) for all analyses and reporting.

APPENDIX B

Consent requests

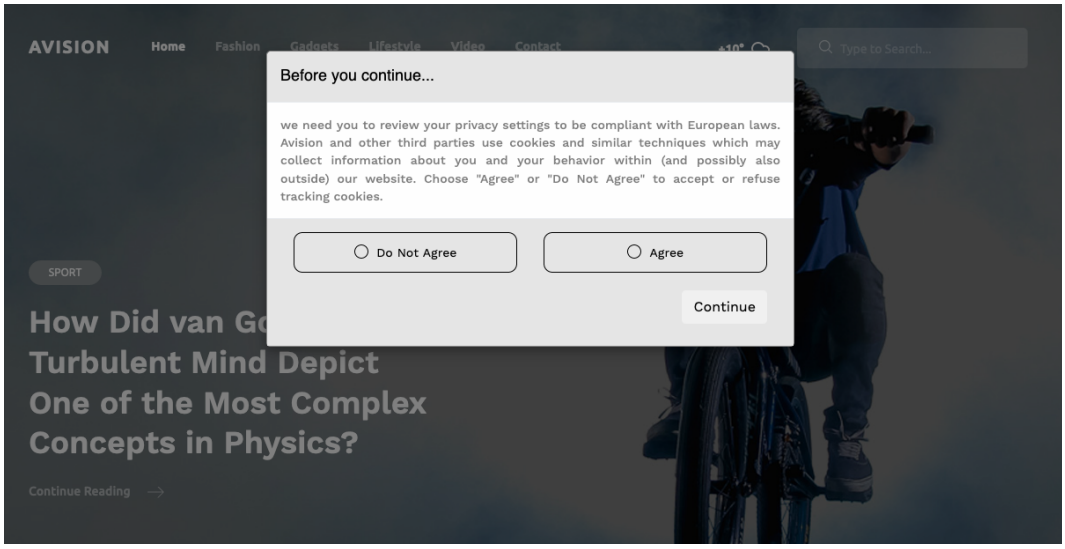

Figure B1. Example Condition 1. Baseline. Website: Avision

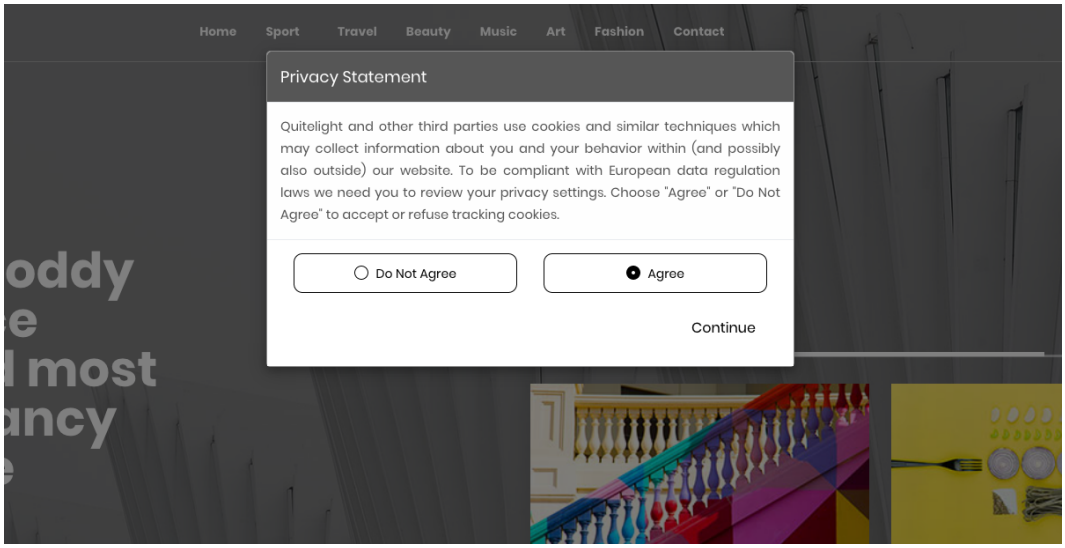

Figure B2. Example Condition 2. Default. Website: Quitelight

APPENDIX C

Example consent request text from condition 1, news website Avision:

"we need you to review your privacy settings to be compliant with European laws. Avision and other third parties use cookies and similar techniques which may collect information about you and your behavior within (and possibly also outside) our website. Choose 'Agree' or 'Do Not Agree' to accept or refuse tracking cookies."

JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 1, 2021, 39–59

IMAGINING THE COMMONING LIBRARY: ALTER-NEOLIBERAL PEDAGOGY IN INFORMATIONAL CAPITALISM

Dimitris Soudias*

ABSTRACT

The ascent of neoliberalism and informational capitalism has been largely successful in privatizing and re-regulating state-subject-market relations in ways that treat them "as if" they are a market situation. Here, we observe both the increasing commodification of digital forms of knowledge, as well as the commodification of the access to this knowledge. As predominantly non-commercial spaces, libraries serve the vital function of deflecting these developments. In this article, I argue for going one step further and imagining libraries as *institutionalized and pedagogical spaces that can negotiate and transgress their institutional limits vis-à-vis public and private resources, discourses, policies, and technologies for the purpose of furthering the commons.* In so doing, libraries serve as alter-neoliberal pedagogies, which democratize the construction and deconstruction of knowledge, as well as the access to them. Here, alternative literacies, ways of learning, and ways of being can be prefigured in practice. In imagining these conceptual potentialities of academic and public libraries, this article sets forth an initial agenda toward the commoning library.

Keywords: Digital Commons; Public Space; Libraries; Neoliberalism; Privatization; Commodification; Austerity; Policy

* London School of Economics and Political Science, United Kingdom.

1 INTRODUCTION

Some thirty years ago, the fortunate combination of innovations in ICT and relative respect for net neutrality allowed for the emergence of novel modes of information and knowledge production, modes, which are based on such principles as cooperation, peer-to-peer production, and shared or collective forms of ownership. Today, Wikipedia and open-source projects such as GNU, LINUX, or Firefox are but a few prominent examples of how digitalization has contributed to the democratization of knowledge, where knowledge is produced, shared, and maintained in ways that render them as digital commons (e.g. Fuchs, 2020; Papadimitropoulos, 2020; Wittel, 2013). At the same time, the ascent of neoliberalism from the 1970s onward has been largely successful in re-regulating state-subject-market relations in ways that treat knowledge "as if" it is in a market situation (e.g. Davies, 2014; Mirowski, 2014). Indeed, the internet itself has undergone significant transformations from a massive publicly funded effort, to a now essentially privately administered system (Tarnoff, 2016). In effect, digital knowledge, and the access to it, has become increasingly privatized and governed by Big Tech, while the politics of austerity across the globe have dismantled public spaces and institutions. This has led to a situation in which the market now actively denies certain groups knowledge and participation.

This article signifies a normative intervention in the conceptual potentialities of libraries as they resist these developments, by fertilizing library and information science scholarship with considerations for the political economy of informational capitalism, science and technology studies, the sociology of space, and the study of the commons. With a predominantly non-for-profit mandate, libraries serve the vital societal function of providing access to knowledge for their respective communities. In so doing, they prevent precisely the kind of commodification of knowledge that is so inherent to neoliberal reason. I argue for radicalizing the mandate of libraries via two mutually constitutive capacities: as facilitators for spaces of commoning knowledge, and as what I call "alter-neoliberal pedagogies." Specifically, I claim this requires conceiving of libraries in a Bourdieusian (2013) fashion, as structured structures, and structuring structures, which facilitate the construction of spaces of commoning, and thereby become themselves agents of commoning. In so doing, libraries may serve an alter-neoliberal pedagogical function—where alternative literacies, ways of learning, and ways of being, are nurtured in practice, thereby suggesting that we think of ourselves as *social* beings in a society, with needs and desires; rather than as individualized, consumerist, entrepreneurial and utility-maximizing *economic* beings in a market.

There are three interrelated caveats that need to be highlighted before developing these claims. First, this article is concerned with imagining the commoning potentialities of "formally institutionalized" libraries. Indeed, there are rich (historical) examples of radical, mostly informal, library experiments, such as the Freedom Libraries in the context of the Civil Rights Movement in the United

States (Selby, 2019), self-organized library structures in squatted university spaces in Greece (Antidrastirio, 2018), or indigenous approaches to knowledge organization in Canada (Webster & Doyle, 2008)—the latter of which points to the need to decolonize library epistemologies (e.g. Duarte & Belarde-Lewis, 2015). While these experiences provide radical imaginaries of what is conceivably possible, this article draws near the Foucauldian assumption to "not begin with liberty, but with the limit" (as cited in Bernauer & Maron, 2005, p. 151), and focuses instead on the potentialities of commoning within the constraints of formally institutionalized, state-funded libraries. This points to the second caveat, which is that this article is primarily concerned with public and academic libraries, though its conceptual considerations may hopefully be picked up by others and extended to special and school libraries. The third caveat relates to the varying library systems across the world, for which this article cannot account for due to its scope. In Germany or Greece, for example, academic libraries provide a variety of services for the wider public, which are often free of charge. In the Unites States, on the other, while land-grant university libraries are more easily accessible to the public than private academic libraries, they generally charge fees for borrowing privileges, and usually restrict access to certain services. The central takeaway is that these realities limit the ways in which commoning practices may be carried out.

To navigate these caveats, a guiding theme throughout this article is to investigate *how libraries, as institutionalized and pedagogical spaces, can negotiate and transgress their institutional limits vis-à-vis public and private resources, discourses, policies, and technologies for the purpose of furthering the commons.* This consideration significantly overlaps with Gayatri Spivak's (2012) concept of "affirmative sabotage", which turns a binary into a subtle dialectic: in suggesting that affirmation can include a critical capacity and vice versa, it pushes against and beyond the dichotomy of affirmative vs. critical culture (in Marcuse's sense), and suggests that public and private instruments of domination can be remodulated so as to become techniques for their transgression—in this case, for furthering the commons. For illustrative purposes, this article lays bare these dynamics sequentially. The following section contextualizes the urgency of imagining a commoning library by shedding light on the ways in which informational capitalism and the politics of austerity have both commodified digital knowledge and dismantled public spaces. Section three reconsiders the spatial functions of libraries in times of austerity. The fourth section mobilizes these considerations, so as to illustrate the commoning potentialities for libraries, while the fifth section highlights the alter-neoliberal pedagogical character of such an endeavor. Section six points to the institutional and organizational limitations of this approach. Then theorizing from these observations, the final section outlines an initial (policy) agenda for the commoning library.

2 INFORMATIONAL CAPITALISM AND THE DUAL COMMODIFICATION OF KNOWLEDGE

Early Austrian neoliberals, such as Friedrich von Hayek and Fritz Machlup, considered ideas as non-rivalrous resources and opposed treating them as property, as this was assumed to create artificial scarcity and monopolies (Slobodian, 2020). From the 1970s onward, however, the narrative shifted: competition, profit, and intellectual property protection have been seen as indispensable to innovation, and central to warrant incentives for intellectual production (Aspragathos, 2013). The installation of a global intellectual property regime in the 1990s has institutionalized the legal framework for patenting ideas, and hence commodifying knowledge, while digital rights management systems started to compromise the private use exemption by commodifying the very access to digital knowledge (Lucchi, 2006).

These developments facilitated the emergence of what Fuchs (2013, p. 419) refers to as "transnational informational capitalism", which is "based on the rise of cognitive, communicative, and co-operative labour that is interconnected with the rise of technologies and goods that objectify human cognition, communication, and co-operation." Informational Capitalism generates revenue through the commodification of knowledge, as well as the commodification of the access to knowledge (e.g. through paywalls, or "free" subscription where we "pay" with our personal data). This *dual commodification* has led to a situation in which various forms of digital knowledge are, regardless of de facto legal constraints, increasingly hosted—and therefore controlled—by large corporations that can define the ways in which knowledge is accessed and used (de Filippi & Said Vieira, 2014). Here, access and use are often regulated technocratically by algorithms whose workings are not only biased (Costanza-Chock, 2018), but usually also opaque and protected as trade secrets (Moore, 2017). In effect, this dual commodification undermines democratic scrutiny and debate (cf. Brown, 2015) and becomes inherently authoritarian as private algorithms decide for us and, increasingly, about us. Digital knowledge forms, ranging from text and code to audio and visual contents, are treated not as public service but as products packaged for profit, while users are treated as consumers, rather than (political) subjects. Worse still, users (or rather: their attention) have themselves become the commodity, as they are increasingly "formatted" to "informational persons" (Koopman, 2019), while their experiences are extracted and translated into behavioral data for profit (Zuboff, 2019).

Arguably, the emergence of "fake news" and misinformation needs to be seen within this context. Gray et al. (2020) convincingly illustrate how the commodification of attention (e.g. through clickbaiting), the metrification of engagement (e.g. through the "like button"), and the ranking of content (via algorithms), facilitates the spread of post-truth discourses. Relatedly, Hirst (2017) has highlighted the susceptibility of algorithms to manipulation. Furthermore, programmed bot armies have repeatedly managed to spread misinformation via

Google and Facebook by mimicking human natural language. Cynically, the algorithmic amplification of misinformation enriches such social media platforms.

While informational capitalism privatizes and commodifies the ways we use *digital* spaces, the politics of austerity across the globe have led to a corrosion of *physical* public spaces and infrastructures of service provision and care, as neoliberal policies—often grounded in the peculiar Hayekian (2005) assumption that collectivity inexorably leads to totalitarianism—seek to dismantle collective institutions, be it youth clubs, unions, or libraries. In so doing, they dissolve precisely the kind of spaces that allow for people to gather in solidarity and critically engage with the status quo. Against the background of the COVID-19 pandemic, this trend is likely to continue, as digitalization is sped up and public spaces are either criminalized (Soudias, 2020a) or dismantled altogether (Honey-Rosés et al., 2020). As I will show in the following sections, libraries may well play an important role in thwarting off the dual commodification of knowledge and the access to knowledge. They can do so by transgressing their public character for the alter-neoliberal pedagogical purpose of facilitating the construction of spaces of commoning.

3 SPATIAL FUNCTIONS: LIBRARIES AS SPATIAL PRACTICE

Historically, libraries have been associated with a certain authority as to the trustworthiness and legitimacy of knowledge (Luke & Kapitzke, 1999). Although popularly still associated primarily with the shelving of books, digitalization has contributed to the transformation of libraries from being mere repositories of knowledge, to becoming "palaces for the people" (Klinenberg, 2018) that provide access to knowledge, social networks, and social capital (Aabø & Audunson, 2012). Today, libraries are less about physically locating authoritative knowledge, and more about (digitally) navigating, situating, and qualifying the plethora of knowledge in informational capitalism, something which is often facilitated through educational programming. This does not mean, however, that the physical space of libraries has become redundant.

As austerity measures in the past decades have hit public service provision in many places around the globe (Pautz & Poulter, 2014), libraries needed to reimagine themselves. In the Netherlands, public libraries became "living rooms" (Messina, 2019), while smaller towns in France—struggling to keep their underfunded libraries open—reconceived them as social and care spaces (Potet, 2015). This rediscovery of the public character of libraries has led library and information scientists to pay attention to the spatial characteristics of libraries (e.g. Elmborg, 2010; Montgomery & Miller, 2011), drawing especially on sociologist Ray Oldenburg's (1999) idea of the "third place." Here, libraries are conceived of as places beyond work and home, creating a sense of community and belonging. Yet, Oldenburg's distinction between place and space is opaque, and does not specifically address libraries. Using coffee shops, beer gardens, or bars as examples for third

places, Oldenburg considers the joyfulness of being together, but fails to consider that, in order to be there, one needs to consume.

Arguably, the "spatial turn" in the social sciences is a fruitful gateway to expand approaches of Oldenburg's conceptualization of spatiality—a consideration that has recently been picked up in the field of radical librarianship (Mattern, 2019; Seale & Mirza, 2019). Thinking of space as being socially constructed is a viewpoint firmly situated in a post-modern, or post-structuralist discourse (Soudias, 2018). Space, here, is broadly conceived of as the relationality between spatiality and human agency. On the one hand, space is the product of agency. But it also shapes our practices and actions, which maintain and reproduce space (e.g. Lefebvre, 2007). This is to say that spaces do not exist in a vacuum: just as they are constrained by the materiality and physical characteristics of the library, they are also defined by the structural conditions of social life. Scholars in the fields of critical geography and urban sociology point out that people act according to intersectional factors such as gender, class, "race" or age "within" and in reaction to space, but also create and modify particular spaces to express their own needs and desires (e.g. Hopkins, 2019).

Making space, then, is a type of practice. From a Bourdieusian (2013) view on practice theory, the spatiality of libraries can be signified as the totality of practices by those actors who e.g. imagine, plan, design, administer, research, teach, clean, maintain, or complain about the library. How these actors "do" practices tells us something about the underlying ontological, epistemological, ethical, and technical principles of their undertaking. Or to put it differently, the kinds of norms and values libraries set for themselves—the ways in which libraries go about their educational programming, lending services, logics of archiving, politics of participation and inclusion, pricing, (anti-)authoritarian interaction with users etc.—structure the spatiality of the library. It is this dialectical relationship that Bourdieu (2013) is referring to when he conceives of social relations as both structuring and structured structures: structuring practices "*within*" space, but also structuring space *through* practices.

This points to the fact that space is inherently pedagogical and experiential, creating "affective atmospheres" (Anderson, 2009) that make users and librarians alike feel e.g. more or less welcome and more or less engaged and belonging. Practicing space, then, is *doing institutions* (Reckwitz, 2016). Here, libraries seem to have a "leap of faith" in the popular imagination. Anthropologist Shannon Mattern (2014) observes that many people think of the library as "a space of openness, egalitarianism and freedom (in multiple senses of the term), within a proprietary, commercial, segregated and surveilled landscape." Against this backdrop, I argue for radicalizing this imaginary in order to conceive of the commoning library.

4 COMMONING FUNCTIONS: LIBRARIES AS FACILITATORS

Since the mid-1980s, what has come to be known as "information commons", foremost in academic libraries in North America and Europe, has highlighted the attempt to provide "a collaborative, conversational space that brings together technology, services, tools, and resources to support teaching and learning and encourage innovative ideas" (Milewicz, 2009, p. 3). Also referred to as "technology commons," "knowledge commons," "digital commons", or "learning commons", the varying appellation chosen for such spaces reflects the shifts in emphasis over time and place. Overall, "commons" in library and information sciences appear to be reduced to the provision of "shared access to the tools, ideas, and instruction needed to perform one's academic work and create new scholarship" (Milewicz, 2009, p. 6).

This rather functionalist definition differs considerably from conceptualizations in radical political theory (Hardt & Negri, 2009), feminist political economy (Caffentzis & Federici, 2014) and more institutionalist theorizations (Bollier & Helfrich, 2019), which all in their own way highlight the potentialities of commoning for providing alternatives to the domination and subordination of the market-state relation. Because commoning is based on prefiguration, "means and ends become, effectively, indistinguishable … in which the form of the action … is itself a model for the change one wishes to bring about" (Graeber, 2009, p. 210). Here, commoning signifies a set of practices that goes beyond the logics of the state and the market and, in its more radical articulations, seeks the construction of "collective spaces created 'outside' of the workings of capital, where different social relations and norms, based upon reciprocity, trust and care—rather than individualism, competition and self-interest—can be nourished" (Cumbers, 2015, p. 63). Spaces of commoning are sustained by a community, where *access* to these spaces must be shared and wide, the *use* of these spaces must be negotiated with agreed-upon rules by a community, the *benefit* from these spaces must be distributed to the community and possibly beyond, and the *care* and *responsibility* for these spaces must be performed by community members (Gibson-Graham et al., 2013).

With the notable exception of Shannon Mattern (2019) and Michael Peter Edson (2017), thinking on commoning and libraries together is an understudied field. A few studies highlight the democratic nature of libraries and their potentially inclusive spatiality (Budd, 2018; Lees, 1997), but they do so in order to further liberal conceptions of "the Public," rather than radical-democratic conceptions of "the Common." In an effort to address this gap, I suggest defining the commons in relation to libraries as shared and collective resources, ideas, and technologies, such as open access contents, open-source code and software, and other freely and openly accessible forms of knowledge. Commoning, then, describes the practices of the shared and self-organized production, acquisition and maintenance of commons.

Consider this mundane, yet relevant, example with regard to state-funded academic libraries: if we think of the process of academic knowledge production, researchers are often publicly funded by taxes. The knowledge they produce in the form of a book, or a research article, oftentimes occurs through library infrastructures, that we have previously identified as information commons. The knowledge they produce by collecting data, reading, analyzing, writing, and talking to their peers and interlocutors, is a practice of commoning knowledge. The final manuscript may be referred to as a commons. When the manuscript is submitted to large publishing houses, the commons is in the process of being commodified. Once published, this article is, more often than not, secured behind paywalls. Academic libraries, in an effort to support their researchers and students, then buy this commodified knowledge via subscription models. In effect, they use public funds to purchase knowledge that has been produced through public funds in the first place. A commoning library seeks to make visible these processes and contest them. In so doing, a commoning library also seeks to challenge ordinary habits of thought of conduct. In the case of such an example, this would mean making the researcher reconsider the potential commodification of the knowledge she produces and instead seek open access outlets for publishing—despite the publishing pressures of the neoliberal university. As such, commoning libraries serve an inherently pedagogical function.

5 PEDAGOGICAL FUNCTIONS: LIBRARIES AS ALTER-NEOLIBERAL PEDAGOGIES

Today, neoliberalism's market-driven discourse can be viewed as a public pedagogy that in many ways defines how we go about our everyday lives. According to Henry Giroux (2004, p. 497), the public pedagogy of neoliberalism "refers to a powerful ensemble of ideological and institutional forces whose aim is to produce competitive, self-interested individuals vying for their own material and ideological gain." The site of this pedagogy is not restricted to schools and universities. "Mediated through unprecedented electronic technologies" (p. 498), a variety of (cultural) institutions, such as social and entertainment media, workplaces, shopping malls, or think tanks, amongst others, contribute to practices and discourses that seek to substitute qualitative (ethical) judgment with quantitative (utility-maximizing) evaluation, and do so in an effort to extend the epistemic logics of the market to non-market phenomena. In consequence, these developments not only economize the ways in which we think about the social, rather, they also depoliticize. As eminent Marxist theorist Raymond Williams (1965, p. 339) remarked over 45 years ago, "the real power of institutions [is], that they actively teach particular ways of feeling, and it is at once evident that we have not nearly enough institutions which practically teach democracy."

The commoning library, I claim, is a space of teaching, learning, and affectively experiencing direct democracy. Here, the commons can be learned and

taught collectively, on a peer-to-peer basis, and—during the process—commons can be created. Indeed, libraries are said to be marked by their "skill in reaching populations that others miss." Despite, or perhaps precisely because of austerity, they "have recently reported record circulation and visitation, despite severe budget cuts, decreased hours and the threatened closure or sale of 'underperforming' branches" (Mattern, 2014). Arguably, as libraries can be conceived of as sites of learning and education beyond formal schooling, they are capable of mobilizing and transgressing their reach, resources, space, discourses, practices and technologies so as to serve the function of what I call an *alter-neoliberal pedagogy*. This requires learning to be based on the acceptance of the factual orderings of neoliberalism, i.e. that they are *constructed*. It also necessitates confrontation with the *normative* nature of these orderings, i.e. that they are value-laden. An alter-neoliberal pedagogy must make the constructed character and the values of neoliberalism visible and explicit and acknowledge that it is itself structured within these realities, so as to be able to prefigure an epistemologically and ontologically alternative vision to neoliberalism. What must be made visible are the opaque ways in which neoliberalism creeps into our everyday conduct by economizing social life through e.g. utilitarian reasoning, quantification, and entrepreneurial practice. In order to provide alternatives, libraries can draw from the rich discussions on "utopian", "militant", "radical", and "feminist" pedagogies, which have, in different ways, highlighted the emancipatory character of egalitarian and anti-authoritarian forms of learning (e.g. Coté et al., 2007; Gounari, 2018; Preece & Griffin, 2005). Additionally, Black radical traditions have underlined the fact that Black spaces are historically structured as spaces of community, knowledge-making, and cultural production that resist racial capitalism by refusing to conform to institutional boundaries (Johnson & Lubin, 2017). In practicing equality and mutual respect, self-governance and direct democratic decision-making, self-organization, and solidarity, libraries can produce affectivities of belonging, self-worth, trust, and collectivity that are antithetical to neoliberal reasoning, the competitive nature of markets, and the authoritarian precepts of the state (Soudias, 2020b). What is pedagogical about these practices and affectivities is that they allow those actors involved to reconsider their ordinary habits of thought and conduct, as they imagine and practice alternatives. At the same time, however, there are institutional limits that need to be addressed so as to further the commons and minimize the reproduction of neoliberal reasoning.

6 INSTITUTIONAL LIMITS: NEOLIBERALISM, CRITIQUE, AND UNWITTING REPRODUCTION

Neoliberalism has been able to survive not least due to how it, almost parasitically, encroaches upon competing worldviews (Plehwe et al., 2020). Today, the initially radical critiques of creativity, autonomy, imagination, sharing, cooperation, openness, and teamwork are increasingly mobilized for the purpose of furthering the capitalist accumulation process, rather than resisting it (Susen, 2014). As

Birkinbine (2020) illustrates to this regard, commons-based peer production and free and open-source software are increasingly being recuperated for profit by corporate firms. At the same time, commercial publishers accumulate capital through so-called "open choice" options, which essentially make digital commons openly available only once authors pay hefty processing charges. These fees are not just financing end-production, but they are also the source of corporate revenues (Fuchs, 2020). More often than not, state-funded open access funds at university libraries are the ones that cover these fees and hence subsidize big publishing.

It is therefore important for libraries to reflect upon the ways in which they themselves partake in the reproduction of particular logics of capital accumulation. To do so, they need to acknowledge their institutional and organizational limitations, so as to be able to actively minimize the dual commodification of knowledge and access to knowledge under informational capitalism. This is because, as Boltanski & Chiapello (2017, p. 29) argue, "the price paid by critique for being listened to, at least in part, is to see some of the values it had mobilized to oppose the form taken by the accumulation process being placed at the service of accumulation." Constituting spaces of commoning, therefore, begins with the acknowledgement that they are only possible with and within that which they are against. To give two examples: libraries produce inequalities due to their hierarchical and often authoritarian organization. In practicing hierarchies, libraries construct spaces that are detrimental to the egalitarian logic of commoning. Librarians ought to try to leverage these limits by acknowledging their existence as constitutive of both the library and their very own individual subject position. Through this acknowledgement, librarians are able to minimize such logics in their everyday labor practices and interactions. I will provide some examples regarding democratic organization in the following section. A second limitation relates to the fact that public funding, and the concomitant budgetary restrictions, are often aligned with market-based or market-derived forms of evaluation. Accountability mechanisms such as new public management (Hood, 1991), and, increasingly, impact management (cf. Huysmans & Oomes, 2013), are used to measure and economize output and performance so as to replace trust with control, judgment with evaluation, and to achieve a "social return on investment." Essentially, this pushes libraries to be organized as quasi-competitive entities, acting "as if" they are in a market situation. In effect, these mechanisms not only undermine the solidarity-based precepts of commoning, but they also further the public pedagogy of neoliberalism.

Such institutional limitations do not allow for libraries to *be commons spaces* properly (cf. Stavrides, 2016). Based on the acknowledgment of institutional limitations, rather than trying to become a commons space, the commoning library seeks to *facilitate the construction of spaces of commoning*. This subtle distinction allows for mobilizing the liminal quality of space. In the conception of anthropologist Victor Turner (2008), liminality signifies the temporary reversal of, or even an expulsion from, the social order; a transitional time in which taken-for-

granted norms, rules and cultural templates of what is conventional, appropriate and justified can be collectively and creatively (re-)negotiated (Schumann & Soudias, 2013). In these out-of-the-ordinary spaces, alternative state-market-subject relations can be imagined and prefigured. This is to say that libraries can facilitate the construction of spaces of commoning, without having to have the authority over their regulation. Within these liminal spaces, knowledge, as well as its production and shape, can be conceived as commons beyond the logics of the state and the market.

True, the COVID-19 pandemic has placed additional limitations on spatializing commoning, as the act of physically coming together has been restricted considerably and is likely to continue for the foreseeable future. Libraries have, however, found ways to adjust their programming by moving some of their activities outdoors (Peterson, 2020). In the spirit of Spivak's (2012) affirmative sabotage outlined earlier, these limitations may make novel forms of reach and visibility possible as libraries now expand their spatiality *beyond* the physical boundaries of their typical physical location. At the same time, libraries have extended their digital and hybrid programming activities, including online information literacy seminars, lectures, edit-a-thons, and serious gaming events. In the next section, I will shed light on the kinds of practices that may be mobilized to assist in constructing spaces of commoning, even against the backdrop of the COVID-19 pandemic.

7 PRACTICES: "DOING" THE COMMONING LIBRARY

Building on the conceptual considerations regarding the spatial, commoning, and pedagogical functions of libraries, this section outlines five sets of practices that may be read as the beginning of a (policy) discussion toward the commoning library.

Democratic Organization: For librarians to facilitate commoning, they themselves ought to reflect upon their conduct in ways that are conducive to "the art of democratic living" (Quan, 2017, p. 174), even under conditions of authority. Against the backdrop of institutional, organizational and hierarchical limitations, how can the everyday librarian labor practices of project planning, decision-making etc. be informed by commoning logics? Anthropological modes of reflexivity (e.g. Brettell, 1993) allow for reflecting upon the intersectional limitations of our subject position, so as to find ways of democratizing how labor tasks and programming are organized within the library. Librarians in superior hierarchical positions may well consider collective ways of allocating tasks, rather than delegating them top-down. This also requires a sense of wariness about discourses on "flat hierarchies", as these often merely camouflage authority. It is on this basis that librarians also democratize the participation with their users: wherever possible, programming should be designed *with* users, rather than *for* users. This radical reconsideration of practices, structures the library as a space that can " 'prefigure' or set the stage for new subjectivities, and by extension, ideally a new society" (Haiven, 2014, p. 75).

Open-Source Infrastructure: Striving to stay technologically relevant is key for modern-day libraries. But, as Mattern (2014) points out, this "can backfire when it means merely responding to the profit-driven innovations of commercial media." The commoning library, therefore, attempts to minimize, wherever possible, the use of proprietary technology. Instead of using commercial integrated library systems, libraries could resort to open-source alternatives, such as Koha or Evergreen, or discovery systems such as VuFind. In making this switch, librarians not only support open-source movements, but, by say, contributing to language versions or (bug) reporting and documentation, librarians themselves take part in the development of open-source software. Such a switch also holds true for other work-flow software and web-based platforms. LibreOffice, instead of Microsoft Office 365; Ubuntu, instead of Windows; Mastodon, instead of Twitter; Matomo, instead of Google Analytics; Nextcloud, instead of Dropbox, BigBlueButton instead of Zoom: these are just a few examples of open-source alternatives to commercial products. Apart from software, we can go one step further: can local Fab Labs or Maker-Spaces help in producing open-source furniture (Souza, 2019) for your library? Or can the production of furniture be integrated into expanding participatory forms of library programming (see below)? It is true that decisions on (software) license agreements are often not made on the local level of library administration. In such instances, concerted efforts of lobbying toward making that change would be the first steps to take locally. In Greece, for example, the Koha Hellenic Users Group is at the forefront of facilitating the transition to the open-source system, which has successfully been implemented at the National Library of Greece. The international network of special libraries of the Goethe-Institut has also switched to Koha and is currently experimenting with the open-source discovery system BOSS in some of its locations. Finally, the recently launched FOLIO ("The Future of Libraries is Open") open-source library service platform is a beacon example for the collective efforts of libraries in the US, Sweden, Germany, the UK, Italy, and Mexico, amongst others, to first lobby for, and finally produce and implement a state-of-the-art community-built platform. This is to say that there are examples of large-scale stakeholders that librarians can draw from as successful examples for furthering their transition effort. Last but not least, the library collection, both physical and digital, should reflect a library's commoning efforts, by a) supporting radical publishers and publishing collectives, b) including media that approach commoning under capitalism, and c) include and promote open access-licensed knowledge forms.

Movement Support: At the same time, commoning libraries can actively support open access initiatives, be it by providing technical support for Open Journal or Monograph Systems, or by partnering with larger stake-holders such as the Public Knowledge Project and publishing coalitions like Libraria or the Radical Open Access Collective. This way, libraries can strategically contribute to a "collective ecology for the Digital Age" (Corsín Jiménez et al., 2015). Beyond these more global efforts, a commoning library supports local initiatives: Peer-to-peer

labs, Maker-Spaces, and especially loose networks of non-institutionalized groups may have needs a commoning library could satisfy. Sometimes, it is as simple as providing the physical space for their activities, or providing server capacity for hosting their digital undertakings. Organizations working at the intersection of science, technology, and society may have archival and repository needs (for their digital commons) for which librarians can provide consultation and infrastructures (think: free and open-source repositories). But it may realistically also include resourceful ways of making public funding or material goods accessible for these organizations by subverting, in Spivak's sense (2012), procurement, donation, and subsidy regulations. There is a cornucopia of potential partners that know more about the commons than librarians do. Cooperation at the peer level is by far the best way forward for libraries to first learn from their partners, and then reimagine themselves as facilitators of spaces of commoning open knowledge.

