European Journal of Political Economy 67 (2021) 101967

Contents lists available at ScienceDirect

European Journal of Political Economy

journal homepage: www.elsevier.com/locate/ejpe

Privacy rights in online interactions and litigation dynamics: A social custom view

Stefano Dughera *, Marco Giraudo

University of Torino, Department of Economics and Statistics, Lungo Dora Siena 100/A, 10153, Torino, Italy

ARTICLE INFO

JEL classification:
K24
K41
O30

Keywords:
Social media
Privacy
Litigation dynamics
Social custom

ABSTRACT

We develop a social custom model where a population of social media users decide whether to remain online and accept the platform's data-gathering policy or abandon the social media and litigate for privacy violations. By allowing the users' concerns for informational security to co-evolve with the number of privacy-related trials, we find that the system may converge to multiple equilibria. When users put relative emphasis on the relational benefits of online interactions, privacy-related trials remain contained and the provider imposes no limitations to its data-gathering activities. Conversely, when users put relative emphasis on the privacy costs of web-mediated interactions, privacy-related trials become endemic and platforms modulate their data-gathering activities by mediating between profitability and the legal implications of their choice. We use these results to comment the recent shift in the users' orientation towards online platforms and caution against the inability of institutions to keep up with the process of technological change.

1. Introduction

Since the internet 2.0 revolution, the digitization of nearly all media and the continuing migration of social and economic activities to the internet is generating petabytes of data every second (OECD, 2014: 9). With the diffusion of broadband access and internet enabled devices, consumers are actively and passively divulging information in exchange for services. The main example are social media. In 2014, for instance, Facebook connected already 1.3 billion people around the world, who generated an average of 1500 status updates every second, but similar phenomena characterize other social media platforms (Stucke and Grunes, 2016; Klonick, 2017).

Over the same period, customer-provided information became increasingly valuable, up to the point where data has been defined as the "new oil" fueling up the digital and non-digital economy. Improving customer experience through the access of their online information has become a mantra for strategists, as witnessed by the tremendous growth of data markets worldwide.[1]

Social media companies played a key role in this transformation. Boosted by growing hype for web-mediated interactions and little consumer interest for the terms and conditions of service (Rubenstein and Good 2013; Bygrave, 2015), they spent the last decade or so collecting their subscribers' information, interpreting the generalized enthusiasm for the service they offer as a "green light" for their data-gathering activities. In the heyday of platforms diffusion, in fact, users showed little concern for the privacy implications of online

* Corresponding author.
E-mail address: s.dughera@unito.it (S. Dughera).

[1] According to the Data Market Study of the European Commission the value of the European and US data economy (which measure the overall impact of data markets on the economy as a whole) exceeded the threshold of 300 billion euros and 155 billion dollars in 2018, with a year-on-year growth of 12% and 10.3% respectively.

https://doi.org/10.1016/j.ejpoleco.2020.101967
Received 17 February 2020; Received in revised form 1 September 2020; Accepted 17 October 2020
Available online 22 October 2020

interactions and welcomed the novel socialization opportunities as a massive breakthrough in interpersonal communication. When Facebook was first put online, for instance, it was applauded as a gateway to « give people the power to share and make the world more open and connected» (Hoffman et al., 2018:200). This enthusiasm reached an acme in 2010, when Zuckerberg was celebrated "person of the year" and the New York Times recognized the existence of a "Zuckerberg Law," whereby, each year, people « share twice as much information as they share … the year before» (Chander, 1808, 2012).[2] At that time, Zuckerberg himself proclaimed to have changed the social norm: «people have really gotten comfortable not only with sharing more information and of different kinds, but more openly and with more people».[3]

More recently, the collective perception of social media started to change. Scandals like the Snowden revelations and Cambridge Analitica[4] drew increasing attention to the privacy implications of the platforms' data-gathering activities, marking the beginning of a new season of class actions and fines against social media companies. The upshot is that providers are less and less seen as enablers providing people with a novel opportunity to connect and more and more as "digital gangster" who « control the interactive landscape» (Horton, 1999:111) without the shackles of state regulation.[5]

In this paper, we rationalize this shift in the users' orientation towards online platforms and provide an explanation to the recent boom of privacy-related trials against the latter. To do so, we develop a framework where a population of users must decide whether to remain online and accept the platforms' data-gathering policy or stop using the social media and litigate for privacy violations. Our key Assumption is that the collective perception of social media deteriorates with the number of privacy trials, as consumers interpret litigiousness in courts as a signal of data violation. In this framework, the individual decision to litigate creates a feedback effect which boosts the dynamics of litigation. When lawsuits are initially abundant, users put relative emphasis on the privacy implications of web-mediated interactions, and litigation escalates. Conversely, when lawsuits are initially scarce, users put relative emphasis on the relational benefits[6] of web-mediated interactions, and litigation dies out. Hence, we highlight a mechanism whereby the individual propensity to go to court varies positively with the presence of litigators in the users' population.[7]