Commons-based Programming: Information literacy education, broadly defined as a sociotechnical practice of learning information seeking and using skills, is at the heart of modern library programming (e.g. Tuominen et al., 2005). The task of a commoning library would be to tweak information literacy education more strongly toward critiquing the political economy of knowledge production in informational capitalism, while making visible viable alternatives, where knowledge is constructed, accessed, and distributed openly, collectively, and prefiguratively. Regarding its alter-neoliberal pedagogical capacities, critical information literacy programming may focus on the ways in which informational capitalism commodifies user data provided through e.g. social media and search engines, and increasingly privatizes access. At the same time, alter-neoliberal pedagogy should make visible the algorithmic governance and concomitant intersectional biases and filter bubbles that govern the kind of information we receive, not least so as to understand the conditions of possibility for misinformation and post-truth discourses. Christian Fuchs (2020) underlines the need for such an education to be essentially anti-entrepreneurial, so as to minimize techniques of capital accumulation. Instead, users ought to reflect "on the complexities and causes of digital society's problems and understand the roots of digital capitalism's contradictions" (p. 13). A critical information literacy would also point to concrete examples of open-source alternatives to Big Tech. This continues to be relevant against the backdrop of COVID-19: while the pandemic has contributed the expansion of remote learning formats, the education technology industry has been able to both generate profits from this crisis (Williamson et al., 2020) and actively censor critical digital events (Lytvynenko, 2020). These realities signify a new urgency for alter-neoliberal pedagogical interventions through libraries. Lastly, commons-based programming seeks to produce commons through the practice of commoning. Collaborative (rather than competitive) Wikipedia edit-a-thons, hack-a-thons, or collective translation workshops are but a few examples. Increasingly, there are also playful and experiential ways in which the commons can be learned collectively, such as commoning training workshops for youth (Soudias

2020c); board games including Commonspoly, The Free Culture Game, The Game of Open Access, Super-Open Researcher; or the live-action Game of Musical Chairs (Pantazis, 2020).

Commons Licensing: Finally, a commoning library makes sure that whatever knowledge is produced through commoning practices—from text, to video, to object-artifacts—is also licensed in a way that assures open access while also denying commercial uses (Soudias, 2019). In essence, these include Creative Commons Licenses and GNU General Public Licenses. Through this licensing, the access to knowledge is "re-commonified." In sum, these five sets of (policy) practices can serve as a template agenda for beginning to work towards conceiving of the commoning library.

8 CONCLUSION

Against the backdrop of the commodification of knowledge, as well as the commodification of the access to knowledge under informational capitalism, this article delineates the potentialities of libraries for countering these developments by becoming agents of commoning. As predominantly non-commercial spaces, libraries ensure their communities access to knowledge. My analysis radicalizes this mandate and disentangles the ways in which libraries can mobilize, and in so doing, subvert their public and private resources, discourses, policies, and technologies, for the purpose of furthering the commons. This would allow for libraries to assume a dual role of being a bulwark against the commodification of knowledge, while also contributing to the production of freely and openly accessible knowledge. This task is not without pitfalls. I have shown that, due to their institutional limitations, libraries are not capable of fulfilling the function of *being* proper commons spaces, without sacrificing and watering down the very epistemic logics and ethical principles of commoning. A state-funded library trying to *be* a commons, for example, would arguably co-opt the commons just as much as, say, private enterprises in the field of cultural management that fetishize and recuperate the radical aesthetics of the commons for the purpose of maximizing profit. Libraries are, however, capable of *facilitating* the construction of spaces of commoning. The spatial and pedagogical functions of libraries lie at the heart of this consideration. In highlighting the dialectics of space as structuring and structured structures, I have pointed to the kinds of practices and guiding principles that would allow for producing spaces of commoning: equality and mutual respect, self-governance and direct democratic decision-making, self-organization, and solidarity—all of which are principles that do justice to the epistemic logics of commoning. At the same time, they provide a viable alternative to the realities of informational capitalism and the reasoning of neoliberalism. This points to the alter-neoliberal pedagogical character of the commoning library. An alter-neoliberal pedagogy begins with the acknowledgment that it is only possible with and within that which one is against to then collectively imagine and practice epistemological and ontological

alternatives to the neoliberal status quo. In facilitating spaces of commoning, the commoning library provides access to alternative literacies, and to ways of learning and being, which prefigure social life in the "here and now." This allows for reconsidering the relationship between the private, the public, and the commons, particularly with regard to knowledge construction, in ways that hopefully influences our everyday habits of thought and conduct. Based on these considerations, I have abstracted an initial agenda through which the commoning library may be imagined *in practice*. I hope that my analysis reflects the beginning of a larger conversation about both the commoning library and alter-neoliberal pedagogy.

ACKNOWLEDGMENTS

I want to thank all my former colleagues at the Goethe-Institut in Athens for imagining the commoning library with me, especially Christel Mahnke, Natalia Sartori, Nikoletta Stathopoulou, Christine Tzimis, and Frauke Weimar. It was the solidarity amongst colleagues, in light of the perplexing injustices of authority, that renders this experiment all the more worth striving for.

REFERENCES

Aabø, S., & Audunson, R. (2012). Use of library space and the library as place. *Library & Information Science Research,* 34(2), 138-149. doi: 10.1016/j.lisr.2011.06.002

Anderson, B. (2009). Affective atmospheres. *Emotion, Space and Society,* 2(2), 77-81. doi: 10.1016/j.emospa.2009.08.005

Antidrastirio (2018). Autoparousiasi tis omadas vivliothikis 'Antidrastiriou' [Self-Presentation of the 'Antidrastirio' Library Group]. *Antidrastirio*. Available at: https://bit.ly/2KPrglU (Accessed: 5 January 2021).

Aspragathos, N. A. (2013). Commons-Based Science and Research and the Privatization of Its Fruits: The Robotics Paradigm. *Journal of Innovation Economics & Management,* 12(2), 175-197. doi: 10.3917/jie.012.0175

Bernauer, J. W., & Mahon, M. (2005). Michel Foucault's Ethical Imagination. In G. Gutting (Ed.), *The Cambridge Companion to Foucault* (2nd ed., pp. 149-175). Cambridge: Cambridge University Press.

Birkinbine, B. J. (2020). *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software*. London: University of Westminster Press. doi: 10.16997/book39

Bollier, D., & Helfrich, S. (2019). *Free, Fair and Alive. The Insurgent Power of the Commons*. Gabriola: New Society Publishers.

Boltanski, L., & Chiapello, E. (2017). *The New Spirit of Capitalism* (2nd ed.). London: Verso.

Bourdieu, P. (2013). *Outline of a Theory of Practice*. (28th ed.). Cambridge: Cambridge University Press.

Brettell, C., (Ed.). (1993). *When They Read What We Write: The Politics of Ethnography*. Westport: Praeger.

Brown, W. (2015). *Undoing the Demos: Neoliberalism's Stealth Revolution*. New York: Zone Books.

Budd, J. M. (2018). Public Libraries, Political Speech, and the Possibility of a Commons. *Public Library Quarterly*, 38(2), 147-159. doi: 10.1080/01616846.2018.1556232

Caffentzis, G., & Federici, S. (2014). Commons against and beyond capitalism. *Community Development Journal*, 49(1), 92-105. doi: 10.1093/cdj/bsu006

Corsín Jiménez, A., Boyer, D., Hartigan Jr, J., & de la Cadena, M. (2015). Open Access: A Collective Ecology for AAA Publishing in the Digital Age. *Fieldsights*. Available at: https://culanth.org/fieldsights/open-access-a-collective-ecology-for-aaa-publishing-in-the-digital-age (Accessed: 5 January 2021).

Costanza-Chock, S. (2018). Design Justice, A.I., and Escape from the Matrix of Domination. *Journal of Design and Science*. doi: 10.21428/96c8d426

Coté, M., Day, R., & de Peuter, G. (2007). Utopian Pedagogy: Creating Radical Alternatives in the Neoliberal Age. *The Review of Education, Pedagogy, and Cultural Studies,* 29(4), 317-336. doi: 10.1080/10714410701291129

Cumbers, A. (2015). Constructing a global commons in, against and beyond the state. *Space and Polity,* 19 (1), 62-75.

Davies, W. (2014). *The Limits of Neoliberalism. Authority, Sovereignty and the Logic of Competition*. London & Thousand Oaks, CA: Sage.

De Filippi, P., & Said Vieira, M. (2014). The Commodification of Information Commons: The Case of Cloud Computing. *Columbia Science & Technology Law Review,* 16, 102-143.

Duarte, M. E., & Belarde-Lewis, M. (2015). Imagining: Creating Spaces for Indigenous Ontologies. *Cataloging & Classification Quarterly*, 53(5-6), 677-702. doi: 10.1080/01639374.2015.1018396.

Edson, M. P. (2017). Patterns of Commoning: The Virtues of Treating Museums, Libraries and Archives as Commons." *P2P Foundation*, Available at: https://blog.p2pfoundation.net/patterns-of-commoning-the-virtues-of-treating-museums-libraries-and-archives-as-commons/2017/03/27 (Accessed: 5 January 2021).

Elmborg, J. K. (2010). Libraries as the Spaces Between us. Recognizing and Valuing the Third Space. *Reference and User Services Quarterly*, 50(4), 338-350.

Fuchs, C. (2020). The Ethics of the Digital Commons. *Journal of Media Ethics*. doi: 10.1080/23736992.2020.1736077.

Fuchs, C. (2013). Capitalism or information society? The fundamental question of the present structure of society. *European Journal of Social Theory,* 16 (4), 413-434. doi: 10.1177/1368431012461432.

Gibson-Graham, J. K., Cameron, J., & Healy, S. (2013). *Take Back the Economy. An Ethical Guide for Transforming Our Communities*. Minneapolis & London: University of Minnesota Press.

Giroux, H. A. (2004). Public Pedagogy and the Politics of Neo-liberalism: making the political more pedagogical. *Policy Futures in Education,* 2(3&4), 494-503. doi: 10.2304/pfie.2004.2.3.5

Gounari, P. (2018). Discourses of Opposition and Resistance in Education. Alternative Spaces for a Militant Pedagogy." In P. P. Trifonas & S. Jagger (Eds.), *Handbook of Cultural Studies and Education*, (pp. 29-41). New York: Routledge.

Graeber, D. (2009). *Direct Action. An Ethnography*. Edinburgh & Oakland, CA: AK Press.

Gray, J., Bounegru, L., & Venturini, T. (2020). 'Fake news' as infrastructural uncanny. *New Media & Society,* 22(2), 317-341. doi: 10.1177/1461444819856912

Haiven, M. (2014). *Crises of imagination, crises of power. Capitalism, creativity and the commons*. London & New York: Zed Books.

Hardt, M., & Negri, A. (2009). *Commonwealth.* Cambridge, MA: Belknap Press.

Hayek, F. A. (2005). *The Road to Serfdom*. London: The Institute of Economic Affairs.

Hirst, M. (2017). Towards a political economy of fake news. *The Political Economy of Communication,* 5(2), 82-94.

Honey-Rosés, J., Anguelovski, I., Bohigas, J., Chireh, V., Daher, C., Konijnendijk, C., Litt, J., Mawani, V., McCall, M., Orellana, A., Oscilowicz, E., Sánchez, U., Senbel, M., Tan, X., Villagomez, E., Zapata, O., & Nieuwenhuijsen, M. (2020). The impact of COVID-19 on public space: an early review of the emerging questions – design, perceptions and inequities. *Cities & Health,* doi: 10.1080/23748834.2020.1780074

Hood, C. (1991). A Public Management For All Seasons? *Public Administration,* 69(1), 3-19. doi: 10.1111/j.1467-9299.1991.tb00779.x

Hopkins, P. (2019). Social geography I: Intersectionality. *Progress in Human Geography,* 43(5), 937-947. 10.1177/0309132517743677

Huysmans, F., & Oomes, M. (2013). Measuring the public library's societal value: A methodological research program. *IFLA Journal,* 39(2), 168-177. doi: 10.1177/0340035213486412.

Johnson, G. T., & Lubin, A. (Eds.). (2017). *Futures of Black Radicalism*. London & New York: Verso.

Klinenberg, E. (2018). *Palaces for the People: How Social Infrastructure Can Help Fight Inequality, Polarization, and the Decline of Civic Life*. New York: Crown.

Koopman, C. (2019). *How We Became Our Data. A Genealogy of the Informational Person*. Chicago: The University of Chicago Press.

Lees, L. (1997). Ageographia, heterotopia, and Vancouver's new public library. *Environment and Planning D: Society and Space*, 15(3), 321-347. doi: 10.1068/d150321

Lefebvre, H. (2007). *The Production of Space* (2nd ed.). Oxford: Blackwell.

Lucchi, N. (2006). The Supremacy of Techno-Governance: Privatization of Digital Content and Consumer Protection in the Globalized Information Society. *International Journal of Law and Information Technology,* 15(2), 192-225. doi: 10.1093/ijlit/eal010

Luke, A., & Kapitzke, C. (1999). Literacies and libraries: archives and cybraries. *Pedagogy, Culture & Society,* 7(3), 467-491. doi: 10.1080/14681369900200066.

Lytvynenko, J. (2020). Zoom Deleted Events Discussing Zoom "Censorship". *Buzzfeed News*. Available at: https://www.buzzfeednews.com/article/janelytvynenko/zoom-deleted-events-censorship (Accessed: 5 January 2021).

Mattern, S. (2019). Fugitive Libraries *Places Journal*. Available at: https://placesjournal.org/article/fugitive-libraries/ (Accessed: 5 January 2021).

Mattern, S. (2014). Library as Infrastructure. Reading room, social service center, innovation lab. How far can we stretch the public library? *Places Journal*. Available at: https://placesjournal.org/article/library-as-infrastructure/ (Accessed: 5 January 2021).

Messina, R. (2019). A Dutch city gets a new public living room — and so much more. *Frame*. Available at: https://www.frameweb.com/news/mecanoo-lochal-tilburg-netherlands-public-library (Accessed: 5 January 2021).

Milewicz, E. J. (2009). Origin and Development of the Information Commons in Academic Libraries." In C. Forrest & M. Halbert (Eds.), *A Field Guide to the Information Commons* (pp. 3-17). Lanham: Scarecrow Press.

Mirowski, P. (2014). *Never Let a Serious Crisis Go to Waste. How Neoliberalism Survived the Financial Meltdown*. London: Verso.

Moore, T. M. (2017). Trade Secrets and Algorithms as Barriers to Social Justice. *Center for Democracy and Technology*. Available at: https://cdt.org/insights/trade-secrets-and-algorithms-as-barriers-to-social-justice/ (Accessed: 5 January 2021).

Montgomery, S. E., & Miller, J. (2011). The Third Place: The Library as Collaborative and Community Space in a Time of Fiscal Restraint. *College & Undergraduate Libraries,* 18(2-3), 228-238. doi: 10.1080/10691316.2011.577683

Oldenburg, R. (1999). *The Great Good Place: Cafes, Coffee Shops, Bookstores, Bars, Hair Salons and other Hangouts at the Heart of a Community.* Cambridge, MA: Da Capo Press.

Pantazis, A. (2020). Teaching the Commons through the Game of Musical Chairs. *triple C: Communication, Capitalism & Critique,* 18(2), 595-612. doi: 10.31269/triplec.v18i2.1175.

Papadimitropoulos, V. (2020). *The Commons: Economic Alternatives in the Digital Age.* London: University of Westminster Press. doi: 10.16997/book46

Pautz, H., & Poulter, A. (2014). Public libraries in the 'age of austerity': income generation and public library ethos. *Library and Information Research*, 38(117), 20-36. doi: 10.29173/lirg609

Peterson, J. (2020). Thinking Outside: Libraries and Placemaking in Pandemic Times. *WebJunction*. Available at: https://www.webjunction.org/news/webjunction/thinking-outside.html (Accessed: 5 January 2021).

Plehwe, D., Slobodian, Q., & Mirowski, P. (Eds.), (2020). *Nine Lives of Neoliberalism*. London: Verso.

Potet, F. (2015). France's libraries discovering a new lease of life beyond just books. *Guardian*. Available at: https://www.theguardian.com/world/2015/may/02/france-libraries-social-workshops-meeting-hub (Accessed: 5 January 2021).

Preece, J., & Griffin, C. (2005). Radical and feminist pedagogies. In P. Jarvis (Ed.), *The Theory & Practice of Education* (pp. 39-54). Milton Park: Routledge.

Quan, H. L. T. (2017). "It's Hard to Stop Rebels that Time Travel": Democratic Living and the Radical Reimagining of Old Worlds. In G. T. Johnson & A. Lubin (Eds.), *Futures of Black Radicalism* (pp. 173-193). London & New York: Verso.

Reckwitz, A. (2016). *Kreativität und Soziale Praxis* [Creativity and Social Practice]. Bielefeld: Transcript.

Schumann, C., & Soudias, D. (2013). Präsenz und Raum in der Arabischen Revolte. Ägypten im Jahr 2011 [Presence and Space in the Arab Revolt. Egypt in the Year 2011. In C. Ernst & H. Paul (Eds.), *Präsenz und implizites Wissen. Zur Interdependenz zweier Schlüsselbegriffe der Kultur- und Sozialwissenschaften* [Presence and Tacit Knowledge. On the Interdependence of Two Key Terms in Cultural and Social Studies] (pp. 297-315). Bielefeld: Transcript. doi: 10.14361/transcript.9783839419397.297

Seale, M., & Mirza, R. (2019). Speech and Silence: Race, Neoliberalism, and Intellectual Freedom. *Journal of Radical Librarianship,* 5, 41-60.

Selby, M. (2019). *Freedom Libraries: The Untold Story of Libraries for African Americans in the South*. Lanham: Rowman & Littlefield.

Slobodian, Q. (2020). The Law of the Sea of Ignorance: F. A. Hayek, Fritz Machlup, and other Neoliberals Confront the Intellectual Property Problem. In D. Plehwe, Q. Slobodian & P. Mirowski (Eds.), *Nine Lives of Neoliberalism* (pp. 70-91). London & New York: Verso.

Soudias, D. (2020a). Griechenlands COVID-19-Krise und die Ökonomisierung von Sicherheit [Greece's COVID-19 Crisis and the Economization of Security]. *Soziopolis*. Available at: https://www.soziopolis.de/beobachten/gesellschaft/artikel/griechenlands-covid-19-krise-und-die-oekonomisierung-von-sicherheit/ (Accessed: 5 January 2021).

Soudias, D. (2020b). Spatializing Radical Political Imaginaries. Neoliberalism, Crisis, and the Syntagma Square Occupation in Greece. *Contention*, 8(1), 4-27. doi: 10.3167/cont.2020.080103

Soudias, D. (2020c). On the Reopening: Some Initial Ideas on Libraries as Spaces of Commoning. *Goethe-Institut*. Available at: https://www.goethe.de/prj/com/en/21818948.html (Accessed: 5 January 2021).

Soudias, D. (2019). Bauhaus Meets Commons. *Goethe-Institut*. Retrieved from https://www.goethe.de/prj/com/en/21621710.html (Accessed: 5 January 2021).

Soudias, D. (2018). On the Spatiality of Square Occupations. Lessons from Syntagma and Tahrir. In A. Starodub & A. Robinson (Eds.), *Riots and Militant Occupations. Smashing a System, Building a World - A Critical Introduction* (pp. 75-95). London & New York: Roman & Littlefield.

Souza, E. (2019). Open Source Furniture: Download, Print And Build Online. *Archdaily*. Available at: https://www.archdaily.com/914166/open-source-furniture-download-print-and-build-online (Accessed: 5 January 2021).

Spivak, G. (2012). *An Aesthetic Education in the Era of Globalization*. Cambridge, MA & London: Harvard University Press.

Stavrides, S. (2016). *Common Space. The City as Commons*. London: Zed Books.

Susen, S. (2014). Is There Such a Thing as a 'Pragmatic Sociology of Critique'? Reflections on Luc Boltanski's *On Critique*. In S. Susen & B. S. Turner (Eds.), *The Spirit of Luc Boltanski. Essays on the 'Pragmatic Sociology of Critique'* (pp. 173-210). London & New York: Anthem Press.

Tarnoff, B. (2016). The Internet Should Be a Public Good. *Jacobin*. Retrieved from https://www.jacobinmag.com/2016/08/internet-public-dns-privatization-icann-netflix/ (Accessed: 5 January 2021).

Tuominen, K., Savolainen, R., & Talja, S. (2005). Information Literacy as a Sociotechnical Practice. *The Library Quarterly,* 75(3), 329-345.

Turner, V. W. (2008). *The Ritual Process. Structure and Anti-Structure* (2nd ed). New Brunswick & London: AldineTransaction.

Webster, K., & Doyle, A. (2008). Don't Class Me in Antiquities! Giving Voice to Native American Materials. In K. R. Roberto (Ed.), *Radical Cataloging. Essays at the Front* (pp. 189-197). Jefferson, NC: McFarland & Company

Williams, R. (1965). *The Long Revolution* (2nd ed). Harmondsworth: Penguin Books.

Williamson, B., Eynon, R., & Potter, J. (2020). Pandemic politics, pedagogies and practices: digital technologies and distance education during the coronavirus emergency. *Learning, Media and Technology, 45*(2), 107-114. doi: 10.1080/17439884.2020.1761641

Wittel, A. (2013). Counter-commodification: The economy of contribution in the digital commons. *Culture and Organization,* 19(4), 314-331. doi: 10.1080/14759551.2013.827422

Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 1, 2021, 60–87

FIGURING DIGITAL CASCADES: ISSUE FRAMING IN DIGITAL MEDIA ECOSYSTEMS

Nathalie Casemajor* and Sylvain Rocheleau**

ABSTRACT

On November 17, 2015, the newly elected Canadian government led by Justin Trudeau made an announcement that became a turning point in the heated debate around the plan to build the Memorial to the Victims of Communism in Ottawa. The government's decision to scale the project down was massively republished and generated a heavy stream of 2,055 publications and interactions. The virality of such phenomena is sometimes described in the literature as an "information cascade" characterized by a complex and expanding series of media content that is republished, shared, and commented upon in digital public spheres, reaching a growing number of people. Our research aim is twofold. From a theoretical point of view, we combine Entman's cascade model with the perspective of platform studies. From an empirical point of view, we put this model to the test through a case study of the cascading data flows that emerged during this public debate. We found three key factors that constituted and shaped this information cascade: 1) the economic structure of the Canadian media market, and especially the concentration of media ownership, which is notably high in the Canadian media ecosystem; 2) data-exchange mechanisms and algorithmic filtering that drive the process of news aggregation, quickly spreading media content without being a significant source of user engagement; 3) grassroots engagement in diasporic media, which activates micro public spheres around nested interests and political standpoints regarding the public issue.

Keywords: Media ecosystems; information cascade; issue framing; digital public sphere; Canadian media

* Institut national de la recherche scientifique, Canada.
** Université de Sherbrooke, Canada.

1 INTRODUCTION

On November 17, 2015, freshly elected MP Mélanie Joly issued a press release as the new minister of Canadian Heritage. This announcement was a turning point in the heated debate that had been mounting for years around the Memorial to the Victims of Communism, a controversial project planned to be built in the federal capital by the previous Conservative government. The press release announced a reform of the project and was massively republished and commented upon. It engendered a considerable stream of 2,055 publications and interactions over the next five days, spanning news media, aggregators, community media, blogs, and social media.

The virality of such phenomena is sometimes described in the literature as an *information cascade* (Cheng 2014) that appears online and flows quickly and massively through the Web. Digital cascades are characterized by a complex and expanding series of replications of a single news item, which is republished, shared, and commented upon in digital public spheres, reaching a growing number of people. In this article, we are interested in the dissemination of news online as a point of entry to studying the relationship between democratic processes and the diffusion of information in digital public spheres.

We propose to examine the cascade as a figure (as both a metaphor and an analytical tool) for analysis of the cross-platform trajectory of public debates on the Web. What factors shaped the information cascade triggered by the government's announcement regarding the Memorial to the Victims of Communism? How can a cascade analysis be used to grasp the process of issue framing in the context of digital information ecosystems? And, more broadly, what are the opportunities and the limitations of the cascade figure as a heuristic tool? Focusing on the study of data flows, we rely here on the double perspective of media framing and platform studies.

Using a media-monitoring service, we plotted the general shape of the cascade and its various branches spanning different platforms and public spheres. We then selected the three most significant branches of the cascade – mainstream media (newspaper networks), news aggregators, and diasporic media – and conducted in-depth analysis of their dissemination dynamics. Our study follows three threads of analysis: 1) investigation of the network of actors engaged in the public issue under debate (governmental agencies, journalists, grassroots movements, and citizens); 2) a study of the Web platform ecology that shapes, acts on, and is acted on by the cascade (how digital protocols and algorithms connect websites and streamline content); 3) insight on Canadian online public spheres as political landscape and media ecosystem. Taken together, these threads map out the different issue framings activated in the spread of the cascade, the economic structure that shapes media ecosystems, and the presence of data plugs and filter algorithms that play a role in the cascade's formation.

2 FIGURING CASCADES IN ONLINE DATA FLOWS

2.1 A Double Perspective: The Framing Approach and Platform Studies

Digital spaces have been established as privileged sites for the dissemination of media information and public debate. These digital public spheres are increasingly characterized by globalization, polarization, fragmentation, and commercialization (Papacharissi 2002; Brants and van Praag 2017). Today, the propagation of information online raises numerous issues, such as fake news and disinformation, the formation of public opinion, and citizen mobilization.

In the field of media studies, several frameworks have been developed to analyze the spread of information online. In this article, we focus on approaches that tackle the trajectories of information propagation in order to study the spatio-temporal dynamics of information in digital public spheres. We argue that studying information trajectories makes it possible to grasp digital public spheres as a socio-material assemblage not only by tracing a configuration of social relations, as already shown by mass media studies (Katz et al. 1963; Jenkins, Ford and Green 2018) and by the literature on the diffusion of innovation (Rogers 1962; Ma et al. 2014) for analog media, but also by revealing the economic structure of national and transnational media ownership and the material arrangements of the Web.

Therefore, we draw on two main approaches that put forth the analysis of information trajectories in the context of digital public spheres: the "cascading" distribution of media texts (Entman 2003; 2004) and the perspective of media platform studies (Smyrnaios and Rebillard 2019). Although they originate in different theoretical backgrounds and use different methods, these theoretical frameworks offer complementary points of view on our subject: in the former, a model was developed to analyze paths in cascades of information; the latter spearheaded comprehension of the material life of data as it travels through different digital spaces. By articulating these two approaches in our case analysis, we are able to examine the various factors that shape digital content trajectories.

In communication studies, the framing paradigm investigates how media content is produced through the selection of certain aspects of a perceived reality, and how the media dissemination of these frames influences the understanding of an issue (Pan and Kosicki 1993). Entman engaged with this paradigm to explain news framing as a series of collective trajectories that he characterized using the metaphor of the cascade. In his model of a "cascading activation network" of frames (2003, 2004), he describes a flow process occurring within a network of actors in which frames are produced and then propagated. This model postulates a hierarchy of levels that successively activate the transfer of media content, creating top-down circulation trajectories. It portrays a pecking order of different social spaces, each characterized by its own media practices and dynamics; at the top is the governmental administration, then, in descending order, non-administration elites (members of parliament, lobbyists), institutionalized mainstream media, non-

institutionalized news production sites, and members of the public. The model predicates that "although feedback loops exist[s] and each level play[s] some role in diffusing interpretive schemas, in this relatively simple hierarchy, ideas flowed mostly from top to bottom" (Entman and Usher 2018, p. 300). Although Entman's initial model was criticized as reductive in the sense that it is linear, centred on the United States, and does not consider the digital transformation of the media ecosystem (Çeçen 2015), it is still useful for grasping some core structures in the Canadian political and economic media ecosystems, such as horizontal integration, and investigating their impact on the paths for information production and dissemination.

The framing approach gives insight into the sociocognitive and economic logics that govern the production and reception of media texts, but it falls short when we seek to explore other crucial processes at play in the formation of digital cascades. Indeed, the distribution and propagation of media content online is also shaped by the techno-material logics of information networks – that is, the possibilities and constraints of system connectivity and system regulation. In this paper, we enhance the framing approach with an exploration of how power in communication systems also lies in "the emergent non-linear socio-technical systems that channel, block and connect the flows" (Lash 2010, pp. 145–46).

Entman's initial cascade model also failed to take fully into account part of the material-technical dimension of digital networks. To incorporate this dimension into our analysis, we turn to the perspective of platform studies, which has largely contributed to foregrounding the socio-materiality of technical networks in the field of media analysis (Casemajor 2015). This framework investigates how the Web as a socio-material assemblage is shaped not only by physical and software architectures but also by social practices and political and economic interests (Bogost and Montfort 2009). More specifically, platform studies (Gillepsie 2010; Helmond 2015) emphasize how the programmable nature of Web platforms shapes the trajectories of online information by allowing or constraining the circulation of data flows. The literature in this field highlights the role of APIs (application programming interfaces) as "specifications and protocols that determine relations between software and software" (Cramer and Fuller 2008, p. 149). It also underlines the role of social buttons, plugins, and filtering algorithms (Gerlitz and Helmond 2013; Comunello et al. 2016), which operate as data-exchange mechanisms shaping the interconnection between websites and the pattern of information circulation. In the case of social media, these architectural features and technological affordances help to forge what Baym and boyd (2012) identified as a new type of "mediated publicness," in which multi-layered audiences, networked publics (boyd, 2010), or hashtag publics (Bruns et al. 2016) engage in information dissemination. According to van Dijck and Poel (2013), the principles of social media logic – identified as programmability, popularity, connectivity, and datafication – become "increasingly entangled with mass media logic" (2013, p. 2), but the complex connections among different types of platforms are hard to map. They argue that this endeavour

requires a combination of historical-cultural, socio-technical, and techno-commercial perspectives (van Dijck and Poell 2015).

In a recent addition to his cascading model, Entman considered the transformation of the media ecosystem in the context of digital public spheres: with his co-author, Usher, he suggested that an analysis of "new digital 'pump-valves' in the flow of political information and frames" be included (2018, p. 299). The new parameters include social media platforms, aggregators (and other curated portals), algorithmic filters (that select and display content based on set parameters), and bots (automated programs that publish content online). These constitutive features of digital platforms disrupt the news ecosystem that he described in his first version of the cascade model, unsettle the boundaries between institutionalized and non-institutionalized media, and complexify the paths followed by information. However, this revision of the model remains a largely theoretical contribution. There is still a strong need for empirical work to illuminate how digital pump valves shape cascading data flows in practice, even though such work may prove methodologically challenging. Although existing scholarly research on information ecosystems (Sonnac 2013; Svetlana 2019), news virality (Al-Rawi 2019; Heimbach et al. 2015), and platform influence (Pavlovic 2017; Gruzd, 2017) has produced insights into the transformation of media ecosystems, it remains necessary to investigate how the cascade framework can be applied empirically in digital settings.

Our contribution in this article is twofold: from a theoretical point of view, we combine Entman's cascade model with the perspective of platform studies (Plantin et al. 2018); from an empirical point of view, we put this model to the test through a case study of cascading data flows that emerged during the public debate around the Memorial to the Victims of Communism. We argue that following the patterns of online cascading data flows sheds light not only on the socio-cognitive framing of media texts but also on the economic structure of media property and the techno-material features of the Web.

2.2 The Memorial to the Victims of Communism: Case Presentation

The empirical contribution of this article deals with digital political communication and the circulation of news media content online. It is based on an inquiry into the public debate surrounding the Memorial to the Victims of Communism (Ottawa, Canada). The monument was originally planned to be inaugurated in 2015, but construction was delayed due to a heated debate (Casemajor, 2019). The project for the memorial was initiated by the Conservative government of Stephen Harper in 2008, to respond to a request by a community group named Tribute to Liberty. The group is composed of representatives of immigrant communities from various ex-Soviet countries in Eastern Europe (mainly Ukraine, Poland, and Latvia) and from former communist countries in Asia (mainly Vietnam). At the time of our research, Tribute to Liberty was active on the Web through a regularly updated website and a presence on Facebook and Twitter.

The framing of the memorial was contested from the outset. A local newspaper, the *Ottawa Citizen*, extensively covered the issue for several years, conducting in-depths investigations. The National Capital Commission first convened an expert committee that recommended that the theme of the memorial be reframed around the memory of refugees escaping from all totalitarian regimes. This recommendation was opposed by Tribute to Liberty and dismissed by the Conservative government, both of which insisted on targeting solely communism, painting it as an "evil" ideology in all of its forms. The project also sparked local opposition in Ottawa by a coalition of urban planners, architects, and heritage experts, as well as by the Ottawa City Council. Moreover, in 2015, a group of opponents formed a collective named Move the Memorial and launched an online petition to ask for the location of the monument to be changed. The collective did not frame the problem as an ideological issue; rather, it opted for an urbanistic and architectural rationale, focusing on and criticizing the plan to place it in front of the Supreme Court of Canada. Move the Memorial was more loosely structured than Tribute to Liberty: although it did not have a website, it managed a Facebook page, as well as a less active Twitter account.

The issue thus became a local political stake during the 2015 federal election. On October 19, 2015, the Liberal Party, led by Justin Trudeau, won the election, defeating the Conservatives. Whereas the previous Conservative government was strongly supportive of the pro-monument group, the newly elected Liberal government's position was closer to the standpoint of Move the Memorial. Upon taking office, the new minister of Canadian Heritage, Mélanie Joly, set out to revise the memorial project and announced a change in the location of the memorial, a reduction in its budget and size, and rejection of the design chosen by Conservative government. This announcement was widely covered in the media and triggered many public reactions (likes, shares, and so on) and comments on social media platforms. The theme of the memorial was also partially reframed by the new Liberal government: the subtitle "Canada, a Land of Refuge" was added to its name in an effort to broaden the scope of the project, reflecting Trudeau's electoral promise to welcome to Canada Syrian refugees escaping from civil war. At time of writing, the inauguration of the memorial was planned for 2020.

2.3 Methodological Approach

Our data-collection process relied mainly on a news-monitoring method to track and collect Web media productions linked to this debate. Initially focused on the federal election period (May 2015 to December 2015), the corpus was later narrowed down to five specific dates in December 2015 that corresponded to the circulation of one press release that we identified as the root of the main cascading event in our sample. The corpus was gathered automatically through the media-

monitoring service Mention (an RSS feed aggregator)[1] using a series of keywords in English and French.[2] This tool allowed us to collect publications on the main news media outlets' websites (daily press, radio, television, online magazines), on the websites of several public and private organizations, on blogs and forums, and on some social media platforms. The initial data corpus was made up of publications in English and French (press articles, news briefs, press releases, blog posts, tweets, Facebook posts), over a period spanning the ramping up of the election campaign, the election itself, and the transition period that followed the change in government.

For each of the identified publications, the data collected through Mention contain the URL, publication time and date, title, description, username (in the case of social media), and, in the case of retweets, the initial URL that was shared. This information was exported to a spreadsheet and submitted to an initial manual pre-processing (clean-up, error correction). To refine the dataset, we undertook a second collection stage, adding publications that had escaped the Mention collection system. We organized the final dataset into six analysis categories (publications, events, individuals, organizations, themes, and excerpts) and processed it manually through double coding. In order to establish correlations and carry out more advanced analysis, we imported the data into a relational database (MySQL).

Queries by dates, titles, and keywords in the database enabled us to identify the main cascade in the dataset, which appeared as the recurrence of the same news (the government's press release issued on November 17) being shared across different platforms. This series of publications was then isolated as a subsample on which we conducted a third manual data collection to further refine the sample and how it spread over various platforms, gathering a final sample of 2,055 publications and interactions. Mention was not able to systematically collect publications on Facebook due to technical limitations;[3] however, we were able to restore some of the Facebook interactions in the sample by conducting manual searches on the Facebook pages of identified media and organizations. Although Mention captured most of the publications on the main news media outlets' websites, organizations' websites, and blogs and forums (about one third of the sample), all of the interactions on social media (likes, shares, comments) and activity in the comments sections of news media websites were manually collected.

Yet the dataset is still not exhaustive: only the publications using our set of keywords were detected by Mention, and we were able to collect Facebook activity only on the pages of the media outlets and organizations already identified in the sample. The volatility of online content was also an issue, as it prevented in-depth

[1] https://mention.com

[2] The keywords used were: monument aux victimes du communisme, monument to the victims of communism, *Tribute to Liberty*, tributetoliberty.ca, Memorial to the victims of communism.

[3] At the time, the Mention service to which we subscribed was not programmed to collect RSS feeds on Facebook pages (even if it had been, only mentions on public pages would have been collected).

analysis of certain publications, particularly on news aggregator websites that tend to frequently close or modify their pages. The Wayback Machine (Internet Archive) allowed us to access some of these unavailable Web pages.

Combining the query results in the relational database with manual observations on the platforms, we analyzed the sample by identifying, for each instance, media type (see Figure 1 in next section), time of publication (see Figures 1 and 2), publication context (type of website or media outlet, author), relationship to other publications in the sample (position in a cascading pattern), and framing (issues discussed; positive, negative, or neutral tonality – see codebook in appendix). Finally, visualizations were generated to reveal the patterns of cascades (see Figures 3, 4 and 5 in the analysis section). Following Entman and Usher's (2018) model, in the visualizations, we organized the publications into hierarchical levels: press releases, press agencies, institutional websites, news media articles, aggregators, blogs, and social media posts and interactions (likes, shares, comments).

3 ANALYSIS

3.1 Overview of the Cascade

Figure 1 shows that this announcement generated a high volume of online publications and interactions (2,055 over five days). The structure of this informational cascade is composed of various branches all originating from the same source: the government's press conference and press release. These branches are formed by multiple sequences of publications (republication of the government's press release, press releases issued by community organizations in reaction to the announcement, news articles, blog posts) and user interactions (comments, shares, and likes).

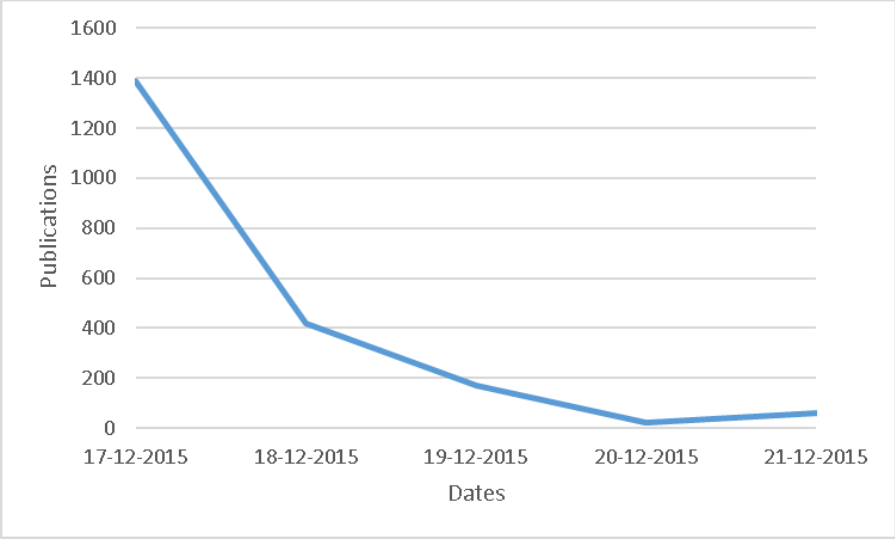

Figure 1. Volume of publications and interactions in the cascade over five days following Min. Joly's announcement (December 17–21, 2015).

Figure 2 shows the distribution of publications and interactions across different types of media and platforms over five days (December 17–21). Within the broad category of mainstream news media, newspapers generated most of the publications (5.9%) with a surge on the fifth day due to an editorial that was widely reproduced in a network of local media. News aggregators generated a smaller share (2.8%) of republications of the government's press release, and some also republished news articles. As to user comments, Facebook posts, likes, and shares form the vast majority of interactions around these publications (51.4%), with comments posted directly on the news media websites (newspapers, TV) holding a smaller but still significant share (20.8%). Lagging behind are discussions on forums (Reddit: 8.5%), posts and interactions on Twitter (7.2%),[4] and reactions to blog posts (1.5%).

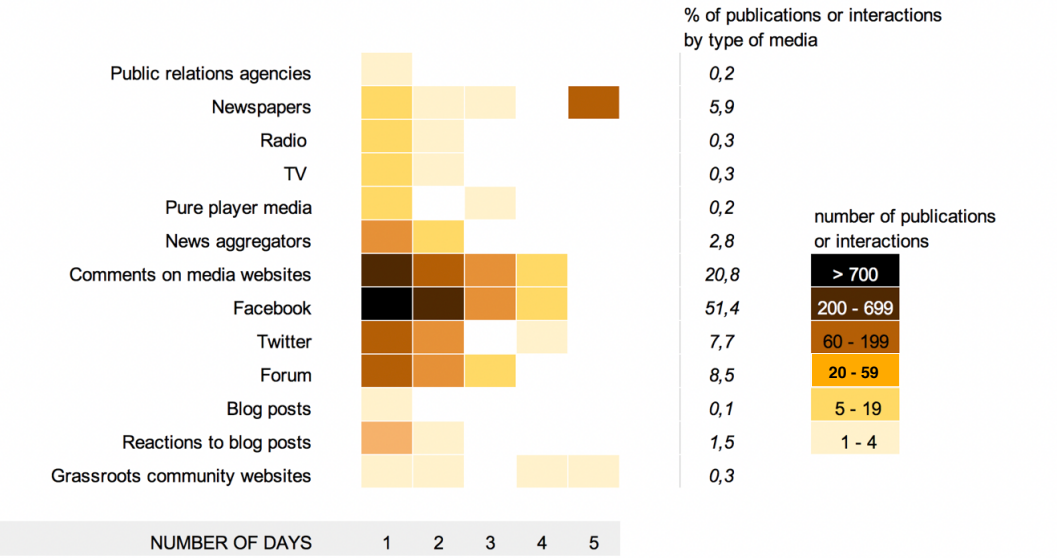

Figure 2: Heatmap distribution of publications and interactions across different types of media over five days (December 17–21, 2015).

We built an inventory of the different branches of the cascade, grouping them into sets by similarities: A) a *mainstream media set* consisting of newspaper articles and TV and radio reports generated by the announcement; most branches in the cascade belong to this set, and several of them are shaped by media concentration; B) an *aggregation set*, composed almost exclusively of publications by press agencies and news aggregators, showing the effects of algorithm-based replication of content, low user engagement, and low degree of relevance for readers; and C) a *grassroots and community media set*, characterized by significant user engagement among the supporters of the memorial. Then we selected for further analysis three branches

[4] A different choice of keywords, such as a combination of "communism" and "#cdnpol" or "#polcan" (for Canadian politics, in English and French) might have returned a higher volume of relevant tweets.

that revealed the most compelling dynamics or the most unusual patterns in each of these sets.

The three branches that we selected differ in several ways: first, in terms of volume of publications and user interactions; second, in terms of their reach down the various media layers; third, in terms of their respective framings of the issue; and fourth, in terms of the types of public spheres they flow through. Below, we provide a detailed analysis of each of these branches based on visualizations that diagram the chronological flows of publications and interactions in each of them, focusing on the most significant dynamics.

3.2 Private Newspaper Network and Horizontal Integration

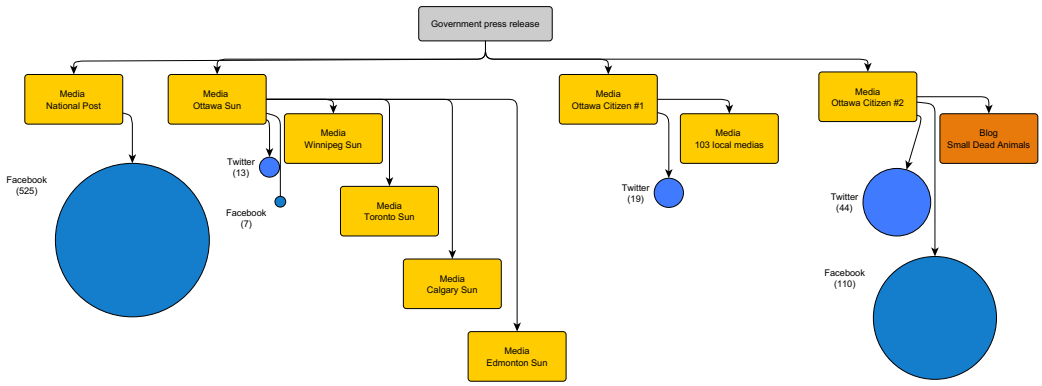

Figure 3. Diagram of a branch of the cascade showing the spread of information in the Postmedia network.

This branch of the mainstream media set in Figure 3 shows the propagation of the government's announcement across a large network of newspapers belonging to a major Canadian media conglomerate named Postmedia Network; each rectangle represents a publication or group of publications and the circles represent user engagement on social media. In this figure, the announcement is propagated in four original articles: one published in a national newspaper (*National Post*), and three published in local newspapers (one in the *Ottawa Sun* and two in the *Ottawa Citizen*). Two of these articles were republished in the network's numerous local newspapers across the country. Particularly striking is the republication of an editorial originally published in the *Ottawa Citizen* in 103 local (including small-town) newspapers. By way of comparison, the *Ottawa Sun* article was republished in four local Sun newspapers based in major Canadian urban centres.

The structure of this branch is heavily shaped by a dynamic of horizontal integration, which characterizes the position of Postmedia Network in the Canadian media ecosystem. Horizontal integration can be described as the acquisition of a company operating at the same level of the value chain in the media business (for instance, a newspaper buying another media outlet such as a radio station). It differs from vertical integration, in which companies expand into upstream or downstream activities (for instance, a newspaper buying a paper mill)

(Martín-Herrán, Sigué and Zaccour 2014). It is a competitive strategy that aims at creating economies of scale, increasing market power over distributors and suppliers, improving product differentiation, and helping media companies expand their market. The downside is that when this strategy succeeds, it is often at the expense of consumers, because it tends to reduce competition, sometimes leading to oligopoly and certainly leading to media concentration (Smyrnaios 2016; Dal Yong Jin 2008).

Headquartered in Toronto, Ontario, Postmedia Network is a fairly new player, established in 2010 through acquisition of the bankrupted CanWest media empire. In 2015, Postmedia purchased from Quebecor Media the English-language operations of Sun Media, Canada's second-largest newspaper chain at the time, with 178 newspapers. That deal made Postmedia the largest newspaper publisher in the country, with close to three times the circulation of Torstar, the second-largest publisher. In a few cities, such as Calgary, Edmonton, and Ottawa, at the time of the study Postmedia owned both the most popular and the second-most popular dailies (Edge 2016). Our findings show that such concentration of media ownership deeply impacts the structure of informational cascades. Figure 3 shows how two articles locally produced in Ottawa newsrooms, concerned mainly with the memorial issue, reached nationwide distribution thanks to republication in Postmedia's extensive network of local media. This branch of the cascade reveals how horizontal integration of media ownership is a compelling factor in the formation of information cascades.

Two other dynamics also contribute to structuring this branch, although to a lesser extent. The first is the engagement of the newspaper's readers on social media, especially Facebook. This occurred both on the national and local levels in Ottawa: an article published on the *National Post*'s Facebook page gathered a considerable number of interactions (525 likes, shares, and comments around the article), whereas the *Ottawa Citizen* gathered a smaller, though still significant, amount of engagement around its first article (110 interactions). The same article published in the *Ottawa Citizen* also attracted a noteworthy number on interactions on Twitter (44) compared to the *Ottawa Sun* (13), as well as a blog post that was commented upon 30 times. The level of engagement around these publications by the *Ottawa Citizen* can be explained by the paper's key role in coverage of the controversy around the monument. One of its journalists was especially committed at the local level to publishing in-depth investigations into the issue. The entire editorial team even committed itself, in an editorial, to praising the government's announcement ("Kudos to the Liberals for moving victims of communism memorial"). Contrary to the strong local resonance of the issue in Ottawa, and on the national level through the *National Post*, there was little to no readership engagement around the republications of the editorial in other local newspapers, showing that the issue had no resonance in other local media across the country.

In terms of framing of the issue, the articles published in all three newspapers were neutral and factual, citing both pro- and anti-memorial opinions, with the

exception of the *Ottawa Citizen* editorial, which was clearly positioned in favour of relocating and downsizing the project. The strong capacity of Postmedia to horizontally republish articles in over 100 local media outlets enabled company management to widely disseminate a particular framing of the issue on a nationwide scale. Another important observation is that the framing of the issue in social media was significantly different from the framing in newspapers. Even when the articles were neutral, the comments that they generated on Facebook and Twitter were predominantly negative regarding the memorial project and raised issues related to public spending and ideology rarely expressed in the newspapers. The predominant opinion on Facebook was that the memorial project should be cancelled in its entirety, because it was seen as useless public spending, irrelevant, or too ideological. The tone of the discussions became clearly acrimonious when it came to opposing Liberal and Conservative views on the project, often leading to heated comparisons of communism, capitalism, and Nazism.

Lastly, despite the strong dominance of anti-memorial framings on Facebook, a wider diversity of opinion could still be observed on this platform, with several users defending the memorial project and criticizing the Liberal government's decision. The situation was quite different in the comments posted on the blog *Small Dead Animals*, which were totally homogeneous in their critique of the Liberal position regarding the monument. Comments on this blog, which defines itself as far-right and adverse to mainstream media, consisted of harsh (and even offensive) critiques of Liberal leaders and communism, several of which reframed the issue around far-right themes such as Islamophobia.

3.3 Aggregators and Algorithm-based Replication

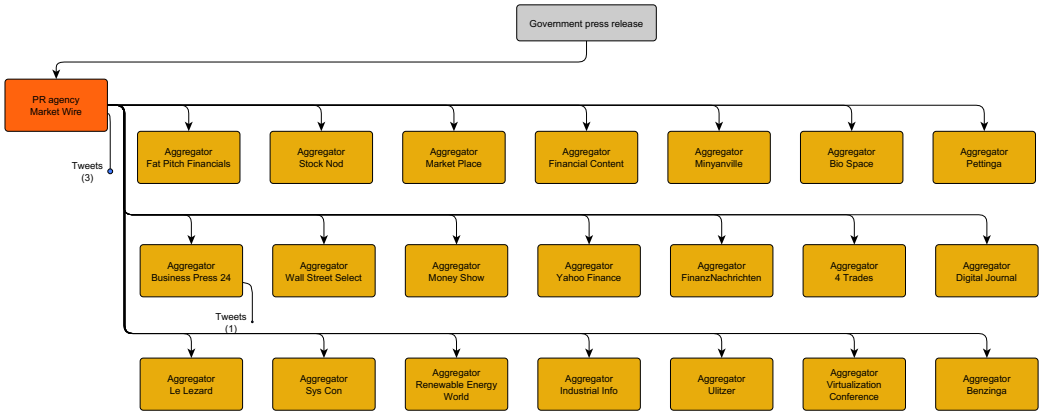

Figure 4. Diagram of a branch of the cascade showing the spread of information in news aggregators.

The branch of the cascade illustrated in Figure 4 is composed of a peculiar trajectory of republications of the press release by 21 news aggregators. This cluster originated in a republication of the press release by Marketwired, a Canadian press-release

distribution service. In this branch, the aggregators republished the press release in its entirety and without comments, a configuration that differed significantly from the other branches of the cascade, in which the press release was analyzed or commented upon by journalists, editorialists, pressure groups, or citizens. According to Tan et al. (2016), it is very rare that an original press release is republished in its entirety in informational cascades, and it "almost never" happens in the case of press releases dealing with politics, which makes the trajectory illustrated above even more unusual. In this branch, the Marketwired website acted as an intermediary hub between the government website and the aggregators. It also acted as a catalyst – a nodal point that multiplies and accelerates the distribution of information on the Web.

What is surprising about this branch is not so much the extensive republication of a press release by several aggregators, but the field of specialization of most of them – finance – which has nothing to do with the content of the press release, dealing with collective memory, monuments, and cultural policy. How can this trajectory, which seems irrelevant both to the public issue and to the aggregators themselves, be explained? Aggregators have become established as key players in the digital content ecosystem over the past two decades (Chyi et al. 2016). They collect information from multiple sources and centralize the display information on their own portal websites. Content producers (news media in particular) criticize their methods of information gathering for being parasitic, especially when they set up clickbait to "pile up pageviews in order to feed a digital advertising-based business model" (Molyneux and Coddington 2019). Yet there are various sets of aggregating practices: some reshape content to add analysis and meaning, whereas others are mere content syndicators that reproduce information produced elsewhere without providing new insight (Coddington 2020). In our dataset, about half the aggregators produce original content on top of syndicating news from other sources. But none provided comments or analysis about this particular press release. They merely reproduced its content with an attribution to Marketwired.

This sequence of republications can be explained by a partnership that Marketwired had at the time with the Nasdaq electronic stock market corporation. Thanks to this partnership, Marketwired services were promoted by Nasdaq to various trading companies. Financial news aggregators heavily republish content related to stock exchanges, including the Nasdaq stock exchange, on which a huge quantity of worldwide major trades take place. According to Lee and Chyi, "news aggregation, the practice of redistributing news content from different established news outlets on a single website, is often based on machine-based algorithms, human judgments, or a mix of both" (2015: 3). Automated aggregation technology relies on Web feeds – data formats that make it possible to collect content from frequently updated sources.

These news feeds operate like data plugs, flowing content from a news source to an aggregator and screening it through a set of filters and keywords. Such feeds

are generally based on the Atom Syndication Format, the RSS (Really Simple Syndication) data standard, or the JSON (JavaScript Object Notation) data standard. For example, several financial aggregators in our dataset are fed by a platform named CloudQuote, which provides APIs supplying "instant access to millions of datapoints in JSON format"[5] from various financial sources. In the case of the branch illustrated in Figure 4, we can postulate that the news-feed algorithms that supply content to the aggregators were programmed to automatically categorize the data points from Marketwired as financial information. The machine-based algorithms act as a type of digital pump valve: by selecting content without the intervention of human judgment, they generate automated republications that shape the flow of information cascades.

A last striking feature of this branch is that it generated almost no engagement on social media. Only four tweets were issued: one was from Marketwired, two mentioned Marketwired, and one was issued by a financial news aggregator promoting its own content. There was no sign of interaction or discussion on the financial news aggregators' platforms or on social media around the republication of the press release by these aggregators. This suggests that in information cascades, the republication of content by news aggregators should not necessarily be interpreted as a sign of attention to and growing popularity of an issue.

To sum up, this branch combines three characteristics that unveil some of the algorithmic and economic underpinnings of digital platforms. First, the digital pump that it exposes is powered by automated scripts that republish content onto news aggregator websites without checking its relevance or adding any extra insight. Second, these data feeds are influenced by corporate deals: indeed, we could find no connection between the press release about the monument and financial information, other than the commercial partnership between the Marketwired PR website and the Nasdaq corporation. Third, being induced mainly by a glitch in the distribution of data flows, this branch of republication generated very little engagement on social media.

[5] https://www.cloudquote.io/ (accessed on March 3, 2020).

3.4 Grassroots Organizations and Diasporic Media

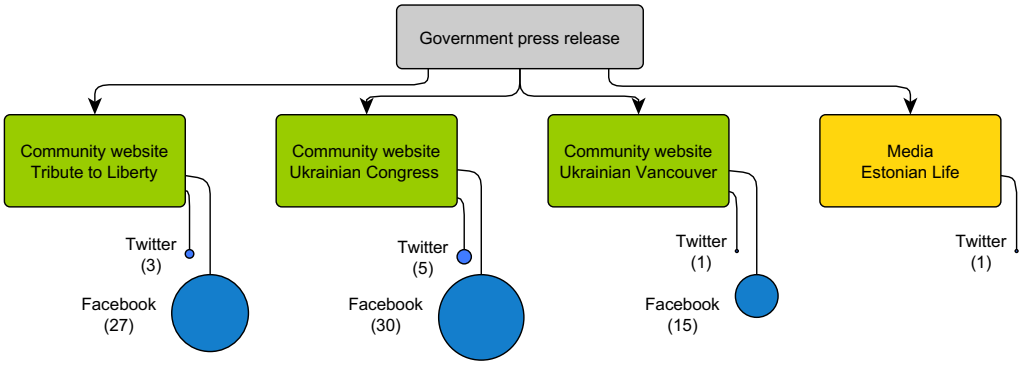

Figure 5. Diagram of a branch of the cascade showing the spread of information in pro-monument grassroots organizations and diasporic media.

Figure 5 presents a branch of the cascade composed of a series of four republications of the press release by grassroots organizations and community media outlets positioned in favour of the memorial. They generated a total of 86 posts and interactions on social media (Twitter and Facebook). The websites in this cluster all belong to Canadian immigrant communities whose members dealt with communist regimes in their country of origin, mostly in Eastern Europe: two of them are grassroots organizations representing the Ukrainian diaspora in Canada (Ukrainian Canadian Congress, Ukrainian Vancouver), one is the organization that initiated the monument project (Tribute to Liberty, with members in various immigrant communities), and one is a daily news website about Estonia and the Estonian communities of Canada (Estonian Life – *Eesti Elu*).

This cluster of websites can be described as a diasporic mediascape (Appadurai, 1996) composed of "particularistic media" – community-oriented media that "complement the role of institutions in charge of the custody and transmission of filiation and memory" for a given group (Dayan 2002, p. 105). In the case of the Memorial to the Victims of Communism, the issue engages both with the national memory of individual diasporic groups (Ukrainians, Estonians) and with a shared experience of living under communist regimes for Eastern European diasporic groups.

The publications in this branch generated 77 reactions on social media, mostly on Facebook. Although the pro-monument groups' websites reached fairly small audiences, the level of engagement from their readers who belong to communities directly concerned with the monument was high compared with publications by major news outlets, with a much larger readership but one that may be less involved with the issue. The Ukrainian diasporic media are especially active in this branch of the cascade and, more broadly, in the citizen mobilization supporting the memorial, the president of Tribute to Liberty being himself of Ukrainian descent.

In terms of framing of the issue, we can observe a discrepancy between the institutional framing of the pro-monument organizations, which was either neutral or positive regarding the government announcement, and the negative framing of some of their supporters on social media. Most of the pro-monument organizations adopted a neutral position regarding the press release: they republished it in its entirety without comment. Tribute to Liberty's president declared to the media that he was satisfied with the new plan for the memorial. But on Tribute to Liberty's Facebook page, about half of the comments posted by followers criticized the Liberal government and its decision to move the memorial to a less prominent site. On the contrary, one of the pro-monument organizations (the Ukrainian Canadian Congress) reframed the government's announcement positively: it issued its own press release, welcoming the government's decision to move forward with the construction of the monument and obscuring its negative consequences (a downgrade in budget and location). It also reframed the resonance of the monument with Canadian values: whereas the government's press release emphasized the liberal themes of openness, welcoming refugees fleeing from oppressive regimes, and the consideration of expert opinion (historians, architects), the Ukrainian Canadian Congress dwelt on the crimes of communism, portrayed as an evil ideology.

In short, this branch of the cascade is characterized by significant engagement by community organizations' readership on social media. It also shows how the framing of the press release changed as it was shared down the different media levels. There were two main reasons for the change in framing. The first was the level of formality of the media: a discrepancy can be observed between the controlled discourse of organizations on their websites and the loose voices of supporters in informal settings such as social media. The second was political positioning, which also affected the framing of the news, as shown in the liberal position of the government and the conservative position of pro-memorial organizations and supporters.

4 FINDINGS AND DISCUSSION

4.1 Key Factors in the Cascade Dynamic

Analysis of the different branches of the cascade reveals three key factors at play in the dynamics of content dissemination: mainstream media ownership, data-exchange and -filtering mechanisms, and grassroots engagement. Our findings show that the most influential dynamic at play in the dissemination of the press release was the structure of mainstream media ownership. This dynamic could be observed particularly in the branch involving Postmedia Network. The newspapers in this horizontally integrated media company produced four articles that cascaded through more than a hundred media outlets, many of them leading newspapers in

their respective local markets, making this branch a good illustration of the impact of media concentration on content diversity. The extent of media concentration in Canada is well documented in the literature (Gasher 2005; Lavigne 2005; George 2015; Amstrong 2016). Recent government deregulation has accentuated this phenomenon even further, making the Canadian media ecosystem one of the most highly concentrated in the world (Winseck 2017). Although our research does not focus on media concentration or media content diversity, our results show that the cascade model is efficient at revealing how a country's media ecosystem is shaped and for evaluating news content diversity within this context.

Data-exchange and -filtering mechanisms are another crucial factor in cascade shaping. Although content replication among the newspapers of a single media conglomerate existed before the Web, it has been accelerated through the use of computers and Internet technologies. On the other hand, algorithmic aggregation, syndication, and filtering are phenomena that could not have emerged without the existence of these technologies. The Marketwired branch shows how content can be rapidly replicated using RSS feeds or data-syndication APIs. Despite the speed advantage of these data-exchange mechanisms, our analysis suggests the limits of their algorithmic filters in terms of content relevancy for their readership. First, the subject of the press release had little to do with the main focus of these finance aggregators; second, as a result of this poor algorithmic filtering, very few people engaged with this content. Nevertheless, the growing efficiency of content-filtering algorithms and the speed at which they can operate is likely to maintain their pivotal role in the shaping of information cascades in coming years.

In contrast to this algorithm-based branch, the grassroots dynamic observed in the cascade is characterized by publications issued by a few organizations closely connected to the issue, which generated a significant number of reactions from their readership on social media.

Despite their different features, these branches, when combined, give us insight into how the information ecosystem has evolved in Canada: it is still driven by mainstream media in terms of audience, content production, and dissemination, but algorithmic-based replication and grassroots media backed by active communities are shaping a new information ecosystem. We believe that these evolutions of the media ecosystem increase the relevance of the cascade as a figure that increases our understanding of how debates evolve in the digital public sphere.

4.2 Cascades Spanning across Plural Media Spheres

Consensus emerging in the public sphere helps to shape public opinion (Habermas 1991). In Habermas's view, consensus is, theoretically, the result of rational discussions about the common interest, during which citizens exchange information and views, sometimes through the media. The Habermasian ideal has been criticized on numerous occasions because this definition of the public sphere refers to the establishment of standards linked to an ideological conception of

society, democracy, and communication (Tremblay 2007). Indeed, disinformation, propaganda, and power struggles are also part of the public sphere. Fraser proposes, instead, a plurality of public spheres that "function as spaces of withdrawal and regroupment" and "as bases and training grounds for agitational activities directed toward wider publics" (2003, p. 68). In this plurality, the media sphere undoubtedly remains the most coveted, as it has a great influence on definition of the issues discussed in public debates – that is, it contributes the most to agenda-setting.

One key finding of our analysis is that cascades can span different digital public spheres (national, local, diasporic) and involve different groups with various interests in setting the agenda. These groups include the Canadian federal government, mainstream media, grassroots organizations, and, to a certain extent, ordinary citizens participating in the debate. Although we identified a branch composed of financial aggregators, we decided not to include them as a group that participated in setting the agenda or shaping the debate. Indeed, the issue of the memorial is completely off target for their readership, and the contribution of aggregators in terms of content is null.

Although the Canadian federal government cannot directly influence media agenda-setting, its public relations effort – a press conference and a press release – is clearly the source of this cascade. So even if the government did not set directly the agenda, it certainly controlled the message on which the other groups had to take a position. Some editorialists congratulated the federal government's decision ("Kudos to the Liberals for Moving Victims of Communism Memorial"), whereas some grassroots groups showed their disappointment and some citizens reaffirmed either their opposition to or support for the project itself.

By taking the lead as the source of the debate, the federal government not only initiated the cascade but also sparked the reactions that emerged in different digital public spheres. This is particularly true in the case of the diasporic media branch, but also in the case of certain online discussions. What materialized is an embryo of a "micro public sphere" (Dahlgren 1994; Dayan 2002), organized around small groups of diasporic media or social media whose readership and framing of the issue differed from "'generalist' media whose messages are conceived for that majority" (Dayan 2002, p. 5). We also observed that although "messages conceived for the majority" – the government press release and mainstream media articles – are often balanced and sometimes neutral, they serve as the base material for far less neutral expressions in micro public spheres.

Of course, the size of a public sphere and its influence on particular issues are best seen as being on a continuum. What appears as "micro" one day can gain momentum later on as certain issues become more popular in the public eye and groups become more organized and efficient at capturing public attention and influencing agenda-setting (Neveu 2011).

4.3 Issue Framings in Digital Cascades

Over the years, the public debate around the Memorial to the Victims of Communism involved a series of successive framings and reframings of the issue by governments, media outlets, and citizen groups. The digital cascade that we studied captured a significant moment in the resolution of this issue. Upon its election, the Liberal government partially reframed the purpose and location of the monument around the idea of Canada's official openness to refugees. The press release that crystallized this interpretation circulated widely in Canadian public spheres. Depending on the type of media and the communities in which it resonated, however, it sparked very mixed reactions. The Liberal government's framing was reproduced verbatim, recontextualized, legitimized, reframed by selecting only a limited aspect of its content, or contested for altering the initial project too much or for not altering it enough.

These reactions can be positioned on a scale from the lowest level of reframing to the highest change of interpretation. Public relations agencies and aggregators lie at the bottom of this scale: they merely reproduced the content of the government announcement.

Mainstream news media outlets are positioned slightly higher than PR agencies on the scale: following established professional journalistic norms, most articles reported the news without taking a position; yet, by giving a dominant voice to the government's announcement, to Liberal party representatives, and to groups opposed to the memorial, they contributed to legitimizing the government's framing. A representative of the main pro-memorial group, Tribute to Liberty, was interviewed in several articles. However, as our results show, he endorsed the Liberal plan in a strategic move to downplay the negative impacts of the announcement on the project. The case of the *Ottawa Citizen* editorial is peculiar, since editorials are freer of the constraints of "frame parity" expected in journalistic practice, in which "two (or more) interpretations receiv[e] something like equal play" (Entman 2003, p. 418). Yet, the editorial strongly supported the Liberal government's decision and unequivocally reinforced its framing. On the journalistic level, Don Butler, investigative journalist for the *Ottawa Citizen*, also played a significant role over the course of the public debate, acting as an intermediary among experts (historians, architects, heritage specialists, urbanists), anti-memorial activists, and the successive – Conservative then Liberal – governments. The editorial was widely disseminated in Postmedia Network but its resonance was limited, judging by the almost complete absence of comments or shares that it generated in social media across Canada.

Pro-memorial organizations stand one degree higher on the scale, as several of them altered the initial framing: by strategically selecting only the positive aspects of the government's announcement, they reframed what was a setback as an achievement. This reframing also hindered the extension of the scope of the memorial to welcoming refugees, because it bore little cultural resonance with the

collective memory of immigrant communities from former communist countries. It may even have acted as a repellent, since, at the time, Eastern European countries such as Hungary and Poland were harshly pushing against taking in new refugees from Syria.

Social media use is positioned at the highest level of the scale in terms of reframing: it was on blogs and on Facebook that we found the most divergent framings, contesting official interpretations, and the most radical points of view. Blog commenters strongly opposed the government's decision, reframing the issue by making connections in crude terms with elements of far-right discourse, such as anti-communism and Islamophobia (a rejection of Justin Trudeau's plea to welcome Syrian refugees to Canada). On Facebook, pro-memorial supporters criticized the government decision in very direct terms, most of them refusing to endorse their leaders' strategic position: rather than focusing on the positive aspects of the announcement, the Facebook comments denounced the Liberals, clearly framing the announcement as a setback. On the mainstream news media's Facebook pages, user comments overwhelmingly supported the government's decision. Yet they framed the issue in a significantly different way than did the news articles: most of the comments redefined it as a matter of worthless public spending, whereas the project costs were only a minor framing in news media stories. Many comments also criticized the ideological bent of the memorial theme (anti-communism), a framing generally ignored by the news media and anti-memorial groups. The latter strategically focused their attacks on a less heated angle, urban planning considerations, which allowed them to stay away from the complex political entanglements of the project that were at the heart of the issue. A majority of comments on the mainstream media Facebook pages favoured a more radical alternative solution to the issue: cancelling the project altogether.