To model this idea, we develop a social custom model[8] where a population of users interacts through a social media supplied by a single provider. To study the link between the platform's data-gathering policy and the users' decision to litigate for privacy violations, we assume that the provider's activities have an ambiguous effect on its subscribers' perception of the service. On the one hand, by collecting more information, the platform improves the online visibility of its subscribers, thus facilitating the consumption of relational goods associated to web-mediated interactions. On the other hand, it aggravates the perception of the privacy implications of using the social media. When the first of these two effects outweighs the latter, we find that the platform finds it rational to impose no limitations to its activities. Conversely, when data-gathering aggravates the perception of the privacy costs more than improves the consumption of relational goods, the platform finds it rational to limit its activities. Hence, we highlight a mechanism whereby the platform's policy co-evolves with the collective perception of social media in the society "out there".

We mean this contribution as an attempt to interpret a series of stylized facts that have characterized the recent history of privacy issues in web-mediated interactions. In its simplicity, we believe that our model is capable of capturing—though in a stylized fashion—the co-evolutionary process that bonds together (i) the individual decision to litigate for privacy violations, (ii) the changing orientation of users towards social media platforms and (iii) the way in which providers structured their business model. We are aware that in order to make sense of this complex array of behavioral, organizational and institutional co-dependencies, we did rely on a series of constraining hypotheses. The key limitation of our model is due to the Assumption that those who file a case for privacy violations also abandon the social media. In reality, there may exist multiple relationships between online and offline behavior. Not only users may simply decide to keep using the platform and simultaneously litigate in court, but they may also engage in complex behavioral patterns

[2] Lev Grossman, Person of the Year 2010: Mark Zuckerberg, TIME (Dec. 15, 2010), available at http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183,00.html.

[3] Privacy concerns, however, have always been there. Already in 2014, Pew conducted a series of surveys where consumers voiced concern about the fact of being « unaware of who has access to their personal information, what data is being used, how and when their data is being used, and the privacy implications of the data's use» (Stucke and Grunes, 2016: 5; see also "Public Perceptions of Privacy and Security in the Post-Snowden Era", Pew Research Center, Washington, D.C. (12 November 2014) retrieved from https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/). Already at that time, the majority of American citizens « feel that their privacy is being challenged along such core dimensions as the security of their personal information and their ability to retain confidentiality». More than 90% of the interviewed agree that they had lost control over the way in which their personal information is collected and used by companies (Stucke and Grunes, 2016: 5) Similarly, 72% of European Internet users « still worry that they are being asked for too much personal data online» (European Commission, Why We Need a Digital Single Market (May 6, 2015) retrieved from https://ec.europa.eu/commission/publications/why-we-need-digital-single-market_en).

[4] See Graham-Harrison and Cadwalladr (2018).

[5] About Facebook, see for instance The House of Commons Digital, Culture, Media and Sport Committee. Disinformation and 'fake news': Final Report. Eighth Report of Session 2017–19. (14 February 2019) Accessed at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

[6] The consumption of relational goods is one in a series of positive byproducts of web-mediate interactions, which also include the accumulation of social capital (Antoci et al., 2012); the consolidation of weak ties (Ellison et al., 2007); the promotion of social learning (Burke et al., 2010), social trust, civic participation and political engagement (Park et al., 2009).

[7] In political economy, feedback dynamics of this sort have been used to explain the sudden rise of unanticipated social changes such as revolutions—see, for instance, Kuran (1989).

[8] The social custom model has been first developed by Akerlof (1980) and widely applied in several contexts, such as tax evasion (Myles and Naylor, 1996), organizational corruption (Chang and Lai, 2002) worker effort (Chang and Lai, 1999), union membership (Booth, 1985) and so on. More broadly, it has been proposed as a framework to analyze collective action and the influence of peer pressure on individual behavior.

that combine litigiousness in court with various strategies of information disclosure—see, for instance, Büchi et al. (2020). The growing literature on the sociopsychology of social media, in fact, shows that users adapt their informational exposure by mediating between their privacy concerns and the benefits they expect to receive from web-mediated interactions—see, for instance, Ellison et al. (2012). In this framework, the decision to file a case for privacy violations may belong to a series of richer behavioral patterns that cannot be accounted for by a simple model like ours. Hence, we hope that our contribution will stimulate future research to disentangle the relationship between online and offline behavior.

The remainder of the paper is organized as follows. In section 2, we provide an overview of the stylized facts related to privacy-issues in online interactions. In sections 3, 4 and 5, we develop a social custom model inspired by these facts. Section 6 highlights the role of institutional incompleteness on the equilibrium outcomes of the game. Section 7 concludes.