Overall, the main finding of our study with regard to framing in the context of digital cascades is that the more the news drifts away from legitimate scenes of expression (press releases, mainstream news media), the more the official framings are contested. It was in the informal settings of social media (blogs and Facebook in particular) that we found the highest levels of dissent from the dominant framing set by the government, legitimized by the mainstream news media, and partially endorsed by the pro-memorial leaders. Comments on social media contested both the problem definition set by the government and news media and the remedy proposed by the minister of Canadian Heritage.

This finding corroborates Entman's observation that media framings are stratified into hierarchic levels characterized by different social spaces, media practices, and degree of political power. But it also contrasts with his conclusion that divergent framings usually come from elites and news media, shaping public opinion. In the context of our study, these alternative framings came, rather, from the general public's expression of counter-narratives on social media. Entman also suggests that "as we go down the levels, the flow of information becomes less and less thorough, and increasingly limited to the selected highlights, processed through

schemas, and then passed on in ever-cruder form" (2004, p. 12). Studying digital cascades more specifically, Tan et al. showed that as information propagates from press releases to news articles and to shares and comments on social media, "it tends to diverge from the source: while some ideas emphasized in the source fade, others emerge or gain in importance" (2016, p. 1).

What we found in our study is not so much a process of distillation and narrowing of a complex framing into simpler forms, but a complexification of the issue in audience framings. The diversity of problem definitions was higher in social media than in the mainstream news media. In particular, the complex yet central topic of ideology was brought back into the arena of discussion by social media users, whereas it was largely avoided by the government, political elites, urban experts, and news media, which tried to avoid taking a position with regard to the tricky moral judgment concerning communism and anti-communism. Furthermore, our results diverge from Tan et al.'s (2016) conclusion that textual expression of positive sentiment declines at every step down the propagation layer, with positive feedback being lowest at the level of Facebook comments. We found, rather, that positive and negative reception of the press release depended not on the social media layer itself, but on the political, social, and cultural composition of the micro public sphere in which the news propagated: the reception was negative on a far-right blog, and positive among the readers of mainstream news media.

4.4 The Digital Cascade as an Empirical Object

Reviewing our epistemological approach, we proposed to consider the cascade as a figure in the sense that it is a heuristic metaphor (an analytical representation) that combines a numerical description of a phenomenon and its visual representation in the form of a diagram. Based on the calculation of the number of times the same action is repeated (for example, sharing a tweet or republishing a news article online), a cascade-shaped diagram reconstructs the order of a sequence of actions: when and where the publication started and how it spreads in time and space. Cascading figures are built mainly around two parameters: first, the temporal dynamic of the process is depicted by chronological lines of transmission (the origin of the publication is often situated on the top of diagram and its replications are placed in descending order); second, the spatial dynamic shows the topology of the network through which information spreads (for example, different social circles in a single social media outlet or different websites in the case of a cross-platform study).

The big data and behavioural perspectives on digital cascades enable us to inductively map out the trajectories of data flows (Goel et al. 2015), but these perspectives are focused on virality prediction and neglect the broader political and economic context of the media ecosystem and the effects of the platformization of news distribution that shape the flows of news content online. Because we engage with thick data (Latzko-Toth et al. 2017) rather than big data, our approach allows

us to proceed with an inductive mapping of data flows while tracing how these flows are shaped by a configuration of actors' relations, by the influence of media ownership, and by the media-technological affordances of Web platforms. This approach contributes to a type of research design that Marres and Moats characterized as being "as symmetrical as possible in its treatment of media-technological, social, and issue dynamics" (2015, pp. 6–7). The authors suggest that researchers "investigate which effects belong to media technologies, which to the issues, and which to both" (Marres and Moats 2015, p. 6). Yet this distinction between entangled logics may often prove difficult in studies that are focused on one issue or one cascade. A comparative study of different issues, spanning across various media platforms, would be best suited to identifying the specifics of issue effects and media effects.

Finally, the capacity of social media framings to influence the course and resolution of an issue also remains an open question. Compared to the long-term trajectory of an issue over several months or years, the short timespan of our cascade did not allow us to estimate the influence of social media counter-frames on the overall trajectory of the issue. More generally, the choice to focus on an individual digital cascade can be a methodological limitation if the goal of the investigation is to understand the broader framing dynamics of a public issue. Due to Facebook's privacy parameters, we could only include public social media accounts managed by the key groups active in the debate, and not private posts on Facebook discussing the issue, whether or not they contained a direct reference to articles, blog posts, or webpages referenced in our corpus. For this reason, the cascade perspective cannot be envisioned as a holistic cross-platform methodology. It stands, rather, as a complement to other approaches that focus specifically on social media discussions.

Indeed, approaches more focused on social media logics have been able to identify other important features of news virality in relation to platform-specific dynamics. For example, Al-Rawi (2019) studied news- sharing habits on YouTube and Twitter in order to address the cognitive and emotional elements that constitute viral news. His analysis of the 50 most-popular news stories shows significant differences between these two platforms, explained mainly by the variation in sociodemographic characteristics and preferences of audiences on YouTube and Twitter. Considering the entanglement of news websites and mass media logic (van Dijck and Poel 2013), another important issue that remains to be further addressed is the feedback loop dynamic of cross-platform information cascades. In this perspective, Lin (2016) observed a mutual influence between Facebook activity and overall mass media agenda-setting during the 2012 election in Taiwan. He argues that "when a posting on a candidate's page gains sufficient attention, mass media has to cover it" (2016, p. 11); however, the framing of this news is then filtered through journalistic values.

5 CONCLUSION

In this article, we proposed to characterize the cascade as a figure for exploration of the spread of information online. Our approach showed how cascade analysis provides a way to consider both the socio-cognitive framing of media texts and the techno-material features of digital platforms. We found three key factors that shaped the trajectory of the cascade under scrutiny: 1) the economic structure of media property, and especially media property concentration, which is notably high in the Canadian media ecosystem; 2) data-exchange mechanisms and algorithmic filtering that drive the process of news aggregation, quickly spreading content without being a significant source of user engagement; 3) grassroots engagement in diasporic media, which activates micro public spheres around nested interests and political standpoints regarding the public issue. More research needs to be done on the impact of data-exchange mechanisms and algorithmic filtering on the creation of feedback loops between social media and legitimate scenes of expression. Finally, the figure of the cascade is a heuristic tool that illuminates snapshots of significant moments in the unfolding of a public issue online, but the data captured through this approach need to be recontextualized in the long-term trajectory of a public debate.

FUNDING STATEMENT AND ACKNOWLEDGMENTS

This work was supported by the Fonds de recherche du Québec – Société et Culture. The authors would like to acknowledge the research assistants who participated in the review of the literature and data collection – Philippe Lachaine, Rosa Iris Rodriguez Rovira, and Khaoula Zoghlami – as well as Bernard Schütze for his translation and Käthe Roth for her editing.

REFERENCES

Al-Rawi, A. (2019). Viral news on social media. *Digital Journalism*, 7(1), 63–79. https://doi.org/10.1080/21670811.2017.1387062

Baym, N. K., & boyd, d. (2012). Socially mediated publicness: An introduction. *Journal of Broadcasting & Electronic Media*, 56(3), 320–329. DOI: 10.1080/08838151.2012.705200

Bogost, I., & Montfort, N. (2009). Platform studies: Frequently questioned answers. *Digital Arts and Culture 2009*. Available at: https://escholarship.org/uc/item/01r0k9br

boyd, d. (2010). Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In Papacharissi, Z. (ed.) *A Networked Self: Identity, Community, and Culture on Social Network Sites*. New York: Routledge, 39–58.

Brants, K., & van Praag, P. (2017). Beyond media logic. *Journalism Studies*, 18(4), 395–408. DOI: 10.1080/1461670X.2015.1065200

Bruns, A., Moon, B., Paul, A., & Münch, F. (2016). Towards a typology of hashtag publics: A large-scale comparative study of user engagement across trending topics. *Communication Research and Practice* 2(1), 20–46. DOI: 10.1080/22041451.2016.1155328

Casemajor, N. (2019). Brutalist Monuments and Mirror Monuments. In Entrepreneurs du commun (ed.), *Monuments aux victimes de la liberté*. Gatineau, QC: Galerie UQO/AXENÉO7, 23–27.

Casemajor, N. (2015). Digital materialisms: Frameworks for digital media studies. *Westminster Papers in Communication and Culture*, 10(1), 4–17.

Çeçen, A. F. (2015). Revisiting Cascading Activation Model. In *Proceedings of the 13th International Symposium Communication in the Millennium*, 357–371.

Cheng, J., Adamic, L., Dow, P. A., Kleinberg, J. M., & Leskovec, J. (2014). Can cascades be predicted? In *Proceedings of the 23rd International Conference on World Wide Web*. New York: Association for Computing Machinery, 925–936.

Chyi, H. I., Lewis, S. C., & Zheng, N. (2016). Parasite or partner? Coverage of Google News in an era of news aggregation. *Journalism & Mass Communication Quarterly*, 93(4), 789–815. DOI: 10.1177/1077699016629370

Coddington, M. (2020). Gathering evidence of evidence: News aggregation as an epistemological practice. *Journalism*, 21(3), 365–380. DOI: 10.1177/1464884918817608

Comunello, F., Mulargia, S., & Parisi, L. (2016). The 'proper' way to spread ideas through social media: Exploring the affordances and constraints of different social media platforms as perceived by Italian activists. *The Sociological Review*, 64(3), 515–532. DOI: 10.1111/1467-954X.12378

Cramer, F., & Fuller M. (2008). Interface. In Fuller, M. (ed.) *Software Studies: A Lexicon*. Cambridge, MA: MIT Press, 149–152.

Dahlgren, P. (1994). La sphère publique à l'âge des nouveaux médias. *Hermès*, 13–14, 243–262. DOI: 10.4267/2042/15528

Dayan, D. (2002). Particularistic Media and Diasporic Communications. In Curran, J. & Liebes, T. (eds.) *Media, Ritual and Identity*. London and New York: Routledge, 113–123.

Edge, M. (2016). *The News We Deserve: The Transformation of Canada's Media Landscape*. Vancouver: New Star Books.

Entman, R. M. (2003). Cascading activation: Contesting the White House's frame after 9/11. *Political Communication*, 20(4): 415–432. DOI:10.1080/10584600390244176

Entman, R. M. (2004) *Projections of Power: Framing News, Public Opinion, and US Foreign Policy*. Chicago: University of Chicago Press.

Entman, R. M. & Usher, N. (2018). Framing in a fractured democracy: Impacts of digital technology on ideology, power and cascading network activation. *Journal of Communication*, 68(2), 298–308. DOI: 10.1093/ct/jqx019

Fraser, N. (1990). Rethinking the public sphere. A contribution to the critique of actually existing democracy. *Social Text*, 25/26, 56–80. DOI: 10.2307/466240

George, É. (2015). *Concentration des médias, changements technologiques et pluralisme de l'information*. Quebec City: Presses de l'Université Laval.

Gerlitz, C., & Helmond, A. (2013). The like economy: Social buttons and the data-intensive web. *New Media & Society*, 15(8): 1348–1365. DOI: 10.1177/1461444812472322

Goel, S., Anderson, A., Hofman, J., & Watts, D. J. (2015). The structural virality of online diffusion. *Management Science*, 62(1), 180–196. DOI: 10.1287/mnsc.2015.2158

Gruzd, A., Jacobson, J., Mai, P., & Dubois, E. (2018). *The state of social media in Canada 2017*. Toronto: Ryerson University Social Media Lab. DOI: 10.5683/SP/AL8Z6R

Habermas, J. (1991*). The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*. Cambridge, MA: MIT Press.

Heimbach, I., Schiller, B., Strufe, T., & Hinz, O. (2015, August). Content virality on online social networks: Empirical evidence from Twitter, Facebook, and Google+ on German news websites. In *Proceedings of the 26th ACM Conference on Hypertext & Social Media*. New York: Association for Computing Machinery, 39–47.

Helmond, A. (2015). *The Web as Platform: Data Flows in Social Media*. PhD Thesis. University of Amsterdam.

Jenkins, H., Ford, S., & Green, J. (2018). *Spreadable Media: Creating Value and Meaning in a Networked Culture*. New York: NYU Press.

Lash, S. (2010). *Intensive Culture: Social Theory, Religion & Contemporary Capitalism*. Los Angeles: Sage.

Latzko-Toth, G., Bonneau, C., & Millette M. (2017). Small Data, Thick Data: Thickening Strategies for Trace-based Social Media Research. In Sloan, L. & Quan-Haase, A. (eds.) *The Sage Handbook of Social Media Research Methods*. Los Angeles: Sage, 199–214.

Lavigne, A. (2005). Concentration des médias et rapports entre les journalistes, leurs dirigeants et leurs sources apparentées: Exploration d'impacts potentiels. *Les Cahiers du journalisme*, 14, 1–20.

Lee, A. M., & Chyi, H. I. (2015). The rise of online news aggregators: Consumption and competition. *International Journal on Media Management*, 17(1), 3–24. DOI: 10.1080/14241277.2014.997383

Lin, L C.-H. (2016). Convergence in election campaigns: The frame contest between Facebook and mass media. *Convergence*, 22(2), 199–214. DOI: 10.1177/1354856514545706

Ma, L., Sian Lee, C., & Hoe-Lian Goh, D. (2014). Understanding news sharing in social media. *Online Information Review*, 38(5), 598–615. DOI:10.1108/OIR-10-2013-0239

Marres, N., & Moats, D. (2015). Mapping controversies with social media: The case for symmetry. *Social Media + Society*, 1(2), 1–17. DOI:10.1177/2056305115604176

Molyneux, L., & Coddington, M. (2019). Aggregation, clickbait and their effect on perceptions of journalistic credibility and quality. *Journalism Practice*, 1–18. DOI:10.1080/17512786.2019.1628658

Neveu, E. (2011). *Sociologie des mouvements sociaux*. Paris: La Découverte.

Pan, Z., & Kosicki, G. M. (1993). Framing analysis: An approach to news discourse. *Political communication*, 10(1), 55–75.

Pavlovic Rivas, M. (2017). Médias et données: une influence sur la diffusion et la qualité de l'information? *Gestion*, 42(1), 80–81. DOI:10.3917/riges.421.0080

Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293–310.

Sandvig, C. (2013). The Internet as Infrastructure. In Dutton, W. H. (ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press, 86–106.

Skinner, D., Compton, J. R., & Gasher, M. (2005). *Converging Media, Diverging Politics: A Political Economy of News Media in the United States and Canada*. Lanham, MD: Lexington Books.

Smyrnaios, N. (2016). L'effet GAFAM: stratégies et logiques de l'oligopole de l'internet. *Communication & langages*, 2, 61–83.

Smyrnaios, N., & Rebillard, F. (2019). How infomediation platforms took over the news: A longitudinal perspective. *The Political Economy of Communication*, 7(1). Available at: http://www.polecom.org/index.php/polecom/article/view/103

Sonnac, N. (2013). L'écosystème des médias: Les enjeux socioéconomiques d'une interaction entre deux marchés. *Communication*, 32(2). DOI:10.4000/communication.5030

Star, S. L., & Bowker, G. C. (2006). How to infrastructure. In Lievrouw, L. A., & Livingstone, S. (eds.) *Handbook of New Media: Social Shaping and Social Consequences of ICTs*. Los Angeles: Sage, 230–245.

Svetlana, L. U. (2019). Media ecosystem in the projection of technological innovations. *RUDN Journal of Studies in Literature and Journalism*, 24(3), 477–485. DOI:10.22363/2312-9220-2019-24-3-477-485

Tan, C., Friggeri, A. & Adamic, L. (2016). Lost in Propagation? Unfolding News Cycles from the Source. In *Tenth International AAAI Conference on Web and Social Media*. Palo Alto: AAAI Press, 378–387.

Tremblay, G. (2007). Espace public et mutations des industries de la culture et de la communication. In Bouquillion, P., & Combès, Y. (eds.) *Les industries de la communication et de la culture en mutation*. Paris: L'Harmattan, 207–225.

Van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and Communication*, 1(1), 2–14.

Van Dijck, J., & Poell, T. (2015). Social media and the transformation of public space. *Social Media + Society*, 1(2). DOI: 10.1177/2056305115622482

Winseck, D. (2017). *The Growth of the Network Media Economy in Canada, 1984-2016. The State of the Digital Media and Internet Industries in Canada*. Canadian Media Concentration Research Project (CMCRP)

APPENDIX

Table 1: Codebook used for content analysis of the publications in the corpus

Publication URL
URL of other mentioned publication If the publication mentions or links to the press release, an article, a tweet, or another publication reference in the corpus (cf. sign of a cascading pattern).
Title Or first words in the case of a social media publication.
Date of publication
Type of publication Press release; press agency publication; page on an institutional website (e.g., grassroots community website); news media article (newspaper, TV, radio, pure player website); comment on news media website; aggregator publication; blog post or reaction (comment) to the post; forum post or reaction (comment) to the post; Facebook post, like, share, or comment; tweet, like, share, or comment on Twitter.
Context of publication Description of the website in terms of mission, functionalities, political orientation (if applicable), ownership.
Author Name, affiliation with an organization (if relevant), other relevant information relative to the issue.
Framing > Issues discussed: monument design; monument funding; monument governance; diasporic issues; monument name and scope; urban planning (location of the monument); other > Tonality: positive (cheerful tone, vocabulary of praise – e.g., "kudos," congratulations, expression of satisfaction, optimism); negative (critical tone, disapproval vocabulary, expression of disappointment, accusations, insults); neutral (factual account of the events, balance in citing both positive and negative points of view or absence of comments, neither praise nor critical tone or vocabulary).
Excerpts Most significative passages in relation to the framings.

JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 1, 2021, 88–105

DATA PERVERSION: A PSYCHOANALYTIC PERSPECTIVE ON DATAFICATION

Jacob Johanssen*

ABSTRACT

This article adopts a psychoanalytic perspective and argues that users are in a perverse relationship with contemporary platforms. Following a review of recent critical scholarship on datafication, which places too much emphasis on platforms and situates users as helpless, the psychoanalytic concept of perversion is introduced. Perversion describes a relationship that is characterised by dominance, exploitation and dehumanization as well as care, love, and idealization. While the pervert (the platform and its owners and developers) is the perpetrator, the other (the user) is also actively participating in the perverse relationship. Contemporary relations are thus marked by foregrounding connectivity, convenience and communication which mask the violence of datafication. Such relations are upheld, because users affirmatively reproduce them by using highly attractive platforms which are customized for each individual. Psychoanalysis can thus offer a complex conceptualisation of the interplay between affirmation, attraction and exploitation that is immanent to platforms and users today.

Keywords: Datafication; platforms; users; psychoanalysis; perversion

* St. Mary's University, United Kingdom

1 INTRODUCTION

The term 'datafication', and associated terms like 'big data analytics,' has acquired important meaning in recent years. This is due to the influence of algorithms on digital data, as well as computers' increased capacity to collect, store, and analyse large datasets (Kennedy, 2016; Lupton, 2019). For this article, datafication is defined as both a description of as well as the effort and mechanism itself through which to gather, extract, process and analyse large amounts of (digital) data or to create such data in the first place through conversion of other analogue data into the digital format. Those data are frequently made up of various smaller data and turned into large datasets which are often automatically analysed. The purpose of creating large datasets is often commercial and datafication has become a far-reaching process that reconfigures the social world itself (Couldry & Mejias, 2019a, b). Nick Couldry and Ulises A. Mejias argue that datafication can be understood as something that transforms human life itself and makes it a continual data source (2019a, b). While datafication takes many forms and has consequences for different sectors, this article specifically takes the transformation of human life caused by datafication, for instance in how platforms are used, as a starting point in order to inquire into the relationship between humans as users and processes of datafication (on and by platforms) that they both actively contribute to and are confronted with. It thereby makes a contribution to theoretical debates.

Datafication has various implications for users online, their data and how they are constructed and constituted through them as data subjects and profiles by companies, governments and others (Cheney-Lippold, 2017). It is often inherently tied to commercial aspects. Datasets are sold by companies to other companies. Such processes promise results that show objectively and rationally coded data that corresponds to real individuals, decisions and content online. Yet, any form of data mining involves a complex interplay of decisions made automatically by algorithms as well as un/conscious decisions by humans before, during, and after the data have been created, analysed or visualised. This not only has implications for how we see datafication, but also for how questions of subjectivity inform it. Datafication is also widely discussed in relation to discrimination, for instance when it comes to biased algorithms (Sandvig et al, 2016; Cheney-Lippold, 2017; Chun, 2018; Noble, 2018).

Datafication as the attempt to turn everything into data has implications for how we think about subjectivity and how individuals experience an atmosphere of complete datafication. Rather than writing about datafication per se, this article specifically theorises datafication on commercial platforms like Facebook, Twitter, Uber, Amazon, or Netflix. Those platforms depend on user data which guarantee a functioning of the platforms (i.e. users, who use them, create data) as well as on

collecting and analysing user data, often done for commercial purposes (Fuchs, 2014).[1]

This article makes the argument that the relationship between users and contemporary platforms is a perverse relationship. Perversion is often more commonly linked to sexual deviance, sexual fetishes and sexualities that go against norms and laws, but it is a clinical-psychoanalytic concept that is far more wide-ranging and complex. Drawing on the psychoanalytic concept of perversion, it is argued that users are simultaneously loved and abused, humanized and dehumanized, by platforms, or rather the developers and owners of them, today. This occurs through datafication processes that ultimately aim at analysing everything about human beings. Such processes are masked by the alleged purposes of platforms: to entertain, inform, connect, or provide commodities for purchase. At the same time, perversion entails that the other who is exploited by the pervert willingly participates in the relationship, because they feel loved, cared for and part of an exciting pact (Stein, 2005). Rather than merely an act of one-sided exploitation, domination or colonialism (as some scholars argue, see the next section), datafication is made possible through a relationship in which both 'partners' are active. The perverse relationship of users and platforms thus comes into being via and on those platforms, for example when an individual uses Facebook or Instagram. I do not mean to argue that platforms themselves have a soul, or similar characteristics to human beings. Instead, they serve as spaces where particular psychodynamics come into play which are shaped by platform owners, developers and users.

This article makes a contribution to the growing area of studies on digital media that draws on psychoanalysis (Turkle, 2011; Balick, 2014; Clough, 2018; Johanssen, 2019; Pinchevski, 2019; Singh, 2019). Psychoanalysis, and its specific concepts, allows for a complex perspective on particular phenomena because it places an emphasis on relational dynamics between subjects that are situated between consciousness and the unconscious. Such a perspective can further enrich studies of datafication that frequently grapple with the intersections of the un/known and in/visible, for instance, of algorithms (Bucher, 2018) or platform policies (Gillespie, 2018). I argue that commercial platforms enable a particular relation that users enter into. Some feelings, experiences and thoughts within this relation are unconscious for users, but nonetheless decisively shape it.

Additionally, in foregrounding the psychoanalytic concept of perversion, a prism is opened up that allows to transcend binary perspectives on datafication, and by extension networked media more broadly, that either show platforms as completely exploitative and dangerous, or as being harmless tools that users draw

[1] The term 'platforms' is used here as an umbrella term to include social media, like Facebook or Instagram, as well as apps such as Uber, ecommerce platforms like Amazon, or streaming platforms like Spotify. While they may have varying business models, all are commercial platforms that depend on user data. They 'are digital infrastructures that enable two or more people to connect.' (Srnicek, 2017, p. 43).

on in their everyday lives. It is psychoanalysis that makes space for contradictory modes of experience in which, for instance, feelings of hatred and love are often messily intertwined and un/consciously motivated (Johanssen, 2019).

2 PERSPECTIVES ON DATAFICATION

By and large, structural social theories (theories that emphasise social-structural rather than individual-subjective dimensions of a phenomenon) have sought to define and analyse the current conjuncture of big data by arguing that we are in the age of 'data colonialism' (Couldry & Mejias, 2019a, b), 'data capitalism' (West, 2017), 'surveillance capitalism' (Zuboff, 2019), 'big data capitalism' (Fuchs 2019) or 'platform capitalism' (Srnicek, 2017).

Many scholars are critical of datafication because it amounts to surveillance. The purpose of datafication on social media for example is primarily to be able to sell certain user data to enable targeted advertising (Fuchs, 2014). Data mining practices are 'discriminatory by design' (Kennedy, 2016, p. 48). Data mining involves the structuring of individual data profiles whereby they are classified according to criteria and often marked as more or less valuable. The precise criteria according to which such data mining occurs are unknown to the general public and, in fact, carefully hidden by its creators and users (Gillespie, 2014; Mosco, 2014). A famous exponent of such a position is Shoshana Zuboff and her arguments on 'surveillance capitalism'. She defines it as 'constituted by unexpected and often illegible mechanisms of extraction, commodification, and control that effectively exile persons from their own behavior while producing new markets of behavioral prediction and modification.' (Zuboff, 2015, p. 75). User data are 'hunted aggressively, procured, and accumulated—largely through unilateral operations designed to evade individual awareness and thus bypass individual decision rights—operations that are therefore best summarized as "surveillance."' (Zuboff, 2019, online). This extends to the active shaping of user actions, she argues. Rather than merely predicting them through data analytics, companies have turned to actively modify user behaviour so that it 'reliably, definitively, and certainly leads to predicted commercial results' (2019, online). The goal, as Zuboff puts it, is to automate and control humans and human behaviour itself.

Couldry and Mejias (2019a, b) make similar arguments as Zuboff when it comes to surveillance in the datafied society. They use the term colonialism not in the metaphorical but in the literal sense to analyse the impacts of datafication. For them, data colonialism refers to 'something [that] is taken from things and processes, something which was not already there in discrete form before.' (Couldry & Mejias, 2019b, p. 2). This means that humans have become the raw material that can be appropriated via datafication.

Like traditional colonialism, which expropriates both territories and humans, under data colonialism humans are exploited and appropriated without much ability to resist. Data colonialism occurs through social relations in which human data are

extracted and appropriated from humans with the aim of profit maximization (Couldry & Mejias, 2019a). Such relations are termed 'data relations' by Couldry and Mejias (Couldry & Mejias, 2019a, p. 27). In short, humans exist to be conquered and used as far as the viewpoint of platforms goes. Practices of data colonialism know no limit; they are about constant exploration, expansion, extraction, exploitation, and extermination in relation to human data (2019a, pp. 91-108). Luke Munn's (2019) argument in relation to Uber illustrates this. He writes that Uber behaves like an imperial power that is primarily interested in growing its user base by conquering cities across the world. Profit is secondary, what matters is user growth (Munn, 2019). In our world, everything and everyone become datafied and part of data relations.

In their book, Couldry and Mejias specifically focus on the human subject whose data are colonised (2019a, chapter 5). They argue that data colonialism fundamentally threatens human autonomy in relation to the social world. Individuals become mere entities 'plugged into an external system' (2019, p. 164). This results in the very understanding of the self that individuals hold being disrupted and undone. There is a contradiction between how the individual sees their own complex identity and how it is mirrored and thrown back at them through datafication (Johanssen, 2019). The datafied self no longer has any space of their own and their freedom is limited. The notion of data relations is particularly useful and can be enriched by putting forward that those relations often take particularly perverse forms.

Antoinette Rouvroy (2013) has similarly argued that data mining and algorithm-based profiling ignore the embodied self behind a user's data and instead construct a dichotomy between them and a statistical subject. For corporations, 'the subjective singularities of individuals, their personal psychological motivations or intentions do not matter.' (Rouvroy, 2013, p. 157). Human experience is reduced to 'measurable observable behavior' (Zuboff, 2019, online), as Zuboff notes.

What all of the above accounts have in common is that they situate datafication (and related processes) as something exterior to humans; as (automated or manually executed) processes that affect humans from the outside. Human subjects lack the knowledge, means, or power to adequately resist such practices they are faced with. Datafication refers to something that is done to them. While from a structural perspective such arguments may have some truth in them, I argue that they are too simplistic and one-sided. Datafication in the form of surveillance may take such forms where an external power spies on individuals or collects their data without their consent, as for instance revealed by Edward Snowden or the Cambridge Analytica scandal. Additionally, datafication also takes the form of corporate surveillance where (often low-paid) workers are continuously tracked. However, such instances are extreme forms of datafication. The scholars named above fail to account for the complexities that are inherent to mundane, everyday datafication. In the logic of the above accounts (a review that is by no means exhaustive), humans are confronted with big, anonymous powers like Google,

Facebook, Tencent, or governments and they cannot help but have their data extracted, analysed and used for purposes they do not fully understand or consent to. Such scholarship points to definitions of datafication and our current conjuncture in which users' behaviour is accessed and monitored (Van Dijck, 2014, p. 1478). Users are frequently discussed in passive terms and their data are seen as being collected and monetized rather than taking into account that it is users who produce and create their data in the first place. Datafication is not only something that is done to users, but they actively participate in such relations as well. Such critical perspectives on platform power are important. I want to take them as a starting point and think further about the active role that users assume. I do not think that terms like 'data colonialism' or 'surveillance capitalism' capture the full complexity at the heart of platforms and their users.

Christian Fuchs (e.g. 2014) has incorporated a more active position in his work on digital labour when he argues that users actually work for free when they use commercial social media and create data which is, secondly, used for targeted advertising and other means of profit maximization by social media companies (see also Jarrett, 2016).[2] For the most part, however, critical scholarship on such questions renders users passive and helpless. Such a perspective fails to account for the triadic relationship of users, data, and platforms in which users play an active and often highly voluntary part. While I agree with the critical stance on datafication that the above scholars adopt, I argue that a psychoanalytic perspective which takes account of the contradictory dimensions of such a relationship can enrich critical works like the ones discussed in this section. Users often want and *desire* datafication and wider surrounding dynamics. They wilfully enter into particular data relationships. The relationship is specifically a perverse one. Conceptualising it as perverse also allows an analysis of the ideology of tech companies which are seemingly about care, user empowerment and communication.

Conceptualising datafication as a relation, and not as an obscure force, omnipotent power, or one-sided process is helpful for taking account of both the users and the platforms that are responsible for datafication (behind which are of course other humans). The conceptualisation of a perverse relation also allows for critical as well as positive dimensions to be analysed in such a relation. Perversion in this context is not meant in a pathologizing way, or used to blame users for being allegedly sexually perverted, sick or stupid. As I discuss below, perversion functions in a relationship in which both parties are active participants.

[2] Deborah Lupton presents an exception and has put forward the notion of 'data selves' (Lupton, 2019) by which she means an intertwinement of human bodies and more-than human phenomena which takes specific account of human agency.

3 PERVERSION AS A CLINICAL CONCEPT

As briefly mentioned, perversion is more commonly associated with sexual practices. The quintessential practice of the perverse in adult sexuality is often named as BDSM: sado-masochism, dominance and submission, or bondage and discipline. Dynamics in which mainstream sexual norms and practices are often changed, reversed, or altered. BDSM, under explicit attention to consent, plays with pleasure and pain, humiliation and degradation, as well as meticulous care, love and idealization. It usually functions along a binary power dynamic where one partner takes the dominant part and the other the submissive part. One gives up all power and agency and hands it to the other. Such dynamics can be thrilling, sexually arousing and liberating for those who practice them (Weiss, 2011; Simula, 2019). 'Perversion is thus not only polymorphous sexual anarchy, but also a powerful means of expressing hostility and hatred' (Stein, 2005, p. 780) through care and love. Within the sexual realm, this is not necessarily problematic for as long as perversion is practiced by consenting adults.

I argue that there is a particular perverse dimension to datafication as it occurs on commercial platforms: a perverse double bind that simultaneously treasures users and exploits their data, cherishes them as subjects and abuses them as objects. Danielle Knafo and Rocco Lo Bosco (2017) have recently written about perversion as a phenomenon in the contemporary age. On a basic level, perversion points to a relationship between individuals (often a dyadic one, for instance in couples) that is fundamentally structured by love and care as well as exploitation, humiliation and destruction. It is a concept which has been conceptualised differently by clinicians (Knafo & Lo Bosco, 2017). Perversion, for many psychoanalysts including Freud, is at the core of sexuality but moves outwards to penetrate all spheres of society and human relationships. For Freud, sexuality is in itself inherently perverse, because it is initially outside of any social norms or particular prohibitions. For the young infant, sexual stimuli can be found in any object and any part of the body. Sexuality only becomes particularly codified and associated with specific pleasures, erogenous zones, sexual orientations, etc. as the individual grows up (Freud, 1981).

It may already become apparent at this stage, that similar dialectical relations can exist when we consider corporate platforms, such as Instagram or Facebook, that are grounded in both exploitation of and love for users on the part of the platform owners, and simultaneous feelings of degradation and intense validation on the part of the users.

Perversion becomes particularly problematic however when it is pathologically and universally used to mask exploitation and destruction through feelings of love, care and (self)-discovery. For that reason, perversion beyond its sexual-consensual imperatives is of particular interest to psychoanalysts. For instance, when they see patients who are in perverse relationships. Such relationships can be deeply destructive and dangerous, in particular for the one who is ab/used by the pervert (Bach, 1994) and yet patients often report great difficulty

in getting out of the relationship because they feel so deeply entranced by and intertwined with the pervert (for case study discussions see e.g. Baker, 1994; Stein, 2005; Celenza, 2014). It is this form of pathological perversion that I take to be similarly present in (data) relations that are enacted by platforms and individuals.

Danielle Knafo and Rocco Lo Bosco name six characteristics that unite different psychoanalytic discussions of perversion. Perversion is universal; it functions across a spectrum of varying degrees; it may relate to trauma and loss which is disavowed and masked through perversion; it may feature sado-masochistic dynamics in relationships; it features experiences of excitement, mastery and illusion; and it is expressed differently by men and women (Knafo & Lo Bosco, 2017, pp. 52-54).

The British object-relations tradition within psychoanalysis in particular has stressed that perversion takes place in relationships. The perverse relationship is often one that comes about because of seduction, enmeshment, intertwinement, or a kind of stumbling movement in which one partner finds themself at the mercy of another while simultaneously desiring and seemingly needing just that (Stein, 2005).