2. Background

2.1. Data-gathering in a context of institutional incompleteness

The user's oscillating orientation towards social media companies has been long nurtured by the incompleteness of the institutional framework. As legislative branches have abstained from regulating internet-related activities in full (Lessing, 1997; Chander, 2014), privacy rights in online interactions have been poorly defined and the providers' entitlement to collect, use and monetize their customers' information remains largely unclear. As the "newness" of web-related technology has been long emphasized to buttress the "internet exceptionalism" (Wu, 2010; Balkin, 2004; Johnson and Post, 1996), a comprehensive federal law governing data ownership in the US is still missing, while the General Data Protection Regulation (GDPR) was recently introduced in the EU to amend a similar long-lasting institutional void (DeMarco and Fox, 2019)), and yet a substantial degree of legal uncertainty remains (Steinrötter, 2020).

In this framework, social media companies have been left alone to play the role of "quasi-rulers", «being responsible for educating a submissive public into wanting new products and accepting the necessity for economic change» (Horton, 1999: 113).[9] The "notice and consent" (N&C) model of contract was the legal innovation through which providers attempted to fill this institutional void. Ideally, such contracts should « ensure that website visitors can give free and informed consent to businesses' data collection and use practices […][thus revealing]an acceptable overall tradeoff between informational privacy and the benefits of information processing» (Sloan and Warner, 2014: 374; see also Posner, 1981; Stigler, 1980).[10] In reality, they are often strategically vague, as to allow providers to modify their activities and legitimate future behaviors through flexible terms like "improving customer experience" (EDPS, 2014: 35).

The institutional uncertainty resulting from the combination of incomplete privacy laws and vague N&C contracts had offsetting implications for data buyers and sellers alike. While users could not but rely on their imperfect information to evaluate the balance between the relational benefits and the privacy costs of web-mediated interactions, platforms had to turn to their users' orientation to fine-tune their data-gathering activities. Retrospectively, this created room for a sort of "legal hazard" (Rubinstein and Good, 2013) that generated what the head of the European data protection watchdog described as a «lack of accountability for millions of micro decisions in a system that nobody could understand anymore».[11] The Price Westerhouse Cooper LLP, which was the audit company charged with the assessment of Facebook's compliance with data protection laws, commented on the company's legal aloofness in the following terms: «they've devised business models […] without much concern about social, economic, or legal consequences […] As the saying goes, it was better to ask for forgiveness than permission» (Chitkara et al., 2018: 8).

2.2. Privacy litigation in the data-driven economy

As anticipated, it took some time before the legal implications of the platforms' data-gathering activities eventually emerge. Not only consumers,[12] but judges and regulators seemed initially cautious in their approach towards privacy matters in online interactions.

[9] Remarkably, Bygrave (2015) uses the term "Lex Facebook" to refer to the platform's terms and conditions, as to underline their key role in shaping the general norms of web-mediated interactions.

[10] Both legal and economic literature offer compelling critiques of such claims. As to legal scholarship, it has been argued that the mere opportunity to read the notice does not guarantee the users' consent, as most consumers simply avoid reading the latter (Ben-Shahar, 2009; Sloan and Warner, 2014; Tene and Polonetsky, 2014). And even if they did, it would take on average 244 h per year to read all the privacy policies presented by the websites an average consumer visits, which amounts to more than 50 per cent of the time they spend on the internet. In addition, lack of contextuality between consent and waiver of fundamental rights to privacy over sensitive data may call into question the actual formation of a meaningful consent to these data-gathering practices (Jolls, 2013). As to economics, the assumptions that the consumers' "true" preferences over privacy issues are revealed through their online activity has also been contested (Stucke and Grunes, 2016: 58). Unawareness of the platforms' practices—who have access to what information, what, when and how these information is being used—may lead to several biases in consumer behavior (Acquisti et al., 2015). Hermstrüwer and Dickertb (2017), Jolls (2013) Willis (2014) and Schudy and Utikal (2015), for instance, provided empirical evidence that users are unable to anticipate the platforms' uses of their personal data and are often affected by optimism bias, status quo bias and hypothetical bias.

[11] Buttarelli, G. (Speech, Brussel, March, 20, 2018) Speech to LIBE on Annual Report 2017 www.edps.europa.eu/sites/edp/files/publication/20-03-18_speech_to_libe_on_ar2017_published_en.pdf.

[12] The initial frenzy towards web-mediated interactions was so widespread that the early litigators contesting Facebook for unlawful uses of their data often felt the need to clarify their position. As an important petition called "Facebook, stop invading my privacy" stated on its page, «a lot of us love Facebook—it's helping to revolutionize the way we connect with each other. But they need to take privacy seriously» (Srinivasan, 2019: 58). Hence, even those who perceived the platforms' practices as unfair could not but celebrate their positive effect on interpersonal communication.