The perverse subject, or pervert, regards the other in a relationship as an object. They are treated with hatred, cruelty and humiliation (Bach, 1994; Stein, 2005). At the same time, a perverse relationship resembles one of recognition and care while those attributes are in reality betrayed (Stein, 2005, pp. 780-781). A perverse relationship constitutes the creation of a singular world that shuts out reality and external influences. New rules for and in the relationship are created. Perversion is thus often an attempt to ignore, subvert or actively go against the law. The pervert's object – whether it be a real person or a physical object - is (ab)used and manipulated while at the same time being idealized and cherished (Khan, 1979; Celenza, 2014).

This article unfolds the theoretical argument that a similar dynamic is at play in the relationship between many contemporary platforms and their users. Under the guise of communication and connection, Facebook for example lures its users into a relationship that is in reality based on exploitation. Users are addressed as unique individuals who are encouraged to express themselves online through the various functions of the platforms and yet they consent (whether to their knowledge or not) to being sold as data profiles to advertisers. This double mechanism with which Facebook, and other platforms, binds users has perverse tendencies. The psychoanalyst Masut Khan argued that the pervert's object resides in a space between her and the other, between fantasy and reality. Therefore, it can be 'invented, manipulated, used and abused, ravaged and discarded, cherished and idealized, symbiotically identified with and deanimated all at once' (Khan, 1979, p. 26). This in-between space at the intersections of user and platform symbolises the rupture between a sense of who users think they are and who they are in the eyes of Google, Facebook, Twitter, Weibo, Netflix, Uber and others. Users are loved and instrumentally used at the same time. Theorising this relationship as one of

perversion opens up a unique perspective through which to analyse it. It places an emphasis on the dynamics between users and platforms, rather than just on platforms themselves. This psychoanalytic perspective opens up an angle that foregrounds ambivalence, contradiction and a love-hate relationship that is at the heart of profit-driven 'data relations' (Couldry & Mejias, 2019a, p. 27) today. Users are often very aware of the exploitative relationship they are in, but feel unable to leave a platform (Karppi 2018). It is this psychodynamic of knowing particular negative aspects of a commercial platform, but of also un/consciously feeling loved and cared for by a platform's structure that can be explored further through psychoanalysis.

4 DATA PERVERSION IN THE PLATFORM

The key characteristics that Couldry and Mejias (2019a) isolate when it comes to data colonialism – the ever-expanding practices of wanting to own, use, and analyse as much user data as possible – point to desires of omnipotence and mastery on the part of the tech companies that we similarly find on the part of the pervert in the perverse relationship. They want to own and manipulate the other at any cost. This works through practices of how such platforms address users as individual subjects, as I outline further in the next section. On the surface, platforms like Facebook, or Netflix are about particular services (communication, maintaining friendships, streaming series and films). They are convenient, easy to use, and popular. Such platforms depend on the collection, tracking and analysis of user data (Kennedy, 2016). 'But there is nothing comforting about this. Even though the new social knowledge is produced through operations that bypass human beings, it is actual human beings, not "doubles," who are tethered to the discriminations that such knowledge generates.' (Couldry & Mejias, 2019b, p. 344). The human subject is abstracted into data and 'traded in proxy form' (2019b, p. 345). We can further analyse such relations by paying attention to their perverse elements. The pervert – i.e. the platform – wishes to own, manipulate, dominate, and play with the other (the users) in the perverse relationship. This is accomplished by 'making submission to tracking a requirement of daily life' (Couldry & Mejias, 2019a, p. 157, italics in original). The term 'submission' is interesting here, for it suggests that users are in a perverse, sado-masochistic relationship to platforms. They are made to submit in exchange for services – and domination. All this happens while platforms fundamentally deny or downplay their datafication practices and restrict external access via their APIs (Bruns, 2018). They emphasise sociability, convenience, entertainment, connection, and care. They create a new reality where legitimate concerns that users have are negated. This is the ultimate aim of the pervert: to create a reality that shuts out everything else that is beyond the relationship. The reality that platforms create is that users need them in order to be able to live full lives and be an ordinary human being. Such strategies of user retention and keeping

users attached to platforms show themselves in a particular way. Stein defines the perverse relationship as:

> Two features common to both sexual and non-sexual perverse relations are (1) the seductive and bribing aspects of perversion, and (2) its means-ends reversal, that is, the turning of the means into an end in itself, and the bending of a purported end into a means for something else, i.e. a hidden agenda. Perversion as a mode of relatedness points to relations of seduction, domination, psychic bribery and guileful uses of 'innocence', all in the service of exploiting the other. (Stein, 2005, p. 781, italics in original)

Such a description can also serve to designate what is meant by data perversion. Users are seduced into using platforms because they offer particular means (e.g. calling an Uber, watching a film on Netflix, buying a book on Amazon, chatting to a friend on Facebook). Those means really do exist and bind users to those platforms. Platforms fulfil a purpose for users and often make their lives easier. However, in reality, as we see with Stein above, those means are just means to an invisible end. The hidden agenda is data collection for the purposes of profit maximization and user growth.

We can see how such dynamics operate by drilling down further into datafication as such. Datafication often makes use of a particular, binary logic: target or waste (Kennedy, 2016). Users are automatically classified into categories which are often constructed based on particular types (in the case of targeted advertising for example). John Cheney-Lippold (Lippold, 2017) has discussed this and comes up with the term 'measurable type'. Based on the data we produce, any data and not just social media data, we are turned into measurable types, or digital subjects. It is not only that user data are sold, they are also used to determine who users are for social media companies such as Google, Facebook, Weibo and Twitter for example. Based on usage of such platforms, patterns are established. Those patterns lead to the automatic creation of profiles (data shadows) of who users are for them.

> Measurable types are most often subterranean, protected and unavailable for critique, all while we unconsciously sway to undulating identifications. Every time we surf the web, we are profiled with measurable types by marketing and analytic companies […]. We are assigned identities when we purchase a product, walk down a street monitored by CCTV cameras, or bring our phones with us on vacation to Italy. (Cheney-Lippold, 2017, p. 66)

This intense monitoring and datafication of individuals leads to a practice of subjects being coded as if they are someone or fit to already established categories rather than being directly addressed in their full complexity, Cheney-Lippold has argued. Additionally, the digital mirror-images of users' online selves are never fixed and always dynamic, depending on if their behaviour online changes. The, at times, fundamental discrepancy and contradiction between who users think they are and who platforms like Facebook or Google think they are introduces an 'alien' (Cheney-Lippold, 2017, p. 193) dimension into the contemporary moment of data-

driven subjectivities. This perverse act of cherishing users and offering them connectivity, information and communication, only to be then turned against them in the form of data mining and profiling amounts to a fundamental practice of dehumanization that is inherent in perversion (Knafo & Lo Bosco, 2017).

Such a relationship means that the subject feels alienated form themself, feels a gap or distance between themself and the data shadow or data double. The goal on the part of the pervert is 'to erase difference'. This is done 'by assuming—and seductively "demonstrating" through creating a semblance of intimacy—that one knows the other from the inside out, that people are knowable by the force of one's will' (Stein, 2005, p. 790). This is precisely what happens in the perverse relationship between users and platforms. Users are clustered together according to specific categories so that similarities and differences can be analysed (Chun, 2018). All of this is done under the illusion of providing knowledge, transparency and connectivity to users. It is suggested that platforms know what users want and can provide it. Datafication is not only about mining data from individual subjects, it is about collecting massive datasets so that patterns can be found and conclusions about millions of individuals can be drawn. Users are both valued as individuals and devalued by becoming just small data points amongst millions of others. The other is thereby rendered 'into a mechanized and digitalized entity, a robotized mechanism, occasionally multiplied into an anonymous crowd of uniform, faceless robots.' (Stein, 2005, p. 778). Such acts demonstrate the violence of datafication that many scholars have highlighted (Fuchs, 2014; Couldry & Mejias, 2019a; Zuboff, 2019).

However, and this is a crucial dimension of perversion as a psychoanalytic concept, such forms of dehumanization and exploitation can only work in a relationship if they are coupled with and masked by intense feelings of love, care, and idealization. The pervert purports to deeply love and worship the other, in order to be able to manipulate her. While perversion is a form of exploitative seduction, it is nonetheless accompanied by love, care and warmth at the same time. The same dynamics are in place on the part of perverse platforms today: they love, idealize and care for their users. Otherwise the platforms would cease to exist. They depend on continuous user engagement and therefore must provide functioning services, more content, new features, constant updates (Chun, 2016) to keep users attached and within the relationship. Contemporary platforms are so effective at achieving this, because they address users individually and communicate how valued each and every one of them is to them. Users feel valued and cared for by the platforms that they use. Such feelings of warmth, communication and care are genuine on the part of the platform owners, because, after all, users lead to revenue. However, it is important to stress that perversion is not a one-sided form of exploitation, violence, or manipulation of the other against her will. It goes beyond forms of colonialism in that sense. Perversion constitutes a relationship, a 'perverse pact' as Stein (2005, p. 774) calls it, in which the other willingly (un/consciously) participates. It 'is essentially a power strategy geared to derail the other by subtly seducing him into

becoming a willing partner and excited colluder in the pervert's project' (2005, p. 782). How then do users come to be voluntary partners in perverse data relations? The next section moves from the perspective of the platform to that of the user.

5 USERS: FEELING LOVED AND VALUED IN THE PERVERSE PACT

A further dimension is added when we consider that users themselves place a great amount of trust into the services that they use. Many believe that for instance targeted advertising, recommendation systems or other automated mechanisms online enhance their lives – and they do. Through their actions they are complicit in the forms of dehumanization they are subjected to.

Couldry and Mejias argue that consent is often implicit within data relations. Users vaguely know or know nothing at all about how their data are used, tracked, or sold on various platforms. Users opt into data relations because otherwise the platforms would be unavailable to them. They claim that if the fact that platforms own user data would be more explicit, users would contest this more often (Couldry & Mejias, 2019a, p. 29). This may be true, but at the same time, there is now widespread knowledge or at least assumption on the part of many users about questions of data ownership (Perrin, 2018; Brown, 2020). The Snowden leaks and the Cambridge Analytica scandal contributed to wider diffusion of such knowledge (Dencik & Cable, 2017; Fuchs & Trottier, 2017). Users are thus perhaps more willing to participate in data relations than Couldry and Mejias think. Why then is this the case? It could be a lack of alternatives and social pressure (Fuchs & Sevignani, 2013). Users simply have to opt in because otherwise they would miss out. This explanation is too simple. Zuboff argues that users defend against datafication, tracking and surveillance:

> User dependency is thus a classic Faustian pact in which the felt needs for effective life vie against the inclination to resist instrumentarian power's bold incursions. This conflict produces a psychic numbing that inures users to the realities of being tracked, parsed, mined, and modified. It disposes users to rationalize the situation in resigned cynicism, shelter behind defense mechanisms ('I have nothing to hide'), or find other ways to stick their heads in the sand, choosing ignorance out of frustration and helplessness. In this way, surveillance capitalism imposes a fundamentally illegitimate choice that twenty-first-century individuals should not have to make, and its normalization leaves users dancing in their chains. (Zuboff, 2019, online)

However, such an argument renders users as innocent and defensive beings who give up resistance in apathy. Instead, I argue that users actively participate in their own domination and exploitation, not because they are duped or manipulated. There is something thrilling about it. The perverse character of such a relation helps to explain the willingness on the part of the users to consent to giving up data ownership. It is not just that users opt in because they have no alternative option, contemporary data platforms are so effective because (1) they show users that they

are loved and needed by those platforms and (2) that users can feel themselves valued and powerful because the platforms are customised for them. The social character of Amazon, Facebook, Uber or Netflix shows itself in individual user accounts. Users construct profiles and their experience of using the platform is shaped by the data they create. Users can use platforms, social media in particular, according to their desires and create content, exchange opinions, find friends, etc. They can use them according to their own thoughts and goals. Platforms (literally) recognize them and suggest exciting opportunities whenever users log on. Stein writes about 'the talent of the perverse person to give her object, the chosen other, an exquisite feeling of entitlement, through keenly sensing the other's wishes and desires and exquisitely fulfilling them, thereby ensuring the other's bondage.' (Stein 2005, 794). Facebook serves as a good example here to illustrate how users are recognized, valued and cared for. 'What is on your mind?, Facebook asks its users. 'What is happening?', Twitter wishes to know. The more time users spend on those platforms and the more data they generate, the more are they rewarded through the inherent interface features of the platforms. At the end of one year, Facebook sent me a celebratory message: 'Jacob, you've made 20 friends on Facebook this year! Thank you for making the world a bit closer. We think this is something to celebrate!'. A few months later, I received the following: 'Jacob, your friends have liked your posts 6,000 times! We're glad you're sharing your life with the people you care about on Facebook.'. After responding to a Facebook survey, I was told: 'Thank you, Jacob! We'll use your feedback to improve Facebook. If you want, you can add comments too.'. It perhaps speaks volumes that upon hiding an advertisement on Facebook, users can select from a number of reasons why they chose to do so: 'Knows too much', 'irrelevant', 'too personal', 'sensitive topic', 'already purchased' or 'repetitive'.

Such messages, distinctly aimed at myself as an individual subject who is in (data) relations with other users, denote a happy feeling of a community on the platform. They address me in positive ways and value my existence on Facebook. They do not say who else has been viewing part of my data and how much money Facebook has made from my data being sold for targeted advertising. I, and everyone else, feels valued and cared for by such messages.

> The other is made to share a vague but intense hope of great fulfillment and often love, and, if the strategy is sophisticated enough, the seduction of the other is made to seem like mutual self-discovery, or like a desire originating from within the seduced person, rather than the premeditated strategy of the seducer that it is. (Stein, 2005, p. 782)

Such feelings are similar to feelings of seduction, because I know that Facebook collects my data for particular purposes. Nonetheless, I am willingly participating in the perverse pact: 'a relationship between two accomplices, a mutual agreement woven of complex, twisted relations and excited games, embedded in multilayered degrees of awareness and obliviousness.' (Stein, 2005, p. 787). Facebook has given

us the opportunity to ignore or negate questions of data ownership, surveillance, etc. because communication, care, and love is foregrounded on the part of the platform. We affirmatively respond to such a strategy by continuing to use the platform, uploading our data, and sharing it with others and often receiving recognition, care, and love from others in return (Balick, 2014). Through such an ideology, which is inherently perverse because it masks the commercial interests of platforms, we happily consent to signing 'an implicit contract […] against reality' (Stein, 2005, p. 793). This contract, signed literally by agreeing to any platform's terms and conditions, is 'aimed at a constant mutual reassurance and the professing of a love that is false' (2005, pp. 793-794).

6 CONCLUSION

This article responds to recent critical scholarship on datafication and presented the argument that users are in a perverse relationship to the platforms they use. Through datafication platforms believe that they are able to fully capture subjects and turn them into commodifiable datasets. In that sense, a subject is made to be mirrored in various datasets they have created online and reassembled by apps, social media companies, streaming services, data brokers and other stakeholders. This is done over and over on a large scale and gives rise to 'big data': large datasets that are made up of thousands of different data points. Individual, subjectively created data thus constitutes the elements of big data and is at the same disavowed through it being bundled together with vast amounts of other data such as meta-data or data that the subject may have left behind involuntarily. Platforms, such as social media, are dependent on individuals who create and use data, but a real meaning and economic asset is only acquired through an accumulation into large datasets. Individual subjectivities and how they are expressed online thus become embraced and disavowed by platforms at the same time. The subject is lured into producing ever more data and turned into a commodified entity that is surveilled and used. Subjects are thus affecting their data creation, voluntary and involuntary, and are likewise affected by datafication processes which often result in their data being merged with other data, sold and bought.

The relationship between users and the services and platforms which mine / use their data is complicated and symbiotic. Users have become embedded in a perverse relationship. There is a strong imbalance between how the users perceive the relation to platforms and how the platforms (and their owners, developers and other staff) perceive their relations to users. While users are, so it appears, cared for by e.g. Facebook, Netflix or Uber in so far as they are given platforms that they can use, where rules are laid down and enforced (Balick, 2014) beneath the surface, this feeling of security is broken and users are denied mastery over their data and their destiny. Users are subjected to love and care, and to abuse and exploitation at the same time by Facebook, Netflix and others through enabling communication and sociality as well as destruction and reshaping of their online subjectivities through

datafication. The clinical concept of perversion furthermore suggests that users play an active part in entering into and sustaining such a relationship. They want to feel valued, cared for and idealized. At the same time, they know what happens to their data and nonetheless remain on the platforms. The positive aspects are emphasised and the dark aspects of datafication are negated or downplayed by users as well as by platforms. Data perversion should thus perhaps be responded to with another psychoanalytic notion: a healthy form of paranoia.

Drawing on the psychoanalytic concept of perversion in order to advance theorisations of big data is useful because it can add further layers of complexity to this topic. Psychoanalysis shifts the focus to (seemingly) contradictory, ambiguous and ambivalent modes and moments within the human subject and intersubjective relations. Such relations include mediated and datafied relations as they express themselves on commercial platforms that rely on big data analytics for their business models. Psychoanalysis upholds that subjects are often embedded within particular psychodynamics that are damaging to their mental health. Yet, they find themselves deeply drawn to and unable to leave such relations, because they are un/consciously and affectively invested in them. Naturally, the platforms that they use also provide convenient services (communication, connection, sharing of content, accessing resources, etc.) that are deeply meaningful to users. Regarding platforms as inherently exploitative or useful only scratches the surface. A psychoanalytic perspective can shed light on how users and owners, developers, and support staff have un/consciously created a complex symbiosis.

FUNDING STATEMENT

No funding was used as part of the research for this article.

REFERENCES

Bach, S. (1994). *The Language of perversion and the language of love*. Northvale, NJ: Aronson.

Baker, R. (1994). Psychoanalysis as a lifeline: A clinical study of a transference perversion. *International Journal of Psycho-Analysis*, 75(4), 743-753.

Balick, A. (2014). *The psychodynamics of social networking: Connected-up instantaneous culture and the self*. London: Karnac Books.

Brown, A. J. (2020). "Should I stay or should I leave?": Exploring (dis) continued Facebook use after the Cambridge Analytica scandal. *Social Media + Society*, 6(1), 1-8. 10.1177/2056305120913884.

Bruns, A. (2019). After the 'APIcalypse': social media platforms and their fight against critical scholarly research. *Information, Communication & Society*, 22(11), 1544-1566. /10.1080/1369118X.2019.1637447.

Celenza, A. (2014). *Erotic revelations: Clinical applications and perverse scenarios*. London: Routledge.

Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York: NYU Press.

Chun, W. H. K. (2016). *Updating to remain the same. Habitual new media*. Minneapolis: University of Minnesota Press.

Chun, Wendy H. K. (2018). 'Queerying homophily'. In: Apprich, C./Chun, W. H. K./Cramer, F./Steyerl, H. (Eds.): *Pattern discrimination*. Minneapolis: University of Minnesota Press and Meson Press, 59-98.

Clough, P. T. (2018). *The user unconscious: On affect, media, and measure*. Minneapolis: University of Minnesota Press.

Couldry, N. & Mejias, U. (2019a). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Palo Alto: Stanford University Press.

Couldry, N., & Mejias, U. A. (2019b). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336-349. 10.1177/1527476418796632.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, 11, 763-781.

Freud S. (1981) *Three essays on the theory of sexuality. The Standard Edition of the Complete Works of Sigmund Freud. Volume VII. A case of hysteria, three essays on sexuality, and other works*. London: Hogarth Press and the Institute of Psycho-Analysis.

Fuchs, C. (2014). *Digital labour and Karl Marx*. London: Routledge.

Fuchs, C. (2019). Karl Marx in the age of big data capitalism. In: Chandler, D. & Fuchs, C. (eds.) *Digital objects, digital subjects: Interdisciplinary perspectives on capitalism, labour and politics in the age of big data*. London: University of Westminster Press, 53–71.

Fuchs, C. and S. Sevignani. (2013). What is digital labour? What is digital work? What's their difference? And why do these questions matter for understanding social media? *triple C—Journal For A Global Sustainable information Society*, 11(2), 237–293. 10.31269/triplec.v11i2.461.

Fuchs, C., & Trottier, D. (2017). A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden. *Journal of Information, Communication & Ethics in Society*, 15(4), 412-444. 10.1108/JICES-01-2016-0004.

Gillespie, T. (2014). The relevance of algorithms. In: Gillespie, T., Boczkowski, P. and K. Foot (Eds.): *Media technologies. Essays on communication, materiality, and society*. Cambridge, MA: the MIT Press, 167–194.

Gillespie, T. (2018). *Custodians of the internet. Platforms, content moderation, and the hidden decisions that shape social media*. New Haven: Yale University Press.

Jarett, K. (2016). *Feminism, labour and digital media: The digital housewife*. New York: Routledge.

Johanssen, J. (2019). *Psychoanalysis and digital culture: Audiences, social media, and big data*. London: Routledge.

Karppi, T. (2018). *Disconnect. Facebook's affective bonds*. Minnesota: University of Minnesota Press.

Kennedy, H. (2016). *Post, mine, repeat: Social media data mining becomes ordinary*. Basingstoke: Palgrave Macmillan.

Khan, M. (1979). *Alienation in perversions*. New York: International Universities Press.

Knafo, D. and Lo Bosco, R. (2017). *The age of perversion: Desire and technology in psychoanalysis and culture*. London: Routledge.

Lupton, D. (2019). Data selves: *More-than-human perspectives*. Cambridge: Polity Press.

Mosco, V. (2014). *To the cloud. Big data in a turbulent world*. London: Routledge.

Munn, L. (2019). Cash burning machine: Uber's logic of planetary expansion. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, 17(2), 185-201. 10.31269/triplec.v17i2.1097.

Noble, S. (2018). *Algorithms of oppression. How search engines reinforce racism.* New York: New York University Press.

Perrin, A. (2018). Americans are changing their relationship with Facebook. *Pew Research Center*, http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebok.

Pinchevski, A. (2019). *Transferred wounds: Media and the mediation of trauma*. Oxford: Oxford University Press.

Rouvroy, A. (2013). 'The end(s) of critique: Data-behaviourism vs. due process'. In: Hildebrandt, M. & De Vries, K. (Eds.). *Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology*. London: Routledge, 143-168.

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2016). Automation, algorithms, and politics. When the algorithm itself is a racist: Diagnosing ethical harm in the basic components of software. *International Journal of Communication*, 10(2016), 4972–4990.

Simula, B. L. (2019). Pleasure, power, and pain: A review of the literature on the experiences of BDSM participants. *Sociology Compass*, 13(3), e12668. 10.1111/soc4.12668.

Singh G. (2018). *The death of web 2.0. Ethics, connectivity and recognition in the twenty-first century*. London: Routledge.

Srnicek, N. (2017). *Platform capitalism*. Cambridge: Polity Press.

Stein, R. (2005). Why perversion? "False love" and the perverse pact. *International Journal of Psychoanalysis*, 86(3), 775– 799. /10.1516/PFHH-8NW5-JM3Y-V70P

Turkle, S. (2011). Alone together: Why we expect more from technology and less *from each other*. New York: Basic Books.

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. 10.24908/ss.v12i2.4776.

Weiss, M. (2011). Techniques of Pleasure: BDSM and the circuits of sexuality. Durham: Duke University Press.

West, S. M. (2017). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, 58(1), 20-41. 10.1177/0007650317718185.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89. 10.1057/jit.2015.5.

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum*. https://newlaborforum.cuny.edu/2019/01/22/surveillance-capitalism/.

JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 1, 2021, 106–118

THE TWITTER EXPLORER: A FRAMEWORK FOR OBSERVING TWITTER THROUGH INTERACTIVE NETWORKS

Armin Pournaki, Felix Gaisbauer, Sven Banisch and Eckehard Olbrich*

ABSTRACT

We present an open-source interface for scientists to explore Twitter data through interactive network visualizations. Combining data collection, transformation and visualization in one easily accessible framework, the *twitter explorer* connects distant and close reading of Twitter data through the interactive exploration of interaction networks and semantic networks. By lowering the technological barriers of data-driven research, it aims to attract researchers from various disciplinary backgrounds and facilitates new perspectives in the thriving field of computational social science.

Keywords: Twitter, complex networks, interface, digital methods, computational social science.

* Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany.

1 INTRODUCTION

Due to its public-by-default nature and the possibility of calling data sets conveniently via an API, Twitter has become a widely used source for the observation and analysis of political debates (Conover, Gonçalves, et al. 2011; Gaumont, Panahi, and Chavalarias 2018), sentiments (Paltoglou and Thelwall 2017), brand communication (Nitins and Burgess 2014), or natural disasters (Bruns and Burgess 2014), to name a few. Different kinds of interactions on Twitter (Rainie 2014) are often represented in the form of networks, such as retweet networks (Conover, Gonçalves, et al. 2011; Conover, Ratkiewicz, et al. 2011), reply networks (Gaisbauer et al. 2020), mention networks (Conover, Ratkiewicz, et al. 2011), follower networks (Myers et al. 2014) or co-hashtag networks (Burgess and Matamoros-Fernández 2016). While many of the employed methods, building on concepts from graph theory and network science, can be regarded as distant reading approaches, it is undoubtedly crucial for social science researchers to perform a close reading[1] of digital traces to gain a more focused and specific understanding of their objects of research. As an interface that bridges the two approaches, the *twitter explorer* gives an "overview of the data that highlights potentially interesting patterns", while allowing a "drill down on. these patterns for further exploration" (Jänicke et al. 2015). This means that the structural overview given by the network allows the user to find the relevant content through a framework we present as "guided close reading". In this context, we conceive the *twitter explorer* as a social media observatory, enabling users to "capture the complexities of social behaviour [...] through computational analyses of digital media data" (Willaert et al. 2020).

2 PREVIOUS WORK

There exists a wide range of tools for collecting, analyzing and visualizing Twitter data, some of which are referenced on Twitter's own website (Twitter 2020e). Among the most popular tools are DMI tcat (Borra and Rieder 2014) for data collection and analysis in combination with the powerful network visualization suite Gephi (Bastian, Heymann, and Jacomy 2009). While many existing solutions are suited for one specific task and rely on the interplay and compatibility of several applications, the *twitter explorer* provides an open framework that combines data collection, transformation and visualization and allows users to explore the collected Twitter corpus interactively, while being open to external data sources and analysis suites through data import and export. To better situate the *twitter explorer* in its context, a comparison of existing tools is presented in Table 1 below.

[1] These terms were originally coined by Franco Moretti in the context of literary studies (Moretti 2000). Close reading refers to "the thorough interpretation of a text passage" (Jänicke et al. 2015), while distant reading "aims to generate an abstract view by shifting from observing textual content to visualizing global features of a single or of multiple text(s)" (Jänicke et al. 2015).

Table 1. A comparison of tools for access, analysis and visualization of Twitter data. Due to the steady pace of tool development in this field of research, this list cannot be exhaustive. However, we aim to give an overview of some popular methods and their features. A checkmark in parenthesis denotes basic or experimental functionality. Note that we included almost only open-source software in the table. Furthermore, we chose to omit tools that were not maintained anymore.

	data access		data analysis		data visualization		data flow		
	search	stream	statistics	networks	static	interactive	input	output	last commit
twitter explorer	✓	–	✓	✓	✓	✓	✓	✓	1/29/21
twarc[2]	✓	✓	✓	✓	–	–	–	✓	1/24/21
DMI tcat[3]	✓	✓	✓	✓	✓	(✓)	–	✓	7/20/20
NodeXL Pro[4]	✓	✓	✓	✓	✓	✓	✓	✓	–
Gephi[5]	–	–	–	–	✓	(✓)	✓	✓	9/28/20
Facepager[6]	✓	–	✓	✓	✓	–	–	✓	1/28/21
Twint[7]	–	–	✓	✓	✓	–	–	✓	12/17/20
vosonSML[8]	✓	✓	✓	✓	✓	–	✓	✓	12/26/20
SMO-TMAS[9]	✓	✓	✓	✓	✓	–	–	–	11/13/19
OSoMe[10] **botslayer/hoaxy**	–	✓	✓	(✓)	✓	(✓)	–	✓	1/12/21
OSoMe Networks	–	(✓)	–	–	✓	✓	–	–	–

3 ARCHITECTURE

The *twitter explorer* consists of three components:

- The collector, a Streamlit-powered[11] (Treuille, Teixeira, and Kelly 2020) application provides a graphical user interface for the Twitter Search API and saves the collected data for further processing.
- The visualizer, a Streamlit-powered application provides a graphical user interface for the generation of interaction networks and semantic networks based on the collected data and saves the interactive networks.
- The explorer interface allows users to interact with the networks and explore the underlying metadata of nodes and links.

Each of these components is conceived in a modular way which facilitates adding new features to the *twitter explorer* (see Figure 1).

[2] DocNow (2020)
[3] Borra and Rieder (2014)
[4] Smith (2013)
[5] Bastian, Heymann and Jacomy (2009)
[6] Jünger and Keyling (2019)
[7] TWINT-Project (2018)
[8] VOSON-Lab (2018)
[9] Young (2020)
[10] Davis et al. (2016)
[11] Streamlit is a Python library for the creation and deployment of data-analytic tools

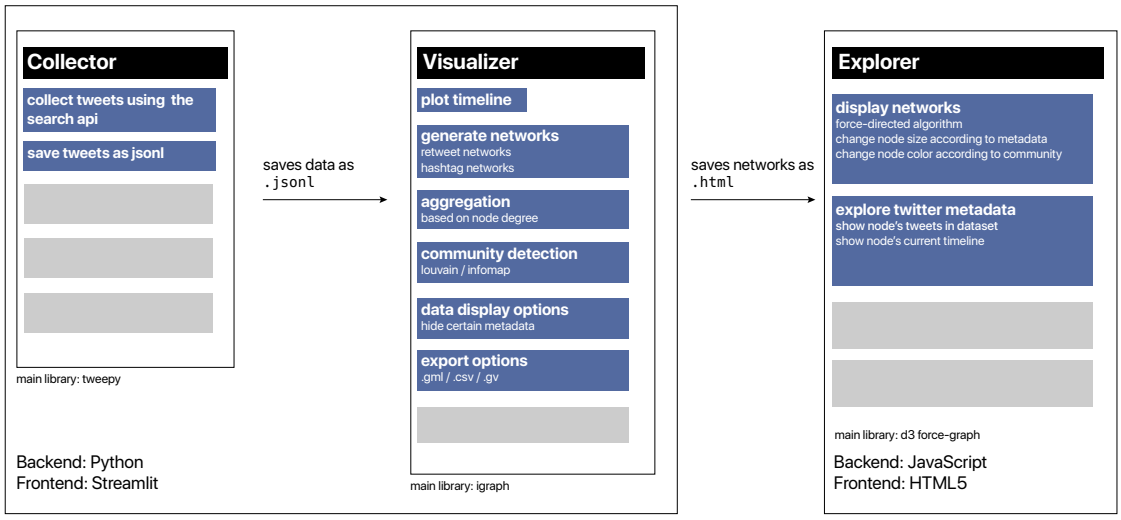

Figure 1. The twitter explorer framework. The collector (left), after having set up the credentials, allows for connection to the Twitter Search API and saves the collected tweets in jsonl format. They are then passed on to the visualiser (middle), where the user can get an overview of the content and then create the retweet- and hashtag networks. The interactive networks are generated as html files that can be explored in the web browser. The modular structure of the three components facilitates the development of new features, which are suggested by the light grey boxes.

3.1 DATA ACQUISITION: THE COLLECTOR

In the collector, the user interacts with the Twitter Search API (Twitter 2020f), giving access to a limited set of tweets from the last 7 days.

3.1.1 Authentication

Since 2018, users need to apply for a Twitter Developer Account in order to access the API (Roth and Johnson 2018). Since the collector makes direct API calls, this step is necessary for its usage. There are developer accounts specific to academic research (Twitter data for academic research 2020). The user can then create app tokens which will allow the *twitter explorer* to connect to the API via Application-only authentication (OAuth 2.0) (Twitter 2020a).

3.1.2 Collection

There are different APIs for users to collect Twitter data. The Stream API (Twitter 2020g) filters all incoming tweets for a given search string. It can be used to collect tweets containing a certain keyword, or to collect all tweets by a certain (group of) user(s). This API allows the retrieval of all published tweets and is only capped by the upper bound of 1% of the total Twitter traffic. The *twitter explorer* has no built-

in feature for the Stream API because we believe that such collections are best done on a headless server which stores the large amounts of incoming data in a database. To collect tweets from the past, we recur to the Search API (Twitter 2020f). The collection of tweets is again initiated by a keyword string, following the rules of a Twitter Advanced Search (Twitter 2020c). This free API comes with limitations: users can only make a limited number of requests per 15 minutes (Twitter 2020d). In the *twitter explorer*, tweets are continuously stored until all possible tweets that the Search API provides are collected.

Note that the Search API gives access only to indexed tweets from the last 7 days. Therefore, a collection created by the Search API cannot be considered extensive, and it is subject to Twitter's nontransparent filtering algorithm. Previous research on the comparison between Stream and Search API however concludes that Twitter filters mostly duplicates and strong language (Thelwall 2015; Black et al. 2012). Measuring the volume of a 48-hour collection of tweets based on the keyword "clubhouse", we find that 80% of tweets from the Stream API collection are contained in the Stream API (see Figure 5 in the Appendix).

3.2 DATA TRANSFORMATION: THE VISUALIZER

The visualizer creates interactive network visualizations from the collected corpus. One can distinguish between interaction networks (with users as nodes) and semantic networks (with words or concepts as nodes). The *twitter explorer* currently supports the creation of retweet networks as interaction networks and hashtag co-occurrence networks as semantic networks. Several data aggregation methods allow for exploration of the network at different scales.