Despite the multibillion size of the emergent targeted advertising market, for instance, the FTC imposed fines in the order of 22 million dollars in cases of major violations by Google (Miller, 2012). Similarly, class actions were settled for a fist of millions of dollars in cases otherwise characterized as « textbook examples of how to violate the principle of privacy by design».[13] When asked to decide on the matter of civil lawsuits, courts systematically dismissed the plaintiffs' claims on the ground of lack of e.g. tangible harm, users' consent to second uses of personal data,[14] as well as lack of expectation of privacy.

The situation dramatically changed after the Snowden revelations and Cambridge Analitica (Rubenstein, 2013; Bygrave, 2015; Klonick 2017). European consumer organizations launched a coordinated campaign of collective actions titled "My Data is Mine" pushing for «a change of paradigm […with] consumers as crucial catalysts of a more sustainable and responsible digital value chain to make the data economy flourish».[15] The collective actions involve hundreds of thousands of consumers « demanding a minimum compensation of €200 per user as compensation for the alleged privacy infringements and unfair commercial practices the platform is responsible for».[16] Similarly, a massive multidistrict litigation consolidated numerous legal actions across the USA in September 2019.[17] In the associated decision, Judge Chabria wrote « Facebook's motion to dismiss is littered with assumptions about the degree to which social media users can reasonably expect their personal information and communications to remain private … Facebook argues that people have no legitimate privacy interest in any information they make available to their friends on social».[18] As the deciding judges emphasized « Facebook's view *could not be more wrong*» (the italics is our), thus clearing the way for a multibillion litigation for privacy violations.[19] In Illinois, a similar action was filed as a result of the alleged misuse of Facebook users' biometric personal data. The claim of the action is that Facebook « illegally collected and stored biometric data from millions of users without their consent » which is explicitly prohibited by the Illinois Biometric Information Privacy Act. In case of unfavorable verdict, the defendant may be liable to pay a compensation from 1000 to 5000 dollars for each violation, depending on whether the latter will be considered intentional or reckless.[20] The Illinois action alone involves more than seven million users. At the time of writing this article, Facebook announced the settlement of the Illinois class action for 550 million dollars. One of the lead attorney emblematically claimed, «I hope and expect that other companies will follow Facebook's lead».[21]

While users were voicing growing concerns for the protection of their privacy, public authorities and regulators started to enforce the legislation on consent requirement with unseen severity. On July 24th' 2019, for instance, the Federal Trade Commission (hereafter, FTC) fined Facebook with a five billion penalty for violating the Consent Order of 2012.[22] In the announcement, the commissioners emblematically wrote, «if you've ever wondered what a paradigm shift looks like, you're witnessing one today».[23] Similarly, Google reached an agreement with the FTC to pay 170 million dollars for illegally collecting data on children[24]; the Italian Competition Authority (AGCOM) fined Facebook Ireland and Facebook Inc. for a total of 10 million euros[25]; the French Conseil National Informatique et

[13] See Saint (2010) and the settlements reported by Ballon (2016: 336). "Fraley v. Facebook, Inc., 638 F. App'x 594 (9th Cir. 2016) (affirming approval of cy pres class action settlement); Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012) (approving an attorneys' fee award of $2,364,973.58 and a $9.5 million cy pres class action settlement in a suit over Facebook's beacon program brought under the Electronic Communications Privacy Act, Video Privacy Protection Act, Computer Fraud and Abuse Act, the California Consumer Legal Remedies Act, and California Computer Crime Law (Cal. Penal Code § 502), and for remedies for unjust enrichment), cert. denied, 134 S. Ct. 8 (2013); In re Yahoo Mail Litigation, No. 13-cv-4980-LHK, 2016 WL 4474612 (N.D. Cal. Aug. 25, 2016) (granting final approval of a class action settlement); Perkins v. LinkedIn Corp., Case No. 13-CV-04303-LHK, 2016 WL 613255 (N.D. Cal. Feb. 16, 2016) (granting final approval of a class action settlement)".

[14] See, e.g., Cain v. Redbox Automated Retail, LLC, No. 12-CV-15014, 2015 WL 5728834 (E.D. Mich. Sept. 30, 2015).

[15] Patrick van Eecke (September, 18 2018) EUROPE: European consumers organizations launching collective GDPR actions. Lexology, retrieved at: https://www.lexology.com/library/detail.aspx?g=8ee34a2a-6567-4f30-9939-aa1847cfb577. To keep track of the several collective lawsuits, see: http://www.mydataismine.com/.

[16] Ivi.