3.2.1 Twitter timeline

The data is presented as a timeline, where tweet counts are plotted over time. The user can get a feeling of the overall salience of the chosen keyword and possible peaks can hint towards special events.

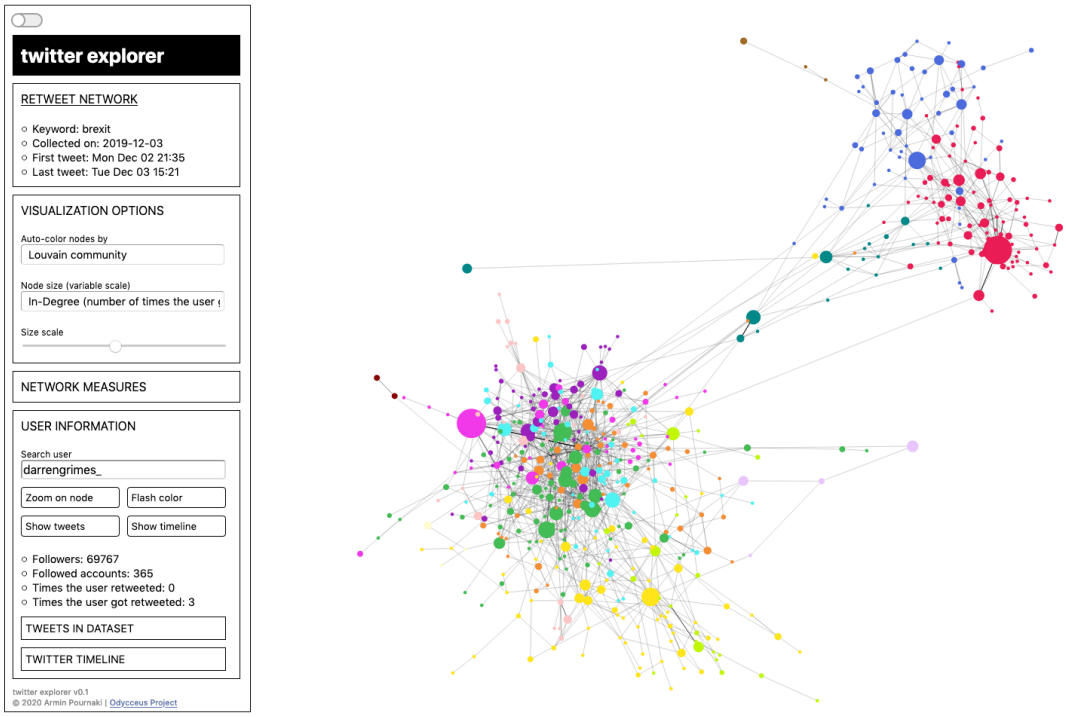

Figure 2. The retweet network exploration interface. The modular command palette (left) can (1) show information about the underlying data, (2) modify the visualization, (3) display network measures and (4) search for and show information about specific users and the content they generated in the dataset. Nodes are colored according to their community. They can be interacted with by clicking or hovering to display the username and relevant metadata in the palette. We invite the reader to test the interactive visualization here: https://twitterexplorer.org/try.html

3.2.2 Interaction networks

There are several ways of interaction on Twitter: retweets, mentions, replies, following, likes, quotes and direct messages. Not all of them are accessible through the API. We focus on retweet interaction which can be represented as a directed network in which nodes are users and a link is drawn from node to if retweets . The *twitter explorer*'s visualizer provides an interface for creating retweet networks which includes the following features:

Community detection. In order to find strongly connected clusters of a network, it has become common practice to employ community detection algorithms. The *twitter explorer* currently supports Louvain (Blondel et al. 2008) and InfoMap (Rosvall and Bergstrom 2007) algorithms.

Force-directed layout. The visualization library (Asturiano 2018) spatializes the network using a force-directed layout in which nodes that retweet each other more often are placed closer to each other (Noack 2009).

Aggregation methods. One challenge for understanding and visualizing complex interaction networks is to find useful aggregation methods necessary to

observe the underlying discourse at different levels of granularity. We therefore propose several methods of node aggregation: (1) removing nodes that only retweet one source and don't generate any content, (2) removing nodes that were retweeted less than times and (3) reducing the network to an interaction network of communities (cluster graph).

Hiding sensitive metadata. Removes all accessible metadata of users that have less than 5000 followers from the interactive visualization. The nodes are visible, and their links are taken into account, but they cannot be personally identified in the interface.

Export abilities. Exports the networks to common formats like edgelist, GML or GraphViz. The framework is therefore compatible with a wide range of existing tools for network analysis (Bastian, Heymann, and Jacomy 2009; Peixoto 2014; Csardi and Nepusz 2006).

An example of a retweet network visualized with the *twitter explorer* can be seen in Figure 2. We collected data using the keyword "Brexit" about 10 days before the General Election in the UK in December 2019. We observe a polarized retweet network, where pro and anti-Brexiteers form two distinct clusters. This hints to the fact that users in the debate tend to mainly share (and endorse) content created by their own opinion group.

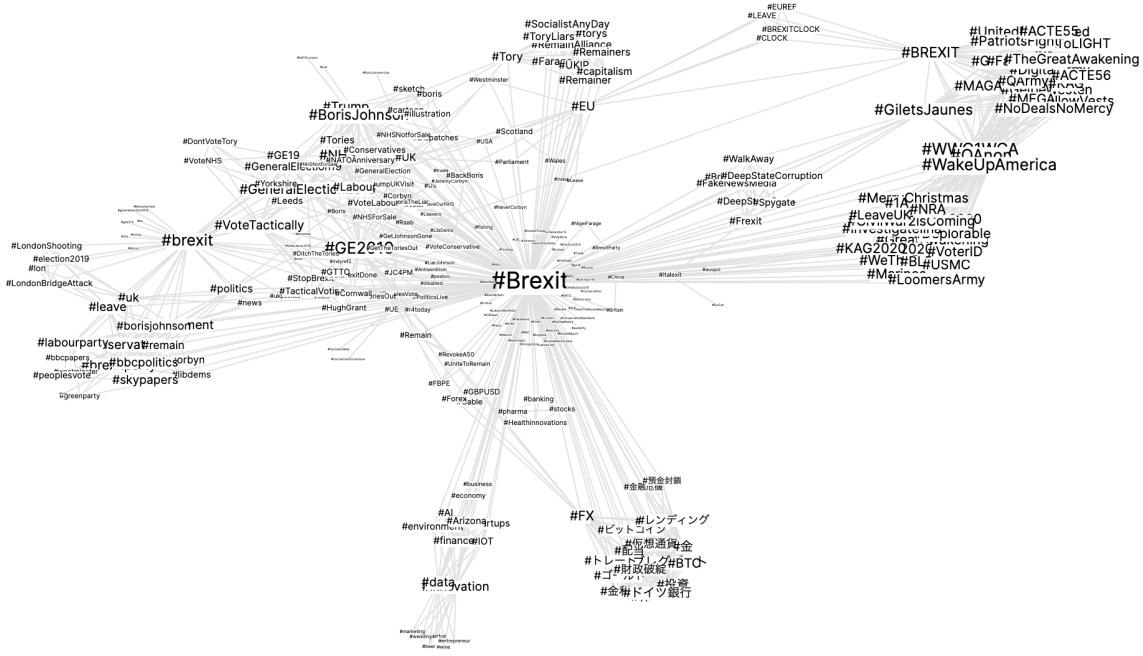

Figure 3. Hashtag network. Every node is a hashtag, and a link is drawn between hashtags for every tweet they appear in together. The size of the text corresponds is proportional to the node degree. We invite the reader to test the interactive visualization here: https://twitterexplorer.org/try_htn.html

3.2.3 Semantic networks

While retweet networks allow to identify the main proponents of a debate and their interaction patterns, looking at the most retweeted tweets might not be sufficient to get an impression of the content structure of the debate. In order to explore the textual content of the data, we propose hashtag co-occurrence networks. Here, every node is a hashtag, and links are drawn between nodes if they appear in the same tweet. By again laying out the network with a force-directed algorithm, the hashtag network gives an overview of the debate's vocabulary and can reveal the different subtopics within a debate.

An example using the previously introduced Brexit data is shown in Figure 3. Hashtags like "#votetactically", "#GetTheToriesOut" or "#VoteConservative" point towards discussions closely related to the General Election, while hashtags like "#DeepStateCorruption", "#TheGreatAwakening" or "#QAnon" shed light on the existence of conspiracy-theory-related sub-discussions in the dataset.

3.3 NETWORK EXPLORATION INTERFACE

The *twitter explorer* offers an intuitive exploration interface (see Figure 2). A modular command palette allows for user interaction and provides insight into the underlying meta data of the network:

Network information. Accesses generic information about the network (keywords used to collect the data, date of collection, first/last tweet of the dataset).

Visualization options. Supports different node colorings according to their community assignment. The node size can be dynamically changed according to their respective metadata values (in/out-degree, number of followers, number of followed accounts). This facilitates for instance the detection of news outlets.

Network measures. Shows the number of nodes and links in the network. This set will be extended to include a wider range of network indicators in future releases.

User information. Search users in the given network and find them by zooming or flashing their color. Display the user's relevant metadata (number of followers, number of followed accounts, number of retweets, number of times retweeted), their tweets in the dataset as well as their current timeline. Note that the interface will only display tweets that are still online at the time of exploration. By doing so, it complies with the Twitter display requirements (Twitter 2020b).

4 INTEGRATION WITH OTHER METHODS

The *twitter explorer* can be regarded an all-in-one-solution for the exploration of Twitter networks, for which it is easy to develop new modules within the existing components (see Figure 1). An example would be to include additional community detection algorithms or new node aggregation methods.

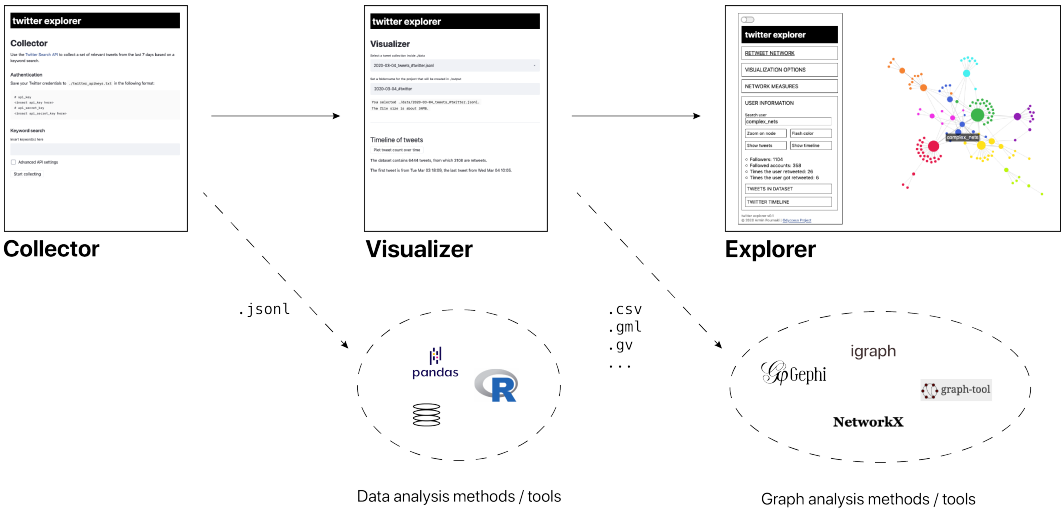

Figure 4. The twitter explorer in context. Its modular structure makes it easy to develop new features for the twitter explorer, but it also allows it to be used in combination with existing data analysis and network science tools. The dotted arrows depict export paths allowing users to integrate the (transformed) data from the twitter explorer into their desired data analysis environment.

At the same time, its modular structure (division into collector / visualizer / explorer) and the ability to export the generated data makes the tool compatible with a variety of other data analysis tools (see Figure 4). Therefore, scientists can use the *twitter explorer* in combination with existing tools from data and network science. For instance, after the collector, the data could be passed on to a database, or passed on to a natural language processing pipeline for content analysis. After the visualizer, the exported network can be imported to a visualization suite like Gephi, where various network measures and layout algorithms can be computed.

4.1 FUTURE DEVELOPMENT

The *twitter explorer* is currently in an open beta stage on GitHub. Future work will include the dynamical nature of retweet interaction in the visualization paradigms. In order to disseminate the framework and attract new audiences to the field of data-driven research, vignettes (use-cases) will be designed to showcase the *twitter explorer*'s use in social science research. They will be published on our blog which is

accessible at https://blog.twitterexplorer.org. Furthermore, it is planned to add the possibility of exploring recently developed measures such as graph curvatures which can provide new insights to the analysis of social networks (Leal et al. 2018). The authors plan to actively maintain the tool and adapt it to Twitter API changes, like the one that was recently announced for Academic Research (Twitter 2021).

4.2 AVAILABILITY

The *twitter explorer* interface can be tested at https://twitterexplorer.org. The source code is available on GitHub, where the current release can be downloaded (Pournaki 2020). It is licensed under the GNU GPLv3 license (Free Software Foundation Inc. 2007).

4.3 TECHNICAL DETAILS

The *twitter explorer* is written partly in Python (data collection and transformation) and JavaScript (interactive network visualization). The frontend for the data collector and the visualizer is made with Streamlit (Treuille, Teixeira, and Kelly 2020), a Python library for the creation and deployment of data-analytic tools. The Twitter objects are stored in the json lines format (Ward 2020). The network operations and community detection rely on the Python implementation of igraph (Csardi and Nepusz 2006). The interactive networks are drawn using D3.js (Bostock 2011), more specifically the force-graph library (Asturiano 2018).

AUTHOR CONTRIBUTIONS AND FUNDING STATEMENT

The idea for the *twitter explorer* originated from fruitful discussions in the context of the ODYCCEUS project between Armin Pournaki, Felix Gaisbauer, Sven Banisch and Eckehard Olbrich. The tool is designed and developed by Armin Pournaki. All authors wrote the manuscript. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732942.

REFERENCES

Asturiano, Vasco (2018). *force-graph*. https://github.com/vasturiano/force-graph. [Online; accessed 29-January-2021].

Bastian, Mathieu, Sebastien Heymann, and Mathieu Jacomy (2009). "Gephi: An Open Source Software for Exploring and Manipulating Networks". In: url: http://www.aaai.org/ocs/index.php/ICWSM/09/paper/view/154.

Black, Alan et al. (2012). "Twitter zombie: Architecture for capturing, socially transforming and analyzing the Twittersphere". In: *Proceedings of the 17th ACM international conference on Supporting group work*, pp. 229–238.

Blondel, Vincent D et al. (2008). "Fast unfolding of communities in large networks". In: *Journal of statistical mechanics: theory and experiment* 2008.10, P10008.

Borra, Erik and Bernhard Rieder (2014). "Programmed method: Developing a toolset for capturing and analyzing tweets". In: *Aslib Journal of Information Management*.

Bostock, Mike (2011). *D3.js*. https://d3js.org/. [Online; accessed 29-January-2021].

Bruns, Axel and Jean Burgess (2014). "Crisis communication in natural disasters: The Queensland floods and Christchurch earthquakes". In: *Twitter and society [Digital Formations, Volume 89]:* ed. by A Bruns et al. United States of America: Peter Lang Publishing, pp. 373–384.

Burgess, Jean and Ariadna Matamoros-Fernández (2016). "Mapping sociocultural controversies across digital media platforms: One week of# gamergate on Twitter, YouTube, and Tumblr". In: *Communication Research and Practice* 2.1, pp. 79–96.

Conover, Michael D, Bruno Gonçalves, et al. (Oct. 2011). "Predicting the Political Alignment of Twitter Users". In: 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, pp. 192–199. doi: 10.1109/PASSAT/SocialCom.2011.34.

Conover, Michael D, Jacob Ratkiewicz, et al. (2011). "Political polarization on twitter". In: Fifth international AAAI conference on weblogs and social media.

Csardi, Gabor and Tamas Nepusz (2006). "The igraph software package for complex network research". In: InterJournal Complex Systems, p. 1695. url: http://igraph.org.

Davis, Clayton A et al. (2016). "OSoMe: the IUNI observatory on social media". In: *PeerJ Computer Science* 2, e87.

DocNow (2020). *twarc*. https://github.com/DocNow/twarc. [Online; accessed 29-January-2021].

Free Software Foundation Inc. (2007). *GNU General Public License*. https://www.gnu.org/licenses/gpl-3.0.html. [Online; accessed 29-January-2021].

Gaisbauer, Felix et al. (2020). "How Twitter affects the perception of public opinion: Two case studies". In: *arXiv preprint arXiv:2009.01666*.

Gaumont, Noé, Maziyar Panahi, and David Chavalarias (Sept. 2018). "Reconstruction of the socio-semantic dynamics of political activist Twitter networks—Method and application to the 2017 French presidential election". In: *PLOS ONE* 13.9, pp. 1–38. doi: 10.1371/journal.pone.0201879. url: https://doi.org/10.1371/journal.pone.0201879.

Jänicke, Stefan et al. (2015). "On Close and Distant Reading in Digital Humanities: A Survey and Future Challenges." In: *EuroVis (STARs)*, pp. 83–103.

Jünger, Jakob and Till Keyling (2019). *Facepager*. https://github.com/strohne/Facepager. [Online; accessed 29-January-2021].

Leal, Wilmer et al. (2018). "Forman-Ricci Curvature for Hypergraphs". en. In: doi: 10.13140/RG.2.2.27347.84001. url: http://rgdoi.net/10.13140/RG.2.2.27347.84001.

Moretti, Franco (2000). "Conjectures on world literature". In: *New left review* 1, p. 54.

Myers, Seth A et al. (2014). "Information network or social network? The structure of the Twitter follow graph". In: *Proceedings of the 23rd International Conference on World Wide Web*, pp. 493–498.

Nitins, Tanya and Jean Burgess (2014). "Twitter, brands, and user engagement". In: *Twitter and society [Digital Formations, Volume 89]:* ed. by A Bruns et al. United States of America: Peter Lang Publishing, pp. 293–304.

Noack, Andreas (Feb. 2009). "Modularity clustering is force-directed layout". In: *Physical Review* E 79.2, p. 026102. doi: 10.1103/physreve.79.026102.

Paltoglou, Georgios and Mike Thelwall (2017). "Sensing social media: A range of approaches for sentiment analysis". In: *Cyberemotions*. Springer, pp. 97–117.

Peixoto, Tiago P. (2014). "The graph-tool python library". In: figshare. doi: 10.6084/m9.figshare.1164194. url: http://figshare.com/articles/graph_tool/1164194 (visited on 09/10/2014).

Pournaki, Armin (2020). *twitter-explorer*. https://github.com/pournaki/twitter-explorer. [Online; accessed 29-January-2021].

Rainie, Lee (2014). "The six types of Twitter conversations". In: Pew Research Center 20.

Rosvall, Martin and Carl T Bergstrom (2007). "Maps of information flow reveal community structure in complex networks". In: arXiv preprint physics.soc-ph/0707.0609.

APPENDIX

Stream vs. Search API

We investigate the difference between the Twitter Stream and the Search API. Using the keyword "clubhouse", we first collect tweets using the Stream API from Jan. 25th to Jan. 27th. We then launch the Twitter Search on Jan. 27th to see how many tweets we can collect until Jan. 25th. The tweet count over time is shown in Figure 5. The Search API provides about 80% of the tweets collected by the Stream API. In our example, 13% of the missing tweets in the Search corpus were original tweets and 13% were retweets.

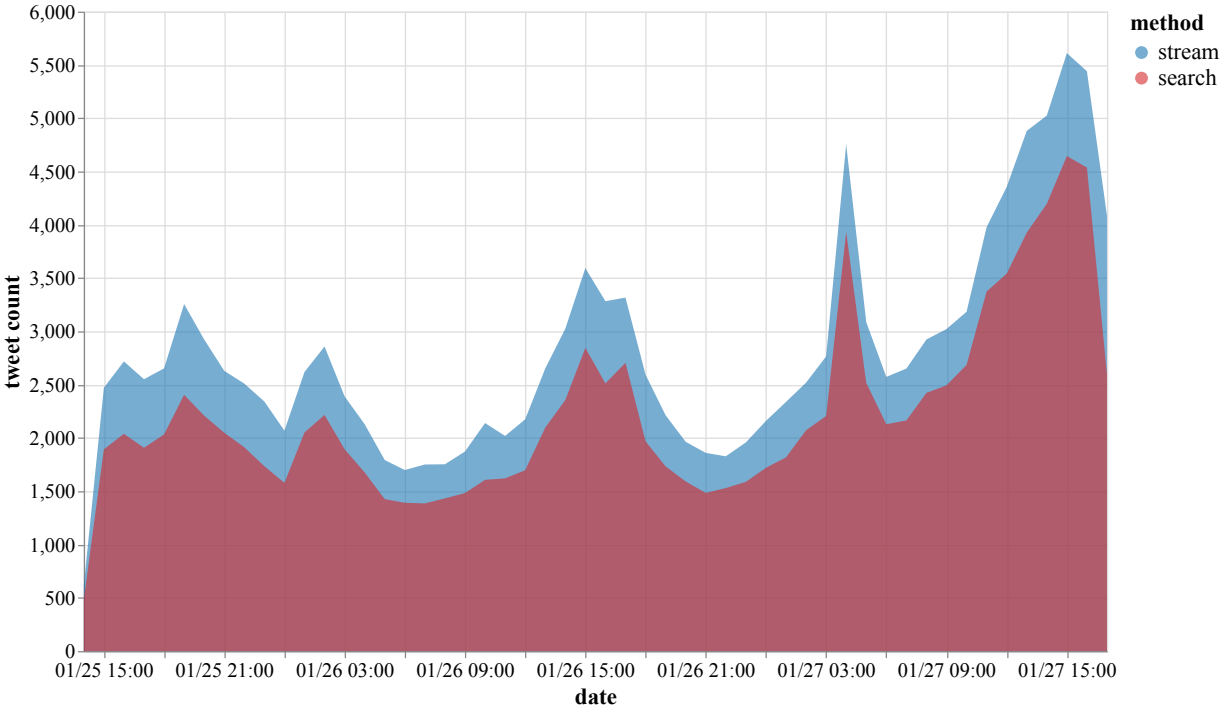

Figure 5. Streaming API vs Search API. We collected tweets using the keyword "clubhouse" for 48 hours using the search and the streaming API and observe that the Search API constantly returns less tweets than the Search API. Over the whole time range, the searched tweets make out 80% of the streamed tweets.

JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 1, 2021, 119–152

PRIVACY ATTITUDES AND BEHAVIORS IN THE AGE OF POST-PRIVACY: AN EMPIRICAL APPROACH

Nicolas Demertzis[a] [b], Katerina Mandenaki[a] [b] and Charalambos Tsekeris[b]

ABSTRACT

The digital world is a field of information and entertainment for users and a field of extraction of the most valuable good of recent years: personal data. How much of a threat to privacy is the collection and processing of data by third parties and what do people think about it? On the occasion of the extensive methods of surveilling citizens and collecting their data, this study attempts to contribute new empirical data evidence from the international research on the use of the Internet by the World Internet Project on attitudes and behaviors of individuals regarding online privacy and surveillance. The aim is to determine whether and to what extent the recorded concerns about the violation of privacy intersects with a growing acceptance of its very absence.

Keywords: World Internet Project; privacy; surveillance; social media; social capital

[a] National and Kapodistrian University of Athens.
[b] National Centre for Social Research (EKKE).

1 INTRODUCTION

From a free and decentralized research and communication tool, the internet has been transformed in recent years into a commodified space without which we can hardly imagine our lives. Various entities operate with a totally new business model, while major players such as Google, Amazon, Facebook, Apple, and Microsoft (GAFAM) offer innovative and mostly 'free' information, communication, sharing and access services, provided conveniently and quickly from the comfort of our home or wherever we are (de Bustos & Izquierdo-Castillo 2019). With a small exchange: they know who we are, when is our birthday, what are we searching for online, our employment, where we have been, what our faces - and those of friends and relatives - look like, what we believe in, even our political views (Curran, 2018; Smith, 2020; Nield, 2019; Norval & Prasopoulou 2017).

This study seeks to contribute with new empirical data to the investigation of citizens' attitudes, concerns and perceptions on issues of online privacy deriving from the World Internet Project in Greece (WIP-GR), implemented by the National Centre for Social Research (EKKE) [1] as part of the internationally collaborative World Internet Project (WIP).[2] The data related to concerns about privacy and online protection highlights a paradox, as these concerns are counterbalanced by the growing engagement of individuals in online experiences and their acceptance that there is no longer any privacy online: users tend to believe that having '*nothing to hide*' makes it acceptable to concede their data to companies or governments oblivious to the fate of those data.

According to the report by Tsekeris (et al. 2019) Greece is one of the allegedly weakest links of the EU Digital Single Market (DSM)[3] although the EU Digital Economy and Society Index (DESI) for 2020 indicates that the country made the most progress compared to the previous year (especially in connectivity and human capital)[4]. However, it is rather obvious that the so-called 'post-crisis Greece' has a long distance to cover compared to other countries. For 2020, the country, in overall, ranked again 27th out of the 28 EU Member States and still belongs to the low-performing group of countries along with Romania, Bulgaria, Italy, Poland, Hungary, Cyprus, and Slovakia. So, although Greece marginally improved its performance regarding its human capital and the supply side of digital public services, it is placed for one more year under the EU average. Nevertheless, Greeks are still considered to be active users of internet services with their number growing (OECD 2019). In addition, the progress in integrating digital technology has been slow. According to the 'eGovernment Benchmark 2019' [5], Greece is at 27% regarding the penetration of e-services, while the EU average is 57%. In the field

[1] https://www.ekke.gr/
[2] http://www.worldinternetproject.com/
[3] https://ec.europa.eu/digital-single-market/
[4] See full scoreboards here: https://ec.europa.eu/digital-single-market/en/scoreboard/greece
[5] https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2019-trustgovernment-increasingly-important-people

of digitization of public services, the country stands at 51%, far below the European average (68%). However, it seems that Greece has been provided with a significant boost from an unlikely quarter, that is, the coronavirus. The COVID-19 pandemic, the world's first digital pandemic and the ensuing lockdown acted as a catalyst as the country has indeed prompted a rush to adopt massive digital solutions for everything from Cabinet meetings to prescriptions (Stamouli, 2020).

But as in other countries, in Greece the pandemic has once again stirred up the debate on privacy issues. Numerous Greek scholars argue about the biopolitics of the pandemic and emerging anti-democratic tendencies (Douzinas, 2020; Kontiades 2020; Spourdalakis 2020) and collective-cultural drama (Demertzis 2020; Demertzis and Eyerman 2020). Others highlight the way governments, like in Hungary, pushed for authoritarian policies with accelerated procedures (Tzarelas, 2020: 315). In cases such as in Australia, China, Italy, Mexico, Singapore, South Korea, and the US, governments in collaboration with private companies, implemented even more generalized and indiscriminate methods of monitoring citizens and collecting data to observe the spread of the virus without them knowing (Tzogopoulos, 2020; Stein 2020; Singer & Sang Hun, 2020). Furthermore, elsewhere, e.g., in Israel, the government allowed the Secret Services to carry out mass surveillance in mobile phones without a court order to control the increase curve of COVID-19 cases (Gross, 2020). However, the sensitive data collected during this crisis were not only exchanged between health organizations and public health services, as Stein (2020) reveals, since in the US the public services activated applications and digital tools as well as location data from Google and Facebook providing these companies with access to confidential information of citizens such as the date they may have contracted the virus, along with their nationality, gender, age and location. Helbing (2020) notes the crisis seems to have pushed states not only towards obligatory testing, but also towards mass surveillance of data on health, on movement, on contacts, towards mass storage of such data, and potentially, later, towards immunity certificates. Apparently, millions of people are experiencing a bio-political condition that can potentially create new modalities of subjection and subjectivation[6]. It has to be noted, however that on various cases, democracies, especially in Western Europe, decided to preserve their citizens' privacy and informational self-determination [7].

In general, the digital life -in Greece and everywhere else- enmeshes with the multiple structural transformations associated with the rise and spread of the so called 'information and communicative capitalism' (Fuchs, 2012) or 'surveillance capitalism' (Zuboff, 2019). It is also related to the experience of late-modern subjects and societies, thus posing the urgent need for a far greater conscious-raising

[6] https://identitiesjournal.edu.mk/index.php/IJPGC/announcement/view/44

[7] In Germany for instance, as the latest debates and decisions on tracking applications for smartphones show, a new framework for the digital society is on its way – one based on decentralization, the right to maintain one's private sphere, and freedom to choose (Busvine & Rinke, 2020)

and awareness to the situated, cultural and sociopolitical contexts of its use (Fuchs, 2015). It is in the same spirit of critical inquiry that the collective and interdisciplinary World Internet Project (WIP) focuses on the specific national settings of internet use, with analytic attention on comparative and international perspectives. Hence, WIP examines the internet as something more than a global information machine or a communication medium. It emphasizes the cultural and sociopolitical dynamics of the constituent internet technologies, as well as the vast complexity of new types and processes of meaningful action, interaction, experience, subjectivity and identity formation that stretch across the turbulent digital world, especially after the triumphal advent of Web 2.0 or Social Web (Tsekeris & Katerelos, 2014). Emanating from WIP-GR, this paper, first, seeks to overview dataveillance and the datafication of society; second, it refers to the privacy paradox and the resignation of individuals to controversial practices of privacy violation despite them being aware of these violations; third, it attempts an explanatory approach to this contradiction through the exploration of social capital and the emotionality of the public sphere; fourth, it presents our analysis of the WIP-GR 2019 data related to privacy and surveillance and attempts to investigate three questions:

1. Does the level of internet engagement affect people's attitudes concerning their online privacy?

2. Do sociodemographic features predict people's attitudes towards online privacy?

3. Which variable predicts the 'I have nothing to hide' attitude?

Our results show that Greek people are on the track of a rather abrupt transition from digital users to digital citizens. The majority of the participants express their concerns about their privacy being violated as they actively try to protect it. However, more than half of the respondents state that they 'have nothing to hide'. We opted to investigate this conviction and we discovered that Greek people have a rather obfuscated idea about the very notion of digital privacy which might undermine their digital citizenship: they tend to identify it with being 'innocent' of controversial activities therefore being transparent and opening themselves up for datafication but still require protection from their government and expect it to exercise further regulation.

2 THIS DATAFICATION AND POST-PRIVACY IN THE ECONOMY OF CONNECTIVITY

Long before the outbreak of the global health crisis, the advent of social media has allowed companies to target specific groups of users and exploit not only their own data but also the data they generate (metadata) when sharing content or communicating with others (Fuchs, 2014). This 'dataveillance' allows governments and corporations to observe and surveil individuals for the purpose of an

unprecedented concentration of personal information and a form of control (Clarke, 1994), as the Snowden files revealed[8] (Lyon, 2014) or as the interviews with the former director of the US National Intelligence Service, Michael Hayden, describe (Hayden, 2014)[9]. This arguably confirms Christian Fuchs (2014: 92) that 'the actual practices of data marketing, control of media as well as corporate and state oversight restrict the liberal freedom of thought, opinion, assembly and association'.[10]

In the universe of GAFAM, a 'non-alternative' is introduced: providing the software and hardware foundations of the entire internet it is almost impossible for users not to engage with their products and services and not to give in to the cost of their 'free' offering: their data. In the '*platform capitalism*' (Srnicek, 2017) the new economy operates through connectivity as the main resource that marks a systemic shift in the process of profitability. As Mark Zuckerberg testified in 2018 to the U.S. Senate Examination Committee, the business model of Facebook and Google is to provide free services to users in exchange for their data. (Hsu & Kang, 2018; Watson, 2018).

Data monitoring and harvesting has been studied for decades (Rule et al. 1983; Clarke, 1994; Derikx et al. 2015). According to Lyon (2001a), the systematic attention given to people's lives is part of a broader process of maintaining social control and economic management, but in order to achieve this control, the boundaries between the private and the public must be blurred. Information technologies play a central role in this, minimizing the cost of obtaining personal information - without obvious social costs - and increasing 'information asymmetry' (Laudon, 1997; Acquisti et al. 2016). Therefore, the information mosaic of the digital selves is the basis of a relationship that goes beyond digitization and leads to datafication (van Dijck, 2014; Mai, 2016). If digitization allowed for greater storage and faster processing of information, datafication allows it to be transformed into shapes that can be quantified, classified, and analyzed in more sophisticated ways (Mayer-Schonberger & Cukier, 2013) in gigantic aggregations raising numerous issues[11]. As van Dijck (2014) notes, even academia has embraced the datafication paradigm by 'assessing big data sets collected through social media platforms as the most scrupulous and comprehensive method to measure quotidian interaction, superior to sampling ('N=all') and more reliable than interviewing or polling' and 'assuming a self-evident relationship between data and people'. What is missing though is that the allegedly 'objective' nature of quantitative analysis cannot exist without a qualitative, critical framing that guides the research with a quite subjective, intentional manner.

[8] https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi

[9] Hayden also commented that following September 11 the CIA "could be fairly charged with the militarization of the world wide web." (Peterson, 2013)

[10] cf. Fuchs, 2015· Cammaerts, 2008· Hindman, 2009· Mosco, 2009.

[11] Cf. ethics of information (Lyon, 2001b), legal issues (Schuster et al. 2017), identification of personal data (Fuchs 2012) exploitation of information for profit (Van Dijck, 2013)

It seems like there are two major starting points for this unprecedented information aggregation and control. First, it was the USA legislative statute known as Section 230 of the Communications Decency Act[12], which was crafted in 1996, during the initial phase of the public internet. It states that '*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*'. The aim of the statute was to clarify intermediaries' liability for the content on their websites, but it inevitably shielded website owners from lawsuits and state prosecution for user-generated content. Thank to this regulatory framework sites like Booking.com can defend even aggressive negative hotel reviews and Twitter and Facebook allow trolls and fake news to 'roam free' without either company being held accountable to the same standards that news organizations are. As it institutionalized the idea that websites are not publishers but rather 'intermediaries', this statute not only freed them from the responsibility of their content (or its providers), but it ended up sheltering the extractive operations of this very content from critical examination. The second milestone came six years later, in the aftermath of the September 11th attacks in USA, when the government's concerns shifted from online privacy protections to a new need for 'total information awareness' (Rosen, 2002) as an unwritten policy of 'surveillance exceptionalism' (Zuboff, 2019) emerged. Legislation to regulate online privacy became a casualty of the 'war on terror', the 'goods' produced in Silicon Valley evaded legislative action and became highly coveted as was the need for higher speed in clandestine digital services.