[17] In re Facebook, Inc., Consumer Privacy User Profile Litig., MDL No. 2843 N.D. Cal. Sep. 9, 2019.

[18] Stempel Jonatan (September 9, 2019) Judge lets Facebook privacy class action proceed, calls company's views "so wrong". Reuters, retrieved at: https://www.reuters.com/article/us-facebook-lawsuit-privacy/judge-lets-facebook-privacy-class-action-proceed-calls-companys-views-so-wrong-idUSKCN1VU2G2.

[19] In re Facebook, Inc., Consumer Privacy User Profile Litig., MDL No. 2843 N.D. Cal. Sep. 9, 2019.

[20] See, Jonathan Stempel (August 8,2019) Facebook loses facial recognition appeal, must face privacy class action. Reuters. retrieved from https://www.reuters.com/article/us-facebook-privacy-lawsuit/facebook-loses-facial-recognition-appeal-must-face-privacy-class-action-idUSKCN1UY2BZ.

[21] Jeff Horwitz, (January 30, 2020) Facebook Reaches $550 Million Settlement in Facial-Recognition Lawsuit. The Wallstreet Journal, retrieved https://www.wsj.com/articles/facebook-reaches-550-million-settlement-in-facial-recognition-lawsuit-11580347594.

[22] Cecilia Kang, (July 12, 2019) F.T.C. Approves Facebook Fine of About $5 Billion. The New York Times. retrieved from https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.htm.

[23] The FTC declared the data transfer to third parties incompatible with the consent order « one specific count alleged that Facebook allowed users to choose settings that supposedly limited access to their information just to "friends" without adequate disclosures that another setting allowed that same information to be shared with the developers of apps those friends used». To settle the case, Facebook agreed to an order that, among other things,: 1) prohibited the company from making misrepresentations about the privacy or security of consumers' information, 2) prohibited the company from misrepresenting the extent to which it shares personal data, and 3) required Facebook to implement a reasonable privacy program.

[24] Rob Copeland (September 4, 2019) You Tube Agrees to 170 $ Fine, New Protections for Children. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/youtubes-ftc-penalty-exposes-divisions-among-federal-regulators-11567602817.

[25] According to the AGCOM, Facebook misled « users in the sign-up process about the extent to which the data they provide would be used for commercial purposes», avoiding to fully disclose the «profitable ends that underlie the provision of the social network» and «forcing an "aggressive practice" on registered users by transmitting their data to third parties, and vice versa, for commercial purposes».

Libertés (CNIL) fined Google LLC with fifty million euros for « violations of obligation of transparency and information under the GDPR»; while in Germany, the Bundesgerichtshof upheld the Bundeskartellamt's decision to prohibit Facebook to combine the data collected by other Facebook-owned services unless subscribers give the platform the explicit consent to do so.[26]

In addition to these contractual and private law infringements, apex constitutional courts and independent authorities underwent a deep scrutiny of the compatibility between fundamental rights and the platforms' business model based on profiling activities (Hijmans, 2016; Cherednychenko, 2016). Pivotal role has been played by the European Court of Justice, which adopted a series of ground-breaking decisions to integrate the digital and the analog world into the unifying framework of the European law of fundamental rights. Digital Rights Ireland,[27] Google Spain[28] and Schrems[29] are other exemplar cases[30] to "see" an historical shift in the regulators' understanding of the digital world.

3. The model: timing and setup

In this section, we develop a social custom model inspired by the stylized facts reported in the above. More precisely, we study a two-stage game where a unit-mass of heterogenous individuals interact through a social media supplied by a single provider.[31] The timing of the game is as follows.

In the first stage (the "policy stage"), the provider realizes its data-driven profits by choosing the amount of information she gathers from its users. In doing so, it internalizes the effect of its activities on its subscribers' decision to litigate for privacy violations. To keep things simple, we assume that the provider optimally selects a single decision variable $\delta \geq 0$ which measures both the quantity and sensitivity of information and the extent to which this is processed and monetized.

In the second stage (the "litigation stage"), users decide whether to remain online and accept the provider's policy (strategy *NL*) or abandon the social media and litigate for privacy violations (strategy *L*). Due to the incompleteness of privacy-related institutions—see section 2.1—the lawfulness of the platform's data-gathering activities is unclear, so that users form ideas on the provider's policy by evaluating the trade-off between the benefits and costs of social media use. Our working hypothesis is that web-mediated interactions involve benefits in terms of consumption of relational goods—see Antoci et al. (2012) and the reference therein—and costs in terms of privacy protection—see Ellison et al. (2012) and the references therein. In addition, we assume that the perception of these costs aggravates with the share of individuals who litigate for privacy violations, indicated as $0 \leq \lambda \leq 1$. In this framework, the individual decision to litigate creates a feedback effect which affects the behavior of the rest of the users' population, thus generating the possibility of multiple equilibria in the dynamics of litigation.

As we are not interested in studying the relationship between the platform's policy and the various strategies of information disclosure—for a review, see Ellison et al. (2012) and the references therein—we assume that web-mediated interactions occurred before the starting of the game. In this framework, the users' decision to disclose their information is not affected by the platform's policy. Hence, we consider a situation where the platform must decide how to treat and monetize the informational capital that has been previously created by its subscribers.

The game is studied by backward induction. In section 4, we derive the equilibrium density of litigators; in section 5, the provider's optimal policy. Hence, we shall look for a couple (λ^*, δ^*) that describes the equilibrium of the game.

4. The litigation stage

4.1. Assumptions and payoffs

In the second stage of the game, subscribers decide whether to leave the platform and litigate for privacy violations (strategy *L*) or remain online and accept the provider's policy (strategy *NL*). In this framework, the decision to litigate is driven by the size of the damage compensation (net of litigation costs) compared to the size of the relational benefits (net of privacy costs). In what follows, we shall specify the relationship between these benefits and costs and the intensity of data-gathering $\delta \geq 0$.

Our working hypothesis is that data-gathering has a positive effect on the users' relational well-being, as it improves their online visibility and facilitates their consumption of relational goods. To refer to this mechanism in an intuitive way, we call it the "social visibility effect". In formal terms, we specify the relational benefits of online socialization as an increasing function of the platform's data-gathering activities. In particular, we express these benefits as $\beta\delta$, where $\beta > 0$. Implicit in this specification is the Assumption that

[26] German Federal Supreme Court, 23 June 2020, decision on Facebook versus Bundeskartellamt Nr. 80/2020. For more information see https://www.huntonprivacyblog.com/2020/06/30/german-bgh-decision-confirms-interplay-between-collection-of-personal-data-and-competition-law/.

[27] EUCJ, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others (2014) ECLI:EU: C:2014:238.

[28] Case C −131/12, Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez [2014].

[29] EJEU, Case C-362/14 Maximillian Schrems v Data Protection Commissioner (2015) ECLI:EU: C:2015:650.

[30] Last is the landmark Grand Chamber judgment of 16 July 2020, where the CJEU confirmed the importance of privacy as a fundamental right and reaffirmed the need to protect users' personal data transferred from the European Union to third countries. See Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems". Retrieved at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[31] A further limitation of our model is that we do not consider the role of market competition on the platform's behavior. We leave this possibility for future research.

all users derive the same level of relational utility from their web-mediated interactions.

Conversely, we assume that the perception of the privacy costs is subjective, as users may have different information of or accord different attention to the platform's data-gathering activities. In formal terms, we assume that the ith-user incurs a privacy cost $-\alpha_i$ when using the social media, where α is assumed to be uniformly distributed over 0 and an upper bound $\overline{\alpha} > 0$ according to the probability density function $f(\alpha)$.[32] To reflect the linkage between the provider's decision (measured by $\delta \geq 0$) and the users' perception of the privacy costs, we follow Chang and Lai (1999) and assume that the upper bound of the belief distribution varies with the level of δ via:

$$\overline{\alpha}(\delta) = \alpha_0 + \gamma\delta \tag{1}$$

where $\alpha_0 > 0$ is a constant and $\gamma > 0$ is a coefficient that captures the shift in the distribution of beliefs following an increase in data-gathering. Ceteris paribus, when the provider collects, processes and monetizes more of its subscribers' information, the latter perceive the privacy implications of web-mediated interactions as more severe. We call this mechanism the "privacy effect". Combining this with the "social visibility" effect described in the above, our modelling strategy implies that the provider's policy has an ambiguous effect on the users' decision to litigate—for further discussions, see section 5.1.

In line with previous contributions in the literature on social custom—see Akerlof (1980); Booth (1985); Naylor (1990); Myles and Naylor (1996); Chang and Lai (1999); Chang and Lai (2002)—we assume that the users' subjective perception of the privacy costs varies with the number of litigators in the economy, as users interpret litigiousness in courts as a signal of data violation. Recalling that the mass of the users' population is normalized to 1 and the share of litigators is measured by $1 \leq \lambda \leq 0$, we assume that the socially influenced perception of the ith-user is given by $-\alpha_i\lambda$. Hence, for any given value of α over the interval $[0, \overline{\alpha}]$, the greater the size of the litigators' group, the greater the emphasis that users put on the privacy implications of web-mediated interactions. As we shall see, this feedback effect has major implications on the outcome of the game, as the system may gravitate towards different equilibria depending on the initial frequency of litigators in the economy.[33]