Harvesting data is not a novel phenomenon (Flick, 2016). What is new is the extent of exposure of this data and how it can be aggregated and transformed uncontrollably (Van Dijck, 2014; Mai 2016). In 2019, the French Commission for the Protection of Personal Data (CNIL) fined Google €50 million for violating EU privacy rules, 'for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization'[13]. Earlier, on the other side of the Atlantic, an investigation by the *Observer* and the *New York Times* revealed that 50 million Facebook user profiles were processed by Cambridge Analytica, creating a program that could predict and influence their electoral behavior sending them targeted and personalized messages based on their data[14]. Moreover, the same investigation revealed that in addition to the US election, the same method was used to manipulate the results of the 2016 British referendum that led Great Britain

[12] Section 230 of the Communications Decency Act, Electronic Frontier Foundation, https://www.eff.org/issues/cda230.

[13] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc; See also https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog

[14] According to information provided by Christopher Wylie the whistleblower that uncovered the story: "we exploited Facebook to collect millions of user profiles and create models to tap into what we knew about them and target their inner demons." Cf. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

to the infamous Brexit pivoting for the first time the whole dataveillance undertaking from commercial to political objectives.

This kind of targeted advertising invented by Google (Zuboff, 2019: 67) paved the way to economic success but also laid the foundation of a 'surveillance capitalism' with 'idiosyncratic economic imperatives defined by extraction and prediction, a 'unique approach to economies of scale and scope in raw-material supply'. Surveillance capitalism begins by unilaterally making a claim to private human experience as free 'raw material' for transformation into behavioral data, making data the very element tech giants may assert authority over -the same way oil companies assert authority over crude- in order to achieve economies of scale in its raw material supply operations. And in transforming 'crude' data into information 'gasoline', GAFAM's machine intelligence operations convert human experience into the firm's highly profitable algorithmic products designed to predict the behavior of its users (Zuboff, 2019).

Profits in the 'attention economy' (Davenport & Beck, 2013; Boyd & Crawford, 2012) comes from the customization and personalization of the information extracted, thus influencing people's attention, emotions, and behaviors (Demertzis & Tsekeris, 2018). The combination with other communication techniques such as neuromarketing (Zurawicki, 2010; Ariely & Berns, 2010), neurobranding (Steidl 2012) or automated social media bots (Shorey & Howard 2016), may generate very effective propaganda, manipulate or even deceive. The ongoing debate about fake news and post-truth society (Keyes, 2004; McIntyre, 2018) as well as post-democracy (Crouch, 2004) can be conducted under a new light in this 'post-privacy' era (Heller, 2011).

Moreover, as today's advertisement is capitalizing on digital technologies to dig further into the needs, interests, and motivations of customers, behavioral advertising, online profiling and 'behavioral targeting' while being shielded from any accountability as to the nature of the content targeted, have become common tactics for suppliers to effectively sell products to customers in the digital environment. Especially in cases of electoral choice, adding to personal profiling based on user activity and interests, 'affinity profiling' (Wachter, 2020) classifies people based on their assumed interests according to groups they supposedly belong to, thus providing online platforms with sensitive information such as ethnicity, gender, sexual orientation or religious beliefs. What is called 'affinity profiling', or profiling which seemingly does not directly infer sensitive data but rather measures an 'affinity' with a group defined by such data (Wachter, 2020), not only violates privacy but might even unlawfully discriminate against users who receive inadequate legal protection as groups. A violation which could undermine the application of the EU General Data Protection Regulation (GDPR) against processing of sensitive data.

3 THE 'PRIVACY PARADOX' AND THE NON-PRIVATE NATURE OF PRIVACY

These practices do not seem to prevent people from using the internet, accepting cookies when visiting a website or participating in social media (Ngwenyama & Klein 2018, Van Dijck 2013). Norberg et al. (2007) coined the term 'privacy paradox' to describe the dichotomy between individuals' willingness to concede their data with almost negligible rewards and their expressed concerns about the violation of their privacy (Kokolakis, 2017). The bloodless 'coup' that has been inflicted on modern societies by digital moguls relies, 'on the most treacherous hallucination people have: that 'privacy is private' (Zuboff, 2021). And giving away or conceding a bit of personal information is a fair 'quid pro quo' if users can get extra service. For example, when Delta Air Lines piloted a biometric data system at the Atlanta airport, the company reported that of nearly 25,000 customers who traveled there each week, 98 percent opted into the process, noting that 'the facial recognition option is saving an average of two seconds for each customer at boarding, or nine minutes when boarding a wide body aircraft.' (Zuboff, 2020; Murgia, 2019). Privacy is not private, because the effectiveness of all private or public surveillance and control systems depends upon the pieces of ourselves that we give up -or that are secretly taken from- even through seemingly innocent micro-activities such as clicking on an angry emoji under a disliked post on Facebook: opinions are collected, assessed and treated as property. And that transaction takes place in a totally asymmetrical distribution of knowledge, as tech giants have control of information and learning whereas a significant number of people have trouble figuring out how to pay their bills online. Unequal knowledge about people produces unequal power over them. And from algorithms that profile people to predict their behavior, surveillance capitalism is reaching a point where predictive knowledge is morphing into modification power as was shown in Facebook's contagion experiments (Bond et al., 2012; Kramer at al., 2014), when it succeeded in modifying human behavior by planting subliminal cues and manipulating social comparisons on its pages, to influence users to vote in midterm elections and to make them feel sadder or happier.

So where does all this leave users' privacy? In an experimental study, Carrascal (et al. 2013) found that internet users priced their internet search history information at around 7 euros, while Egelman (et al. 2012) showed that consumers were willing to pay a price to buy the protection of their privacy but it was a small one.[15] Earlier research on user attitudes indicated that privacy and the collection of information is something that particularly concerns users (TRUSTe 2014; Madden 2014) although they can give it away as soon as they realize there is something to gain (Brown, 2001; Spiekermann et al. 2001). Taddicken (2014) showed that privacy concerns do not affect self-disclosure if the communication pattern between users is performed on an exchange basis like '*tell me about you and I will tell you about*

[15] Users were not willing to pay more than $ 1.50 to 'buy' the security of their privacy.

me' or includes the benefit of shareability (Lee et al. 2013). Zafeiropoulou (et al. 2013) investigated users' attitudes about their location data and discovered that even in this case that concerns a particularly sensitive information,[16] users willingly reveal it or provide constant access to it in exchange for participating in an internet activity or enjoy a free service. Ngwenyama & Klein (2018) argue that the compliance of individuals with controversial practices of privacy violation is due to a voluntary 'amnesia' and a lack of awareness related to the confusing nature of social media surveillance practices. They concluded that data monitoring, control and financial exploitation involve ethical contradictions, covert purposes, agendas and ideology.

Examples like that lead to what Draper & Turow (2017) call 'digital resignation', arguing that the very notion of the '*privacy paradox*' is faultily burdening users: people do not give up personal information just to get discounts or services nor do they lack comprehension for the consequences of that disclosure. They do so because they are accepting as inevitable the undesirable ways marketers use personal information and resign to them. A purposeful strategy of commercial interests and not an accidental byproduct of 21st century digital life, 'digital resignation' is something to investigate on multiple institutional and societal levels and understand its nature and origins. Internet users cannot learn enough about privacy risks to make informed decisions about their privacy as it is impossible to gain sufficient knowledge of the ways in which personal data are processed and analyzed by thousands of organizations and numerous obscure techniques. The advent of large-scale 'Big Nudging' (Helbing, 2015) and 'Big Data surveillance' (Lyon, 2014), has established omnipotent technologies of control, calculability and prediction (Kucklick, 2014), which, produces unprecedented power asymmetries between the state and its citizens, (Brunton & Nissenbaum, 2015) and corporations and their customers. According to the JRC Science for Policy Report of the European Commission (2020)[17], companies use several questionable techniques like *defaults*, *framing*, *nudging* and *dark patterns* to build choice architectures and dissuade users from making active or informed choices leading not only to the sharing of personal information but to manipulation and deception. For instance, framing and wording may be used to nudge users towards a choice by presenting the alternative as risky (e.g., on Facebook, users are encouraged to keep face recognition turned, because it ostensibly helps 'protect you and others from impersonation and identity misuse and improve platform reliability.')[18]. Choice architectures may also require a take-it-or-leave-it decision, like a choice between accepting specific privacy terms or deleting an account. They may even be designed

[16] Although geolocation data are not considered "sensitive" in a legal point of view they are personal and of importance to the safety of users providing very intimate and accurate overview of their habits and patterns. Retaining location data forever and obtaining a single privacy consent for multiple purposes are practices already unacceptable. https://iapp.org/news/a/what-the-gdpr-will-mean-for-companies-tracking-location

[17] https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/technology-and-democracy

[18] https://www.facebook.com/help/122175507864081

in such a way that the privacy-friendly option requires more effort and knowledge from users. The very task of trying a 'self-managed privacy' is futile so long as the various decisions people must make about their privacy and the tasks they must do regarding it (reading privacy policies, opting out, changing privacy settings etc.) make it a complex and never-ending project (Solove, 2013; 2020). Resignation is a rational response to the impossibility of privacy self-management rather than a voluntary servitude.

4 SOCIAL CAPITAL IN THE EMOTIONAL PUBLIC SPHERE

There is a number of further aspects influencing users' interest in protecting their privacy on the Internet, their attitude towards others and the very ability to be anonymous online. Active participation in social networks associated with self-disclosure is related to three needs: the need for entertainment, for social relationships and the need to construct identity (Debatin et al. 2009). For most users, meeting the above needs outweighs the risks of personal data exposure and privacy violation by responding to a 'ritualistic' integration of online socialization. Social networking is a way of gaining social capital (Ellison et al. 2011) that is exchanged for the disclosure of personal information[19]. Demertzis & Tsekeris (2018: 16) note that the tools and control mechanisms involved in the 'governmentality of the neoliberal debt economy' create new emotional rules, informalize behaviors and compose an emotional public sphere in which people, freed from the constraints of the past, express themselves freely following the track of the '*emancipation of emotions*' (Wouters, 2007). If the concession of private information is the cost of engaging networked but disconnected individuals in the 'emotional public sphere' where narcissistic disclosure of emotionality takes place in the name of '*authenticity of the self*' (Sennett 1993), then the benefit may be considered great.

It seems, however, that people are beginning to doubt the data-for-free-services-exchange they have involved themselves too. According to Pew Research Center[20], 81% of Americans believe the potential risks of companies' data collection outweigh the benefits but they have no comparable alternatives of living their digital lives (Auxier et al. 2019). So, where do Greek people place themselves in this landscape of distorted digital communication?

[19] Stutzman et al (2012) have shown that if a person reveals a medical problem, they are more likely to attract sympathy and support from members of their network.

[20]https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

5 WIP-GR SURVEY: SAMPLE DESCRIPTION AND DATA DEFINITIONS

The third wave of WIP-GR[21] was implemented in Spring 2019 by the National Centre for Social Research (EKKE)[22] as part of the international World Internet Project (WIP). WIP is a major survey-based research program, launched in 1999 and directed by the Annenberg School Center for the Digital Future at the University of Southern California, looking at the social, political and economic impact of the internet, as well as at how individuals adopt and use the internet and other new technologies, and what implications this has on their everyday lives and communities. This program becomes increasingly important because in order to get closer to the kind of internet we want, 'we need a better understanding of the internet that we have' (Bernal, 2018: 2).

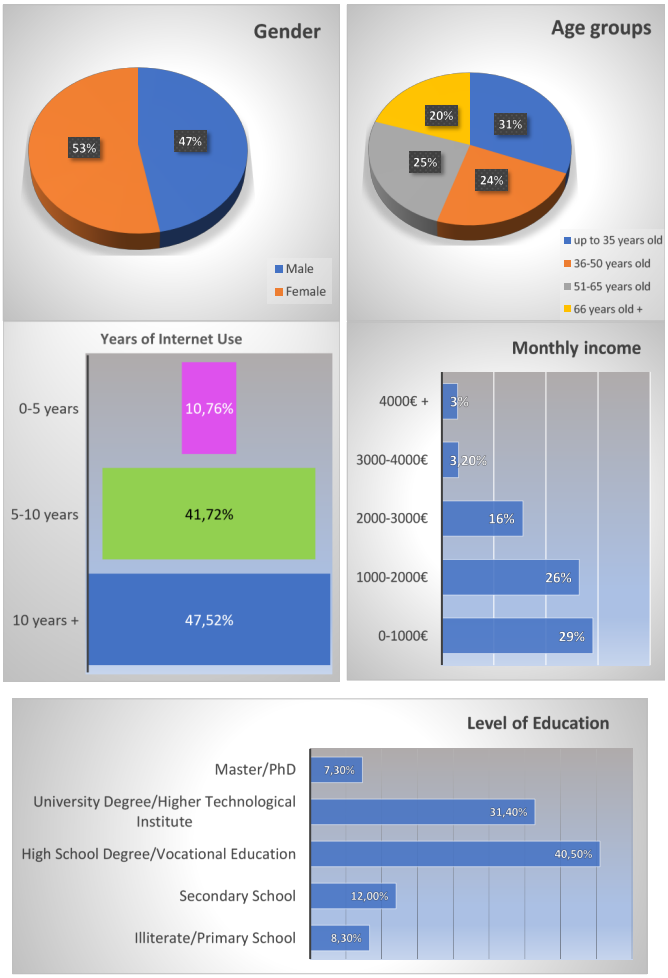

Figure 1: Demographic features

[21] The first wave of the survey in Greece was conducted in November and December 2015, and the second between 31st January and 21st February 2017. The present study offers a comprehensive presentation of the empirical results of the third wave of the survey, which was conducted between 12th April and 23rd May 2019.
[22] https://www.ekke.gr/

The research methodology was designed by EKKE and 1,208 interviews were conducted by using a structured questionnaire via CATI by trained interviewers from EKKE's Web Lab. The data were collected 12 April – 23 May 2019 and cleaned accordingly. [23] There are several modules in the questionnaire explored for the purpose of this study. The demographic variables we utilized are: Gender, Age, Education, Internet use experience and Monthly income (See Figure 1).

In the total sample both genders (women 52% - men 47%) were almost equally represented while the age span of the participants was from 15 to 97 years. Almost half the respondents are early Internet users with 10+ years of experience. The majority of the participants have either High School diploma or vocational training and one third possess a University degree. Finally, half our respondents are economically located in the lower to middle income levels with a minority of 6% stating a higher financial status.

6 RESEARCH QUESTIONS AND METHODOLOGY

To clarify privacy attitudes among Greek users, we followed a two staged strategy. First, we investigated what Greek uses are more concerned about presenting metrics on 5 statements measuring privacy attitudes and 4 statements [24] measuring respondents' perceived safety for exercising their freedom of speech online. On the second part of our research, we analyzed our data. First, we created scales to measure internet engagement and social media use in order to investigate the degree to which online convenience and gaining social capital affect peoples' attitudes. Second, we correlated the scales and the sociodemographic characteristics of our users with their attitudes. Finally, we opted for an interpretation of the '*I have nothing to hide*' attitude to determine whether it is an indication of digital resignation that justifies a more submissive attitude on behalf of our participants. The above are tested in the following research questions:

Q1: Does the level of internet engagement affect people's attitudes concerning their online privacy?

Q2: Do demographic features predict people's attitudes towards online privacy?

Q3: Which variables predict the attitude 'I have nothing to hide'?

[23] The dataset was weighted according to the 2011 Population Census and the Labor Force Survey.
[24] The statements were measured on a 5 grade Likert scale from "strongly agree" to "strongly disagree".

7 FINDINGS: PRIVACY ATTITUDES AND CONCERNS

7.1 Privacy concerns-descriptive statistics

As can be seen in Figure 2, 54% of the respondents claim that '*There is no privacy, accept it*', whereas only 23% somewhat and strongly agree with the statement that '*concerns about online privacy are exaggerated*'. Almost 60% of the users feel they '*can control*' their privacy online, and 70% state that they '*actively protect*' it. Furthermore, we observed a dichotomy between the meaning the majority of the respondents' attributes to the statement *I have nothing to hide* (55,8%) and their strong concerns about their privacy being violated by corporations (75.6%), the government (60.8%) and other people (62.2%).

*Figure 2: Privacy Concerns and attitudes**

In the WIP-GR survey the biggest concern about online privacy being violated is about *corporations* which is probably explained by the fact that most users often receive targeted advertisements and several digital marketing products. It is not enough for a company like Facebook to store 300 million photos or record the 2.7 billion likes that are clicked daily; using several algorithms, it mines this data, processes, and combines them committing 'abuse through transformation' (Schyff et al. 2018; Smith (2016).

Another concern for 62% of the respondents is about governments. Governments surveil citizens and collect information and data to deal with cybercrime, fraud, terrorism, or other violations (Amoore & De Goede 2005), to establish a more efficient bureaucracy or to control immigration. As shown in

Figure 3, the WIP-GR research participants express caution and an underlying awareness.

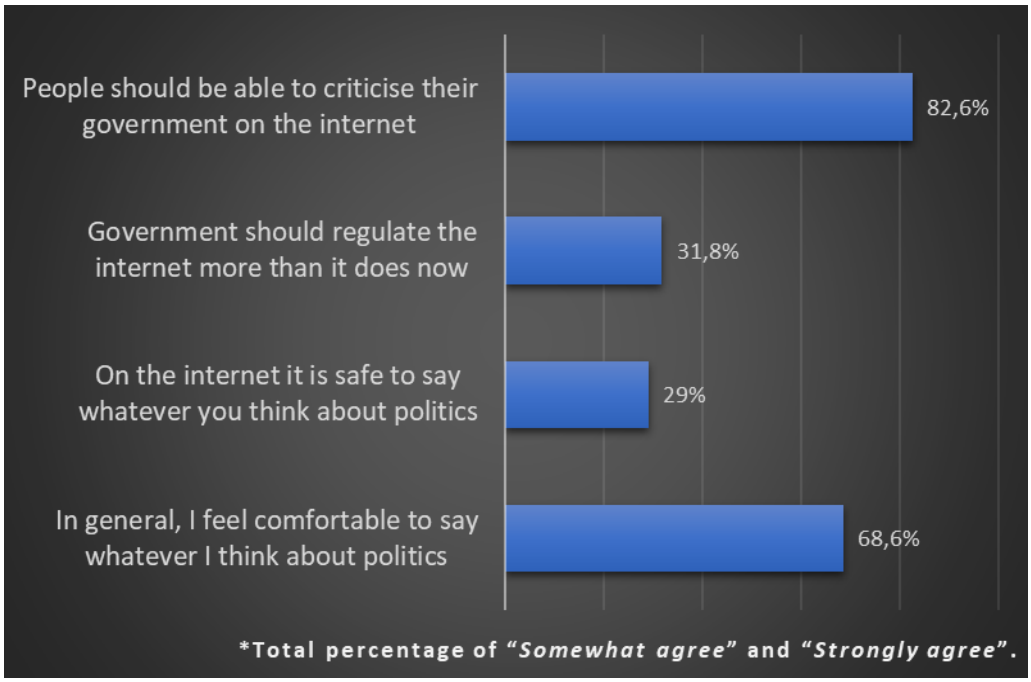

*Figure 3: Freedom of Speech**

The grand majority hold that '*people should be able to criticize their governments online*' (86%). Fewer respondents state that they feel '*comfortable saying whatever they think about politics*' in general (68%) -admittedly denoting a significant degree of freedom of speech in Greece- however, much fewer believe that the internet is a safe place to express political ideas (27,20%). In the same vein, more than four out of ten people (48%) reject potential increase of internet regulation by the government. Apparently, participants believe that the internet ultimately involves the risk of exposing their political profile both to centers of power that may be surveilling them and to opposers who may be attacking. Political cyberbullying is a raising issue in various online communities (Bauman, 2019), while in the American elections of 2016 the phenomenon was seriously escalated especially due to the inflammatory rhetoric of Presidents' Trump campaign.[25]

In addition to companies and governments, personal data are also being coveted by other individuals with controversial goals, mainly of a delinquent nature, such as identity theft, bank robbery, blackmail, or harassment, a danger that concerns 63% of Greek users. Apparently, users' concerns about the violation of their data by other individuals are associated with 'social privacy' which differs from 'institutional privacy' and violations by companies or governments (Park et al. 2018). In short, collecting and processing data from the socio-economic background of users for the purpose of profit or control does not seem to bother them as much as e.g., having to deal with embarrassing photos being posted on

[25] www.sciencedaily.com/releases/2019/01/190109090917.htm

Facebook by a malicious person. This is an indication of a cognitive dichotomy, given that users worry about something they haven't really experienced while high rates of concerns about violations by others indicate that the issue of privacy appears to be a matter of infringement, criminal activity or social exposure and ashaming. It is also likely that respondents have not assessed several mundane cases as indicative of privacy violations, like targeted ads or recommendations to rate restaurants or cafes as soon as they exit them.

8 ANALYSIS

8.1 Q1: Does the level of internet engagement affect people's attitudes concerning their online privacy?

We implemented twenty-two variables and conducted an exploratory factor analysis (Floyd & Widaman, 1995; Gorusch, 1990) to develop scales that would measure peoples' level of internet engagement (deVellis 2003). We used principal axis factoring (Worthington & Whitaker 2006) with Promax (orthogonal) rotation. To estimate the contribution of specific socioeconomic variables to respondents' attitudes, we focused on gender, age, monthly income, and education level and implemented multinomial logistic regression (Gould, 2000; see also Papadoudis 2018). Ordinal regression analysis was used to determine what are the convictions of people who believe they have *nothing to hide.*

The analysis yielded three factors explaining a total of 47,266% of the variance for the entire set of variables (see Table 1). Factor 1 was labeled 'O*nline Sociability*' due to the high loadings by items such as: frequency of posting content, sharing content, instant messaging and phone calls online, maintaining relationships, create relationships, download videos and music. The second factor was labeled '*Internet use Frequency*' due to the high loadings by items concerning how often users go online for several activities e.g., to get information about a product, buy things, make travel reservations, pay bills, etc. The third factor was labeled '*Internet Proficiency*' because the 4 items that loaded onto it were related to the users' self-declared level of knowledge of performing tasks on the internet and their ability to effectively navigate it. The KMO score (0,843) and Bartlett's Test of Sphericity ($p<0,001$) both indicate that the set of variables is well related. We tested the internal consistency of the items by computing the Cronbach's a score for each factor. Finally, we attributed Anderson Rubin scores (Mean = 0, Variance of 1) to create 3 new variables labeled *Online Sociability scale*, *Internet Frequency Use scale* and *Internet Proficiency scale. (Table 1).*

Table 1: Factor Analysis - Internet engagement scales

	Loadings			***Communality***
	Factor 1: Online sociability (*Cronbach's a =0.837*)	Factor 2: Internet Frequency use (*Cronbach's a= 0.787*)	Factor 3: Internet Proficiency (*Cronbach's a =0.901*)	
Instant messaging	0,711		0,565	0,536
Post your own content (videos, photos etc.)	0,689		0,436	0,477
Maintain your relationship with people with a similar social status	0,681			0,464
Re-post or share links or content others have created	0,642		0,406	0,415
Keep your existing relationships with family/friends	0,576			0,342
Make or receive phone calls over the Internet	0,568			0,323
Download or watch videos	0,537			0,300
Find people of a similar social status	0,499			0,261
Download or listen to music	0,493			0,255
Get information about a product		0,673		0,453
Buy things online		0,661		0,443
Compare prices of products/services		0,572		0,332
Make travel reservations/bookings		0,562		0,318
Look for travel information		0,501		0,253
Pay bills online		0,480		0,236
Find or check a fact		0,479		0,242
Look up a definition of a word		0,435		0,221
Look for news (local, national, international)		0,409		0,169
I know how to create content and upload to the internet	0,562		0,920	0,851
I know how to adjust it to what share content online	0,550		0,891	0,799
I know how to download applications on a mobile phone or tablet	0,435		0,749	0,563
I know how to open a file downloaded from the internet	0,413		0,723	0,543
Eigen value	6,350	2,397	1,652	
% of Total Variance	28,862	10,897	7,508	
Total Variance			47,266	

We created these scales to examine if online sociability, frequency of use and internet proficiency affect people's attitudes towards privacy concerns. We hypothesized that people who score high in online sociability and internet frequency use would be more willing to declare their concerns as conscious users but still exhibit a dichotomy since they are the ones to benefit most from internet's free services and activities. So, we performed a one-tail Pearson correlation to see also the direction. According to the results shown in Table 2 there is a significant deviation in people who score higher in the frequent use scale to be more concerned about corporations violating their privacy online. Another notable finding is people who score highly in both online sociability and internet proficiency tend to disagree with the notion '*I have nothing to hide*' indicating that their involvement in the internet's allure has in fact instilled in them the idea that wanting to be private doesn't mean that you hide something. However, respondents who scored highly on the internet proficiency scale is the only group that disagrees with the statement '*there is no privacy accept it*'. This is a good indication that the 'connoisseurs' understand two things: a) there are ways to protect ones' digital privacy and they probably know about them and b) they are not inclined to yield to the easy refuge of admitting that since there is no privacy online there is nothing we can do other than conceding private information to enjoy free services and social capital. Digital 'socialites' also tend to disagree with this statement but not significantly.

Finally, while initial results showed that the majority of the respondents disagree with the statement '*on the Internet, it is safe to say whatever you think about politics*' (48,3%)[26], if we look closer to the respondents who score high in all three scales, they are most likely to agree with this statement. Being 'safe' to express political views online is not only about evading government surveillance, it also concerns being able to post opinions and participate in online discussions without being bullied. So, respondents who are highly engaged with the internet, possibly are not so concerned of being surveilled by the government rather than being able to handle online bulling and the emotionally charged spaces were politics might be discussed. However, all types of users, socialites, frequent users and connoisseurs tend to disagree with the statement that the '*governments should regulate the internet more than they do now*', an indication of sharing the libertarian culture of netizens initiated already at late 1990s.

[26] Total percentage of "Somewhat disagree" and "Strongly disagree".

Table 2: Correlations between internet engagement and privacy attitudes and behaviors

		Online Sociability Scale '*socialites'*	Frequency use scale '*frequent users*'	Proficiency scale '*connoisseurs'*
Privacy violations by Governments	Pearson r	0,021	0,052	-0,029
	Sig.	0,271	0,068	0,203
Privacy violations by Corporations	Pearson r	0,049	,134**	,066*
	Sig.	0,080	*0,000**	*0,030**
Privacy violations by Other people	Pearson r	-0,020	0,007	0,012
	Sig.	0,287	0,423	0,366
I actively protect my privacy online	Pearson r	0,033	0,023	0,040
	Sig.	0,170	0,255	0,128
Concerns about privacy online are exaggerated	Pearson r	-0,027	-0,020	-0,021
	Sig.	0,216	0,282	0,272
I have nothing to hide	Pearson r	-,101**	-0,016	-,086**
	Sig.	*0,002**	0,320	*0,007**
I feel I can control my privacy online	Pearson r	-0,043	-0,056	-0,008
	Sig.	0,107	0,055	0,410
On the Internet, it is safe to say whatever you think about politics	Pearson r	,138**	,094**	,133**
	Sig.	*0,000**	*0,004**	*0,000**
The government should regulate the internet more	Pearson r	-,089**	-0,053	-,115**
	Sig.	*0,006**	0,067*	*0,001**
There is no privacy, accept it	Pearson r	-0,004	0,015	-,058*
	Sig.	0,449	0,329	*0,048*

***. Correlation is significant at the 0.01 level (1-tailed). *. Correlation is significant at the 0.05 level (1-tailed).*

8.2 Q2: The demographics of online privacy concerns

The theme for this analysis is centered on four demographics and the three constructed scales of internet engagement to examine if these parameters can predict the respondents' privacy attitudes and concerns. For the estimations in Table 3 we implemented multinomial logistic regression reporting coefficients and odds ratios (OR). Each OR takes values higher than 0 and lower or higher than 1 which is the focal point (a value of 1 means that there is no contribution of the variable). Values below or above 1 may also interpret the direction of the attitudes according to which group is set as the reference group. In this case the reference category was *Disagree* because we wanted to use it as a baseline. The regression was performed to model the relationship between the predictor variables and participation in the three response groups (Agree, Disagree and Neither/nor Agree/Disagree). The predictive variables were all treated as covariates. The general significance of the model is good as shown both by the p value ($p<0,005$) in most cases and the χ^2 test. Therefore, the variables contribute to explain the essence of the privacy attitudes and representations of the respondents[27]. There are interesting results coming out of our explorations:

[27] It should be noted that due to the realistic nature of our data there were cases of missing values which we are reporting in the footnote of Table 3.

Concerning gender, women tend to declare they 'actively protect their digital privacy' more prominently than men and they also tend to believe that they 'feel they can control their privacy online'. Women also appear to have given in the 'nothing to hide' concept as they tend to agree with this statement more than men although they do not believe that the internet is a safe place to discuss politics as strongly as men.

The factor of age only seems to affect people's perception about 'having nothing to hide' as they grow older therefore showing a mild positive direction to the statement as younger people appear more strongly in the Disagree side of the statement. We could hypothesize that older individuals, when presented with this statement, might perceive it as a challenge to their personal idea of dignity (they have done nothing wrong) rather than a challenge to their privacy.

The economic status of the respondents seems to significantly affect their efforts to 'actively protect their privacy', the odds ratio of being in the 'Agree' group rather than the' Disagree' are multiplicatively increased by 1,342. Also, the higher the income the less likely is the respondent to agree with the statement that governments violate online privacy (B=-0,230). However, their efforts to actively protect their privacy must be considered along with their significant agreement with the statement that 'there is no privacy online accept it' (OR=1,219), a statement that is mostly rejected by respondents who scored highly on the internet proficiency scale, as was also seen previously in the correlations (Table 2).

An interesting result derived from the variable of education as people of lower educational levels state they more actively protect their privacy online (Figure 6) than the more educated users possibly because people with higher education may realize that actively protecting their privacy will not essentially protect them from violations, since they don't feel they can control it as indicated by the negative coefficient (B=-0,227). However, people with higher education tend to disagree with the statement 'concerns about online privacy are exaggerated' (Figure 7) whereas people with lower education tend to populate in higher percentages the 'Agree' and 'Neither/nor' area of the discussion.

People with higher internet proficiency scores significantly agree with the statement that it is safe to discuss politics online (B=0,275, p=0.004) but they reject the idea that governments should regulate the internet more, as indicated by the negative coefficient (B=-0,288, p=0,036) in the Agree category. 'Connoisseurs' don't believe that there is no privacy online (B=-0,426, p<0,01) however people with higher online sociability scores seem to have accepted this idea (B=0,255, p=0,019).

Table 3: Multinomial logistic regression

Parameter Estimates

Privacy violations by Governments[a] [(x2(14)=26.244, p=0.024)]					I have nothing to hide[f] [(x2(14)=31.707, p=0,04)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	-0,230	0,092	0,013	0,794	0,197	0,101	0,051	1,218
Age	-0,159	0,117	0,175	0,853	0,385	0,131	0,003	1,470
Gender	0,015	0,193	0,937	1,015	0,400	0,202	0,048	1,491
Level of Education	0,163	0,131	0,212	1,177	-0,127	0,136	0,351	0,881
Online sociability	-0,021	0,118	0,857	0,979	0,010	0,123	0,936	1,010
Internet frequency use	0,198	0,190	0,296	1,219	0,111	0,193	0,564	1,118
Internet Proficiency	-0,195	0,140	0,166	0,823	-0,071	0,144	0,621	0,931
Privacy violations by Corporations[b] [x2(14)=21.708, p=0,08]					I feel I can control my privacy online[g] [(x2(14)=16.131, p<0,001)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	-0,102	0,126	0,417	0,903	0,181	0,103	0,079	1,199
Age	-0,021	0,159	0,895	0,979	0,189	0,131	0,151	1,208
Gender	-0,194	0,258	0,453	0,824	0,422	0,206	0,040	1,525
Level of Education	0,414	0,174	0,017	1,513	-0,227	0,139	0,104	0,797
Online sociability	-0,087	0,155	0,576	0,917	0,014	0,124	0,911	1,014
Internet frequency use	0,116	0,252	0,643	1,124	-0,209	0,193	0,281	0,812
Internet Proficiency	0,203	0,176	0,248	1,226	0,195	0,143	0,173	1,215
Privacy violations by Other people[c] [(x2(14)=9.189, p=0,819)]					On the Internet, it is safe to say whatever you think about politics[h] [(x2(14)=25,698, p=0,029)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	-0,046	0,103	0,652	0,955	0,129	0,088	0,145	1,138
Age	-0,237	0,128	0,063	0,789	-0,071	0,114	0,534	0,932
Gender	0,176	0,210	0,402	1,193	-0,634	0,184	0,001	0,531
Level of Education	0,105	0,141	0,458	1,111	-0,116	0,123	0,345	0,890
Online sociability	-0,053	0,126	0,676	0,949	0,143	0,112	0,201	1,154
Internet frequency use	-0,134	0,201	0,506	0,875	0,106	0,175	0,546	1,112
Internet Proficiency	0,041	0,146	0,779	1,042	0,275	0,134	0,040	1,317
I actively protect my privacy online[d] [(x2(14)=26.033,p=0.026]					There is no privacy, accept it[i] [(x2(14)=40.593, p<0,001)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	0,270	0,117	0,021	1,310	0,157	0,089	0,078	1,170
Age	0,175	0,142	0,217	1,191	0,090	0,111	0,417	1,094
Gender	0,452	0,227	0,046	1,571	-0,100	0,179	0,576	0,905
Level of Education	-0,376	0,154	0,015	0,687	0,018	0,123	0,885	1,018

Online sociability	0,096	0,133	0,471	1,100	0,255	0,109	0,019	1,290
Internet frequency use	0,154	0,216	0,477	1,166	0,076	0,174	0,662	1,079
Internet Proficiency	0,242	0,152	0,112	1,274	-0,426	0,130	0,001	0,653

	Concerns about privacy online are exaggerated[e] [(x2(14)=24.258, p=0,043)]				The government should regulate the internet more than it does today[j] [(x2(14)=25.658, p=0,029)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	0,099	0,098	0,310	1,105	0,057	0,094	0,541	1,059
Age	0,107	0,124	0,387	1,113	-0,045	0,122	0,711	0,956
Gender	-0,144	0,202	0,477	0,866	0,199	0,192	0,299	1,221
Level of Education	-0,356	0,136	0,009	0,700	-0,277	0,129	0,032	0,758
Online sociability	0,081	0,123	0,509	1,084	-0,019	0,117	0,869	0,981
Internet frequency use	0,082	0,192	0,668	1,086	0,187	0,184	0,308	1,206
Internet Proficiency	-0,043	0,142	0,759	0,958	-0,288	0,138	0,036	0,750

** Significance at the 0.05 level. p≤,005.*

a. Missing=558,36. b. Missing=553,53. c. Missing=555,51. d. Missing = 550,74. e. Missing=551,36. f. Missing= 548,46. g. Missing=550,63. h. Missing=553,92. i. Missing=551,38. *J*. Missing=573,69.