Putting together the above definitions of relational benefits and privacy costs, we can write the utility function of a non-litigator as:

$$U^{NL} = \beta\delta - \alpha_i\lambda \tag{2}$$

Conversely, as litigators are assumed to abandon the social media, their utility does not depend on the benefits and costs of online socialization, but rather, on the benefits and costs of filing a case for privacy violations. Formally, we write these benefits and costs as:

$$U^{L} = q_U F - C \tag{3}$$

where $0 \leq q_U \leq 1$ measures the users' ex-ante expectation (belief) of winning the trial, $F > 0$ the damage compensation and $C > 0$ the litigation costs.[34] From an ex-ante perspective, equation (3) can be referred to as measuring the "incentives to litigate", about which we make the following reasonable Assumption:

Assumption 1. *ex-ante, the users' expectation of winning the trial is not so low to make it irrational for the individual user to litigate for privacy violations. Parametrically, this corresponds to* $q_U > C/F$*—so that* $q_U F - C > 0$.

The ith-user will join the litigators' group if and only if $U^L > U^{NL}$, or alternatively, if the incentives to litigate measured by equation (3) are greater than the benefits of using the social media, measured by equation (2). In what follows, we shall look for a value of αwhich makes the idiosyncratic user just indifferent between litigating and not, that is, for a value α^* which satisfies $U^L = U^{NL}$, or, alternatively:

$$\alpha^*\lambda - \beta\delta + q^U F - C = 0 \tag{4}$$

Since all users with $0 \leq \alpha_i < \alpha^*$ will play L, while all users with $\alpha^* \leq \alpha_i < \overline{\alpha}$ will play NL, the critical threshold α^* separates the population in two groups, litigators and non-litigators. From the Assumption of the uniform distribution of α, it is straightforward to derive the density of the litigious group as:

$$\lambda = \int_{\alpha^*}^{\overline{\alpha}} f(\alpha)\mathrm{d}\alpha = 1 - \alpha^* \Big/ \overline{\alpha} \tag{5}$$

Which entails that $\alpha^* = (1 - \lambda)\overline{\alpha}$. To analyze the formation of the equilibrium share of litigators, we follow previous contributions in the literature on social customs—see e.g. Booth (1985) and Chang and Lai (1999)—and assume that the stationary density of the litigious

[32] The Assumption of the uniform distribution implies that a change in the intensity of data-gathering affects not only the spread of the interval but also the mean of the subjective perception of the privacy costs.

[33] To some extent, this is consistent with the sociological notion of the "social construction of risk", whereby « risk and safety are not objective conditions "out there" [but] exist in and through social organization» (Stallings, 1980: 80; see also Covello and Jhonson, 1987). In this framework, the individual decision to litigate creates a feedback effect that determines how and if the "privacy risk" of social media use emerges as a social construction.

[34] We anticipate that the parameter q^Uwill allow us to investigate the role of institutional incompleteness in the dynamics of litigation. In the absence of clear rules that regulate data ownership, in fact, data buyers and sellers may develop diverging expectations on the outcome of privacy trials, and this, in turn, may have offsetting implications for the equilibrium configurations of the game.

group evolves according to the following (payoff monotonic) dynamics:

$$\dot{\lambda} = k(U^L - U^{NL}) = k(\alpha_i \lambda - \beta\delta + q_U F - C) \tag{6}$$

where an overdot indicates the rate of change with respect to time and $k > 0$ is the speed of adjustment. Equation (6) states that the share of litigators in the economy will grow when the incentives to litigate measured by equation (3) exceed the utility from using the platform measured by equation (2), that is, when the utility of litigating is greater that the utility of non-litigating ($U^L > U^{NL}$).[35]

In what follows, we shall look for a stationary value λ^* that satisfies $\dot{\lambda} = 0$, that is, for the equilibrium share of litigators which leads the dynamics described in equation (6) to a steady state. Recalling that α^* is implicitly defined by equation (4) as the critical value of α that separates the users' population in litigators and non-litigators, we make use of equations (5) and (1)and substitute the relations $\alpha^* = (1-\lambda)\overline{\alpha}$ and $\overline{\alpha}(\delta) = \alpha_0 + \gamma\delta$ in equation (6). By doing so, we derive the expression which implicitly defines the stationary density λ^* that satisfies $\dot{\lambda} = 0$, which is given by:

$$k[\lambda(1-\lambda)(\alpha_0 + \gamma\delta) - \beta\delta + q_U F - C] = 0 \tag{7}$$

Since equation (7) has two roots, the dynamics of litigation admits multiple equilibria. The next task is to inquire further in the stability properties of these equilibria and investigate the role of initial conditions on the long-run evolution of the system.