8.3 Q3: Which variable affects the attitude '*I have nothing to hide*'?

So far, the '*I have nothing to hide*' attitude was not explained by any variable, therefore, in order to determine which factors are incorporated in this particular attitude we performed an ordinal regression analysis between the attitudes themselves to determine what are the convictions of people who believe they have *nothing to hide*. As shown in Table 4 the model seems good ([$\chi^2(18)=98.760$, $p<.001$] and it provides us with three significant results deriving from the 'Disagree' category:

1) The attitude '*concerns about online privacy are exaggerated*' was a significant predictor of '*I have nothing to hide*' attitude as there is a predicted decrease of 0.064 in the log odds of disagreeing with this statement as opposed to agreeing. This indicates that a person who believes that concerns about privacy online are being exaggerated is more likely to state they have nothing to hide.

2) The statement '*I feel I can control my privacy online*' was also a significant predictor in the model as there is a decrease of 0.098 in the log odds of disagreeing with the statement. This also indicates that people who feel they can control their online privacy are more likely to state *they have nothing to hide*.

3) Finally, the variable 'the government should regulate the internet more' significantly contributed to the model with a strong inverse relationship of -0,733 to the category 'Disagree' indicating that people who have nothing to hide tend to state that the government should exert a stronger presence in regulating the Internet. These results might indicate people's perception of a digital inefficacy that may lead to a digital resignation regarding their privacy which they may perceive as vulnerable.

Table 4: Ordinal regression analysis 'I have nothing to hide'

*Parameter Estimates**

		Estimate	StdError	Wald	Df	Sig.
Privacy violations by Governments	Disagree	-0,368	0,224	2,700	1	0,100
	Neither agree/disagree	-0,216	0,251	0,742	1	0,389
	Agree	0[a]			0	
Privacy violations by Corporations	Disagree	-0,022	0,288	0,006	1	0,939
	Neither agree/disagree	-0,046	0,295	0,024	1	0,876
	Agree	0[a]			0	
Privacy violations by Other People	Disagree	0,242	0,229	1,125	1	0,289
	Neither agree/disagree	-0,046	0,226	0,042	1	0,837
	Agree	0[a]			0	
I actively protect my privacy online	Disagree	-0,144	0,230	0,393	1	0,531
	Neither agree/disagree	-0,387	0,202	3,683	1	0,055
	Agree	0[a]			0	
Concerns about privacy online are exaggerated	Disagree	-0,642	0,197	10,632	1	*0,001*
	Neither agree/disagree	-0,428	0,241	3,154	1	0,076
	Agree	0[a]			0	
I feel I can control my privacy online	Disagree	-0,987	0,213	21,580	1	*0,000*
	Neither agree/disagree	-0,570	0,195	8,567	1	0,003
	Agree	0[a]			0	
On the Internet, it is safe to say whatever you think about politics	Disagree	-0,317	0,168	3,576	1	0,059
	Neither agree/disagree	-0,110	0,215	0,264	1	0,607
	Agree	0[a]			0	
The government should regulate the internet more	Disagree	-0,733	0,181	16,321	1	*0,000*
	Neither agree/disagree	-0,678	0,223	9,232	1	0,002
	Agree	0[a]			0	
There is no privacy, accept it	Disagree	0,196	0,166	1,384	1	0,239
	Neither agree/disagree	-0,568	0,215	6,970	1	0,008
	Agree	0[a]			0	

*a. This parameter is set to zero because it is redundant. *Missing values:435,86*

9 DISCUSSION AND CONCLUSIONS

The findings of our analysis indicate that people who state they have nothing to hide also believe that concerns about online privacy are exaggerated and they feel they can control their online privacy. That may lead to the tacit assumption that users' digital selves are likely to be surveilled, but if they have *nothing to hide*, then, this surveillance is not harmful. They believe in their 'innocence' so far so they are not guilty of collaborating with terrorists or committing cyber (or other) crimes; they also feel they can control their online privacy alone, but they need their governments to protect them. Therefore, this might indicate a partial

understanding of dataveillance: people who state they 'have nothing to hide' tend to project in their digital lives the same expectations they have from their governments in the physical world, to regulate the digital environment and protect them against violations that might occur e.g., either by corporate abuse of information power or attacks from cyber-criminals. We also showed that internet proficient respondents -in both the web and social media- are the ones who disagree with this statement, indicating that the demand for digital privacy does not entail having something to hide. We also discovered that people with higher digital skills believe internet privacy is within reach indicating that they do comprehend the inner mechanisms of the 'surveillance capitalism' but opt to manage them alone since they discard any further regulation on behalf of governments. This attitude is revealing of the dark colors with which governments have been painted due to surveilling practices they implemented in the name of security thus undermining their citizens' trust (Lyon 2003, 2014; Benkler, 2016), an issue much debated in virtue of the Covid-19 pandemic.

Does that mean that for a big part of our respondents dataveillance is accepted? Although comparative qualitative research is needed to thoroughly answer this question, it seems that peoples' assumptions about the violation of their digital privacy only go so far as to the acceptance that some companies may target them to and present them with advertisements that they will simply ignore. They may even think that they might be exposed to a few state officials and, since they are not guilty of hiding something, they should not be bothered if the exchange is the benefit of a free service or an online activity (Solove, 2007). In other words, '*I have nothing to hide*' seems to be derived from the comparative value of privacy over security. In an article published on Washington Post in 2005, judge Richard Posner was writing:

> 'collecting and processing data from machines cannot be considered a violation of privacy […]. Because of their huge volume, data is being 'sifted' by computers looking only for names, phones or addresses that may have some value for security reasons', whereas the machine keeps most of these data from being read by any intelligence officer' (Posner, 2005).

Bernal (2018: 71-77), however, argues against this '*myth of neutrality*', as the presumed innocence of the 'technical, automatic and passive' process performed by a network or an algorithm, ceases to be valid once the processing of the information leads to decisions and purposes that the original owner of the information does not control. People can be marginalized or become targets of algorithmic discrimination (Conrad, 2009; o' Neil, 2016; Noble, 2018) as important moments in their lives, such as being accepted to a university or receiving a loan can be determined based on profiles created by random online data (Helbing 2015: 7; O 'Neil 2016: 1; Eubanks 2018). Human lives are becoming more and more visible, while power asymmetries are becoming more invisible and, thanks to the growing establishment of complex data systems, are also becoming commonsensical (Lupton

2014). As a result, under the pretext of security, digital media do not contribute to the 'democratization of democracy' but rather to its destabilization when governments surveil citizens and corporations 'flesh them out' of streams of data to manipulate them and potentially modify their behavior (Foa & Mounk, 2017).

Users, quite justifiably, require protection in their digital lives as they are expected to deal with violations occurring on such high technological levels they don't even know exist: in our study the majority of the respondents state that they '*don't feel they can control their online privacy*'. However, the propagation of the '*I have nothing to* hide' attitude raises three problems. First, it assumes that privacy is about being able to hide something bad (Posner 1978; Schneier 2006; Bernal 2018). Second, it narrows down the debate on surveillance and exploitation of personal data to the irrelevant issue of whether one has something to hide and diverts it from the real questions which are, as Zuboff (2020) so aptly puts them, '*Who knows? Who decides who knows? Who decides who decides who knows*?' The third problem concerns the misconception of people who believe that, since they 'have nothing to hide', they will be permanently 'innocent' by neglecting the version in which their digital existence can be incriminated by anyone who might have an agenda. Shephard (2016) observes that when 'a person loses control of his information, he/she also loses control of the potential transformations of that information'. This is more likely to happen through 'surveillance assemblages' which 'datafy' aspects of identity, individuality and diversity (Poullet & Dinant 2006; Haggerty & Erickson 2000). If the challenge behind the claim '*I have nothing to hide*' is '*then you have nothing to fear*', that implies that 'good' people do not need privacy, as long as they have nothing to hide and 'bad' people do not deserve it, since obviously what they want to hide is harmful. Which reminds us of Zuboff's 'treacherous hallucination' that privacy is private. Within the confusing gap between what we know and what is known about us, we neglect that the very value of privacy is public - a collective good that is inseparable from the values of human autonomy and self-determination upon which privacy as well as citizenship depend (Weintraub & Kumar, 1997).

Therefore, **legislation and regulation** are firstly required in order to tackle the epistemic inequality. It is obvious that self-regulation of tech giants is coming to an end and state-based regulation and stronger enforcement of existing legislation is necessary. In Greece, the right to the protection of personal data is enshrined in the 2001 revision of Article 9A of the Constitution and is regulated by the General Rule for the Protection of Data (2016/679) which was enforced on May 2018 along with law 4624/2019 which defines the enforcement measures that integrated the European Directive (2016/680). However, according to the Special Eurobarometer 487a Survey[28], although Greek people seem coordinated with the rest of Europe concerning their knowledge about the existence of the General Data Protection Regulation, 39% of the respondents have not even heard which are the six rights GDPR protects landing them well below the European average. Which gives rise

[28] http://ec.europa.eu/commfrontoffice/publicopinion

to a second imperative: **information and digital literacy**. In Greece, as well as throughout Europe, the legal framework is set but people need to know their rights and the authorities that protect them. Enhancing informational channels about the legal status of peoples' online rights can only advance digital citizenship skills along with proper education. With Google in the lead, the top surveillance capitalists seek to control labor markets in expertise – including data science – eliminating competitors such as start-ups, universities, high schools, municipalities, established corporations in other industries or less wealthy countries. People need to familiarize themselves with the language of the digital world to the best of their abilities. If 20th century politics were defined by who owns the means of production, 21st century politics needs to be based on who owns the production of meaning. Introducing digital literacy in schools is of the utmost importance especially given the fact that children and teenagers today are digital natives that need to be best equipped in order to adapt to the even more complex and technically defined world of the future.

Although it is unfair for the users to carry once again the burden of securing their own privacy having to deal with technological savants behind algorithmic curtains, that is where a third imperative comes in: **algorithmic transparency through explainable AI.** One of the sections of the EU's General Data Protection Regulation (GDPR) focuses on the right to 'explanation'. Essentially, it mandates that users be able to demand the data behind the algorithmic decisions made for them including recommendation systems, credit and insurance risk systems, advertising programs and social networks. In doing so, it tackles 'intentional concealment' by corporations. However, the ambiguity and limited scope of the 'right not to be subject to automated decision-making' contained in Article 22 (from which the 'right to explanation' derives) raises questions over the actual protection provided to data subjects (Wachter et al., 2017). Furthermore, article 22 does not address the technical challenges associated with transparency in modern algorithms. Explainable AI (Miller, 2017; Pasquale, 2014; Edwards & Veale, 2017) is actually algorithms that can reveal how they work and why they end up in making a specific decision. Therefore, systems that work by analyzing and reporting which information input weighted the most in a decision-making algorithm, e.g., measuring and presenting how important the number of accidents a driver might have had in calculating the cost of their car insurance, may lift the veil over the 'man behind' the algorithmic 'curtain' …

FUNDING STATEMENT AND ACKNOWLEDGMENTS

This article is an output of the project "Research, Education and Infrastructures: the triangulation of EKKE strategic axes (REDI)", which is co-financed by the European Regional Development Fund in the framework of the Operational Programme "Competitiveness, Entrepreneurship and Innovation 2014-2020"

(EPAnEk). The authors thank the anonymous reviewers for their constructive suggestions for the article to take its final form.

REFERENCES

Acquisti, A., Taylor, C. & Wagman, L., 2016, "The Economics of Privacy". *Journal of Economic Literature* 54 (2): 442-92.

American Educational Research Association, January 2019, "Voter preference for Trump linked to bullying in middle schools". *ScienceDaily*. Retrieved April 2020, from www.sciencedaily.com/releases/2019/01/190109090917.htm

Amnesty international Report, 2019, 'Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights'. Retrieved January 2020 from https://amnestyusa.org/wp-content/uploads/2019/11/Surveillance-Giants-Embargo-21-Nov-0001-GMT-FINAL-report.pdf

Amoore, L., & De Goede, M., 2005, "Governance, Risk and Dataveillance in the War on Terror". *Crime, Law and Social Change* 43: 149-173.

Ariely, D. & Berns, G.S., 2010, "Neuromarketing: the hope and hype of neuroimaging in business". *Nature Reviews. Neuroscience*, 11(4): 284-292.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar M. & Turner, E., 2019, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information', Pew Research Center. Retrieved February 2021 from: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Bauman, S., 2019, *Political Cyberbullying: Perpetrators and Targets of a New Digital Aggression*. Praeger

Benkler, Y., 2016, 'We cannot trust our government, so we must trust the technology', *The Guardian*, 22 February 2016. Retriever February 2021 from https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi

Bernal, P., 2018, *The Internet, Warts and All. Free Speech, Privacy and Truth*. Cambridge University Press

Bond, R., Fariss, C., Jones, J. 2012, 'A 61-million-person experiment in social influence and political mobilization'. Nature 489: 295–298. https://doi.org/10.1038/nature11421

Boyd, D. and Crawford, K., 2012, Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662-79.

Brown B., 2001, "Studying the internet experience". *Hp Laboratories Technical Report HPL* 49. Retrieved February 2020 from https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.

Brunton, F. & Nissenbaum, H., 2015, *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press

Busvine, D. & Rinke, A, 2020, 'Germany flips to Apple-Google approach on smartphone contact tracing', Reuters, 26 April 2020. Retrieved February 2021 from https://www.reuters.com/article/uk-health-coronavirus-europe-tech-idUKKCN22807X

Bustos de, C.M. & Izquierdo-Castillo, L., 2019, "Who will control the media? The impact of GAFAM on the media industries in the digital economy". *Revista Latina de Comunicación Social* 74: 803-821.

Cammaerts, B., 2008, "Critiques on the participatory potentials of Web 2.0". *Communication, Culture and Critique* 1(4): 358-77.

Carrascal, J.P., Riederer, C., Erramilli, V., Cherubini, M., de Oliveira R., 2013, "Your browsing behavior for a Big Mac: economics of personal information online". In *Proceedings of the 22nd international conference on WorldWideWeb*, Rio de Janeiro, Brazil, 189–200.

Clarke, R. 1994, "Dataveillance by Governments: The Technique of Computer Matching". *Information Technology & People* 7(2): 46-85.

Conrad, K., 2009, "Surveillance, Gender, and the Virtual Body in the Information age". *Surveillance & Society* 6(4): 380–387

Crouch, C., 2004, *Post Democracy*, Polity, Cambridge

Curran, D., 2018, "Are you ready? Here is all the data Facebook and Google have on you". *The Guardian*, 30 March 2018. Retrieved March 2020 from https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy

Davenport, T. H. & Beck, J. C., 2013, *The Attention Economy: Understanding the New Currency of Business*. Cambridge, MA: Harvard Business Press.

Debatin, B., Lovejoy, J.P, Horn, A.K. & Hughes, B.N, 2009, "Facebook and online privacy: attitudes, behaviors, and unintended consequences". *Journal of Computer-Mediated Communication* 15(1):83 – 108

Demertzis, N., 2020, 'The pandemic as trauma' (Η Πανδημία Ως Τραύμα). In Γεωργακόπουλος, Θ (ed), Οι Ιδέες Της Πανδημίας-15 κείμενα για το πώς ο κορωνοϊός αλλάζει την Ελλάδα και τον κόσμο. διαΝΕοσις Publications, Athens

Demertzis, N. and Eyerman, R., 2020., "Covid-19 as Cultural Trauma". American Journal of Cultural Sociology, 8 (2): 428-450. DOI 10.1057/s41290-020-00112-z

Demertzis, N. & Tsekeris, C., 2018, "Multifaceted European Public Sphere – Socio-Cultural Dynamics". In B. Cammaerts, N. Anstead & R. Stupart, Media@LSE Working Paper Series. Media and Communications, Media@LSE, London School of Economics and Political Science.

Derikx, S., De Reuver, M., Kroesen, M., & Bouwman, H., 2015., "Buying-off Privacy Concerns for Mobility Services in the Internet-of-things Era: A Discrete Choice Experiment on the Case of Mobile Insurance". In

Proceedings of the 28th Bled eConference. Retrieved February 2020 from http://aisel.aisnet.org/bled2015/28

DeVellis, R. F., 2003, *Scale Development: Theory and Applications*. Thousand Oaks, CA: Sage.

Douzinas, K., 2020, 'The Biopolitics of the Pandemic' ('Η Βιοπολιτική της Πανδημίας'). In Π. Κ α π ό λ α, Γ. Κ ο υ ζ έ λ η ς & Ο. Κ ω ν σ τ α ν τ άς (Ε π ι μ) *Α π ο τ υ π ώ σ ε ι ς Σ ε Σ τ ι γ μ έ ς Κ ί ν δ υ ν ο υ*, Ε τ α ι ρ ε ί α ς Μ ε λ έ τ η ς τ ω ν Ε π ι σ τ η μ ώ ν τ ο υ Α ν θ ρ ώ π ο υ, Νήσ ος Publication, Athens

Draper, N. & Turow, J., 2019, 'The corporate cultivation of digital resignation'. New Media & Society 21(4), DOI: 10.1177/1461444819833331

Edwards, L. & Veale, M., 2018, 'Enslaving the algorithm: From a 'right to an explanation' to a 'right to better decisions?' IEEE Security & Privacy

Egelman, S., Felt, AP & Wagner, D., 2012, "Choice architecture and smartphone privacy: there's a price for that". In *Proceedings of the 11th annual workshop on the economics of information security*. Berlin, Germany.

Ellison, N.B., Vitak, J., Steinfield C., Gray, R. & Lampe, C., 2011, "Negotiating privacy concerns and social capital needs in a social media environment". In: *Privacy online*. Berlin Heidelberg: Springer, 19–32.

Eubanks, V., 2018, *Automating Inequality How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Publishing Group

European Commission Joint Research Centre Report, 2020, 'Technology and Democracy'. Retrieved February 2020 from https://ec.europa.eu/jrc

European Commission Special Eurobarometer 487a, 2019, The General Data Protection Regulation. Retrieved February 2021 from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/1974/yearTo/2019/surveyKy/2222

Floyd, F. J. & Widaman K. F. (1995). Factor Analysis in the Development and Refinement of Clinical Assessment Instruments. *Psychological Assessment* 7(3): 286-299.

Flick, C., 2016, "Informed Consent and the Facebook Emotional Manipulation Stud". *Research Ethics* 12(1): 14–28.

Foa, R.S. & Mounk, Y., 2017, "The Signs of Deconsolidation". *Journal of Democracy* 28(1): 5-15.

Fuchs, C. 2012, "The Political Economy of Privacy on Facebook". *Television & New Media* 13(2): 139-159.

Fuchs, C. 2014, "Social Media and the Public Sphere', tripleC: Communication, Capitalism & Critique, *Journal for a Global Sustainable Information Society* 12(1): 57-101.

Gross, J.A., 2020, "Government okays mass surveillance of Israelis' phones to curb coronavirus". *Times of Israel*, 15 March 2020. Retrieved April 2020 from https://www.timesofisrael.com/government-okays-mass-surveillance-of-israelis-phones-to-curb-coronavirus/

Gould, W., 2000, "Interpreting logistic regression in all its forms". In: *Stata Technical Bulletin* 53: 19-29.

Haggerty, K.D. & Ericson, R.V., 2000, "The surveillant assemblage", *British Journal of Sociology* 51(4): 605–622.

Hayden, M., 2014, General Michael Hayden Beyond Snowden: An NSA Reality Check. *World Affairs* 176 (5): 13-23

Helbing, D., 2015, *Thinking Ahead—Essays on Big Data, Digital Revolution, and Participatory Market Society*. Springer

Helbing, D., 2020, The Corona Crisis Reveals the Struggle for a Sustainable Digital Future. TRAFO – Blog for Transregional Research, 21.05.2020, https://trafo.hypotheses.org/23989

Heller, C., 2011, *Post-Privacy: Prima leben ohne Privatsphäre*. München: Beck.

Hindman, M., 2009, *The myth of digital democracy*. Princeton, NJ: Princeton University Press.

Hsu T. & Celia Kang, C., 2018, "Demands Grow for Facebook to Explain Its Privacy Policies". *New York Times*, 26 March 2018. Retrieved March 2020 from https://www.nytimes.com/2018/03/26/technology/ftc-facebook-investigation-cambridge-analytica.html

Keyes, R., 2004, *The Post-Truth Era: Dishonesty and Deception in Contemporary Life*, St. Martin's Press

Kokolakis, S., 2017, "Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon". In *Computers & Security* 64: 122–134.

Kontiades, X., 2020, *Pandemic, Biopolitics and Rights – The World after Covid-19* (Πανδημία, Βιοπολιτική και Δικαιώματα – Ο κόσμος μετά τον Covid 19). Kastaniotis Publications, Athens

Kramer, A. D. I, Guillory, J. E, & Hancock J. T., 2014,' Experimental evidence of massive-scale emotional contagion through social networks'. PNAS 24: 8788-8790. https://doi.org/10.1073/pnas.1320040111

Kucklick, C., 2014, *Die granulare Gesellschaft. Auf dem Weg ins Zeitalter der Ungleichheit*. Berlin: Ullstein Buchverlage.

Laudon, K., 1997, "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information". New York University Stern School of Business, Working Paper IS-97-4.

Lee, H., Park H. & Kim J., 2013, "Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk". *International Journal of Human-Computer Studies* 71(9): 862–77.

Lyon, D., 2001a, *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D., 2001b, "Facing the Future: Seeking Ethics for Everyday Surveillance", *Ethics and Information Technology*, 3 (3): 171-180.

Lyon, D., 2014, "Surveillance, Snowden, and Big Data: Capacities, consequences, critique". *Big Data & Society*, 1-13.

Lyon, D., 2003, *Surveillance After September 1 1*(Themes for the 21st Century). Malden, MA: Polity

Madden, M., 2014, "Public perceptions of privacy and security in the post-Snowden era". Pew Research Center. Retrieved February 2020 from https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/

Mai, J. E., 2016, "Big data privacy: The datafication of personal information". *The Information Society* 32 (3): 192-199

Mayer-Schonberger, V. & Cukier, K., 2013. *Big data: A revolution that will transform how we live, work and think*, New York, NY: Houghton Mifflin Harcourt.

McIntyre, L., 2018, *Post Truth*, The MIT Press Essential Knowledge series

Miller, T., 2017, Explanation in artificial intelligence: insights from the social sciences. Retrieved February 2021 from https://arxiv.org/pdf/1706.07269.pdf.

Mosco, V., 2009, *The Political Economy of Communication*. London: Sage.

Murgia, M., 2019, 'Who's using your face? The ugly truth about facial recognition', *Financial Times*, 18 Sep 2019. Retrieved February 2021 from: https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e

Ngwenyama, O. & Klein, S., 2018, "Phronesis, Argumentation and Puzzle Solving in IS Research: Illustrating an Approach to Phronetic IS Research Practice". *European Journal of Information Systems* 27(3): 347-366

Nield, D., "All the Ways Google Tracks You—And How to Stop It". The Wired, 27 May 2019. Retrieved April 2020 from https://www.wired.com/story/google-tracks-you-privacy/

Noble, S.U., 2018, *Algorithms of Oppression How Search Engines Reinforce Racism*, NYU Press

Norberg, P.A, Horne, D.R, Horne D.A., 2007, "The privacy paradox: personal information disclosure intentions versus behaviors". Journal of Consumer Affairs 41(1): 100-126.

Norval, A., & Prasopoulou, E., 2017, 'Public Faces? A Critical Exploration of the Diffusion of Face Recognition Technologies in Online Social Networks". *New Media & Society* 19(4): 637-654.

O'Neil, C., 2016, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Books, New York.

OECD, 2019, *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*. Paris: OECD Publishing.

Papadoudis, G., 2018, "Multiple Discrimination and Inequalities: An Empirical Investigation". In *Tackling multiple discrimination in Greece*. ION Publishing Group & National Centre for Social Research, 213-233.

Pasquale, F., 2014, *The black box society: the secret algorithms that control money and information*. Cambridge: Harvard University Press

Park, Y.J., Chung, J.E & Shin, D.H., 2018, "The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. *American Behavioral Scientist*, SAGE Publications, 1-19.

Peterson, A., 2013, 'Former NSA and CIA Director Says Terrorists Love Using Gmail,' Washington Post, September 15, 2013, retrieved February 2021 from https://www.washingtonpost.com/news/the-switch/wp/2013/09/15/former-nsa-and-cia-director-says-terrorists-love-using-gmail/ .

Posner, R., 1978, "The Right of Privacy". *Georgia Law Review* 12: 393-428.

Posner, R., 2005, "Our Domestic Intelligence Crisis", *Washington Post*, 21 Δεκεμβρίου 2005. Retrieved January 2020 from https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/

Poullet, Y & Dinant, J.M., 2006, "The internet and private life in Europe". In Kenyon, A. T. & Richardson, M., *New dimensions in privacy law: international and comparative perspectives*, Cambridge University Press, 60-90

Rosen, J., 2002, 'Total Information Awareness', 15 Dec 2002, The New York Times Magazine, retrieved February 2021 from https://www.nytimes.com/2002/12/15/magazine/the-year-in-ideas-total-information-awareness.html

Rule, J. B., McAdam, D., Stearns, L., & Uglow, D., 1983, "Documentary Identification and Mass Surveillance in the United States. *Social Problems* 31(2): 222-234.

Schneier, B., 2006, "The Eternal Value of Privacy". *The Wired*, May 18 Μαΐου 2006. Retrieved February 2020 from http://www.wired.com/news/columns/1,70886-0.html

Schuster, S., Van den Berg, M., Larrucea, X., Slewe, T., & Ide-Kostic, P., 2017, "Mass Surveillance and Technological Policy Options: Improving Security of Private Communications". *Computer Standards & Interfaces* 50: 76-82.

Sennett, R., 1993, *The Fall of Public Man*. London: Faber and Faber.

Shephard, N., 2016, "Big data and sexual surveillance". APC Issue Papers. Retrieved February 2020 from http://www.apc.org/sites/default/files/BigDataSexualSurveillance_0.pdf

Shorey, S. and Howard, P. N., 2016, "Automation, big data, and politics: A research review". *International Journal of Communication* 10(2016): 5032-55.

Singer, N. & Sang-Hun C., 2020, "As Coronavirus Surveillance Escalates, Personal Privacy Plummets". *The New York Times*, 23 March 2020. Retrieved April 2020 from https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

Smith, G. J. 2016, "Surveillance, Data and Embodiment: On the Work of Being Watched. *Body & Society* 22(2): 108-139

Smith, D., 2020, "Google keeps a frightening amount of data on you. Here's how to find and delete it". *Cnet*. 7 March 2020. Retrieved April 2020 from https://www.cnet.com/how-to/google-keeps-a-frightening-amount-of-data-on-you-heres-how-to-find-and-delete-it/

Solove, D. J., 2007, "I've got nothing to hide' and other misunderstandings of privacy". San Diego Law Review 44: 745

Solove, D., 2013, 'Privacy Self-Management and the Consent Dilemma', 126 Harvard Law Review 1880 . Retrieved January 2021 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

Solove, D., 2020, 'The myth of the Privacy Paradox', GW Law School Public Law and Legal Theory Paper No. 2020-10. Retrieved January 2021 from https://ssrn.com/abstract=3536265

Spiekermann, S., Grossklags J. & Berendt B., 2001, "E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior". In *Proceedings of the 3rd ACM conference on electronic commerce*. Florida, USA, 38–47.

Spourdalakis, M., 2020, 'The post-coronavirus Democracy – Will it be socialistic or will it not exist?' (Η μετά κορωνοϊού - Δημοκρατία θα είναι σοσιαλιστική ή δεν θα υπάρχει). In Π. Καπόλα, Γ. Κουζέλης & Ο. Κωνστάντας (Επιμ) *Από τους πώσεις Στις Συγμές Κίνδυνου*, Εταιρεία Μελέτης των Επιστημών του Ανθρώπου, Νήσος

Srnicek, N., 2017, *Platform Capitalism*. Polity Press.

Stamouli, N., 2020, 'Coronavirus bundles Greece into the digital era'. Politico, 4 Feb 2020, retrieved February 2021 from: https://www.politico.eu/article/coronavirus-bundles-greece-into-the-digitalera/amp/

Steidl, P., 2012, *Neurobranding*. CreateSpace Independent Publishing Platform.

Stein. A., 2020, "How to restore data privacy after the coronavirus pandemic". *World Economic Forum*, 31 Mar 2020. Retrieved April 2020 from https://www.weforum.org/agenda/2020/03/restore-data-privacy-after-coronavirus-pandemic

Stutzman, F., Vitak J., Ellison N.B., Gray R., & Lampe C., 2012, "Privacy in Interaction: exploring disclosure and social capital in Facebook". In *Proceedings of the 6th international conference on weblogs and social media* (ICWSM 2012), Dublin, Ireland.

Taddicken M., 2014, "The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics and the perceived social relevance on different forms of self-disclosure". *Journal of Computer-Mediated Communication* 19(2):248–73.

TRUSTe, 2014, US Consumer Confidence Privacy Report Consumer Opinion and Business Impact. Retrieved February 2020 from http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

Tsekeris, C., & Katerelos, I. (eds), 2014, *The social dynamics of Web 2.0: Interdisciplinary perspectives*. London: Routledge.

Tsekeris, C., Demertzis, N., Linardis, A., Iliou, K., Kondyli, D., Frangiskou A. & Papaliou, O., 2020, Investigating the Internet in Greece: findings from the World Internet Project. Hellenic Observatory Discussion Papers on Greece and Southeast Europe, no 153

Tzarelas, D., 2020, 'The Return of the State in the midst of the pandemic' ('Η επιστροφή του κράτους εν μέσω πανδημίας'). In Π. Καπόλα, Γ. Κουζέλης & Ο. Κωνσταντάς (Επιμ) *Από τους πώσες ις Σε Σ τι γμές Κίνδυνου*, Ετα ιρεία Μελέτης των Επιστημών του Ανθρώπου, Νήσος Publications, Athens.

Tzogopoulos, G. N., 2020, "The Internet in the Coronavirus Era, *The Begin Sadat Center for Strategic Studies*, 30 March 2020. Retrieved April 2020 from https://besacenter.org/perspectives-papers/coronavirus-internet/

van der Schyff, K., Krauss, K.E.M. & Kroeze, J.H., 2018, "Facebook and Dataveillance: Demonstrating a Multimodal Discourse Analysis", *Twenty-fourth Americas Conference on Information Systems,* New Orleans

van Dijck, J. 2014, "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society* 12(:2): 197.

van Dijck, J., 2013, *The Culture of Connectivity: A Critical History of Social Media*, Oxford: Oxford University Press.

Wachter, S., 2020, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising'. Berkeley Technology Law Journal, Vol. 35:2

Wachter, S., Mittelstadt, B. & Floridi, L., 2017, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation'. International Data Privacy Law 7-2: 76–99, https://doi.org/10.1093/idpl/ipx005

Watson, C., 2018, "The key moments from Mark Zuckerb'rg's testimony to Congress. *The Guardian*, 11 April 2018. Retrieved February 2020 from https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments

Weintraub, J. & Kumar, K. (eds.) 1997, *Public and Private in Thought and Practice. Perspectives on a Grand Dichotomy.* Chicago: The University of Chicago Press.

Worthington, R. & Whitaker, T., 2006, "Scale Development Research-A Content Analysis and Recommendations for Best Practices". The Counseling Psychologist 34 (6): 806-838

Wouters, C., 2007, *Informalization: Manners and emotions since 1890*. London: Sage

Zafeiropoulou, A.M, Millard, D.E, Webber, C & O'Hara, K., 2013, "Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?". In: Proceedings of the 5th annual ACMWeb Science Conference, May 2–4, Paris, France

Zuboff, S., 2019, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, PublicAffairs, New York.

Zuboff, S., 2020, 'You Are Now Remotely Controlled', *The New York Times*, 24 Jan 2020. Retrieved February 2020 from https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html

Zuboff, S., 2021, 'The Coup We Are Not Talking About', *The New York Times*, 29 Jan 2021. Retrieved February 2021 from https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html

Zurawicki, L. (2010). *Neuromarketing: Exploring the brain of the consumer*. London: Springer.