4.2. Multiple equilibria of litigation

Following Naylor (1990) and Chang and Lai (1999, 2002), we visualize the relationship between equations (5)and (6) in the α, λ plane reported in Fig. 1. The $\dot{\lambda} = 0$ locus depicts the pairs of λ and α that satisfies $\dot{\lambda} = 0$ in equation (6). To appreciate that the $\dot{\lambda} = 0$ locus is a triangular hyperbola as depicted in Fig. 1, observe that:

$$\left.\frac{\partial \lambda}{\partial \alpha^*}\right|_{\dot{\lambda}=0} = -\frac{\lambda}{\alpha^*} < 0$$

and,

$$\left.\frac{\partial^2 \lambda}{\partial \alpha^{*2}}\right|_{\dot{\lambda}=0} = \frac{\lambda}{\alpha^{*2}} > 0$$

In addition, the relation $\partial\dot{\lambda}/\partial\alpha > 0$ implies that the number of litigators will rise (resp., fall) in the area which is at the right (resp., left) of the $\dot{\lambda} = 0$ locus, as indicated by the arrows that point upward (resp., downward) at the right (resp., left) of $\dot{\lambda} = 0$ locus.

Conversely, the *DS*locus visualizes the pairs of λ and α that satisfies the distribution schedule *DS* derived in (5). To appreciate the fact that the *DS* locus is a downward sloping line as reported in Fig. 1, observe that:

$$\left.\frac{\partial \lambda}{\partial \alpha^*}\right|_{DS} = -\frac{1}{\overline{\alpha}} < 0$$

and,

$$\left.\frac{\partial^2 \lambda}{\partial \alpha^{*2}}\right|_{DS} = 0$$

From Fig. 1, we see that the graphs of the $\dot{\lambda} = 0$ and *DS* loci intersect twice, at *T* and *S*. Hence, we have two possible equilibria, the stability properties of which are analyzed in the following Proposition:

Proposition 1. *The dynamics in equation (6) has two boundaries, at $\lambda = 0$and $\lambda = 1$, and two stationary points, at $\lambda_S = 1/2 + \epsilon$and $\lambda_T = 1/2 - \epsilon$, with $\epsilon > 0$. The densities $\lambda = 0$ and λ_S are stable equilibria, while $\lambda = 1$ and λ_T are unstable. In particular, λ_T can be viewed as a threshold for litigation to escalate: if initially $0 < \lambda < \lambda_T$, the equilibrium density of litigators will be pushed to $\lambda = 0$, while, if $\lambda_T < \lambda < 1$, it will converge to λ_S.*

[35] As anticipated in the introduction, a key limitation of our model is that we collapse the users' online and offline behavior. In doing so, we rule out the possibility that individuals may keep using the platform when filing a case for privacy violations. A more sophisticated model would allow the investigation of complex (and thus more realistic) behavioral patterns. As a partial justification for this limitation, we advance the following remarks. First, let us define $\widehat{\alpha}$as the threshold belief that satisfies $\beta\delta - \widehat{\alpha}\lambda < 0$. Second, observe that all the agents with idiosyncratic beliefs $\alpha_i \geq \widehat{\alpha}$would quit using the platform even in the absence of any incentives to litigate, as remaining online would entail a net utility loss. Third, since Assumption 1 ensures that the incentives to litigate are always positive, all the individuals with $\alpha_i \geq \widehat{\alpha}$would also find it rational to go to Court. In short, this entails that our model only rules out the possibility that the individuals who experience a net utility gain from using the platform (those who have $\alpha_i < \widehat{\alpha}$) may however decide to exploit the positive incentives to litigate and file a case for privacy violations. Despite admittedly limiting, imposing this kind of "coherence" between online and offline behavior seems acceptable to preserve the tractability of the model.

Table 1
Each column reports the effect of changing the parameter's value on the equilibrium and threshold densities λ_S and λ_T.

	$/\partial F$	$/\partial q^U$	$/\partial C$	$/\partial \beta$	$/\partial \gamma$	$/\partial \delta$
$\partial \lambda_S$	>0	>0	<0	<0	>0	$\gtrless 0 \Leftrightarrow \lambda(1-\lambda)\gamma \gtrless \beta$
$\partial \lambda_T$	<0	<0	>0	>0	<0	$\gtrless 0 \Leftrightarrow \lambda(1-\lambda)\gamma \lessgtr \beta$

Proof: see the Appendix.

Proposition 1 highlights the snowballing characteristic of our model and draws attention to the social externality of filing a case for privacy infringements. Given the Assumption that users interpret litigiousness in court as a signal of data violation, the individual decision to litigate creates a feedback effect which generates a critical mass situation. When litigators are initially scarce, litigation die out; when litigators are initially abundant, litigation become endemic.

Albeit admittedly stylized, we believe that this result can be used to comment the mechanism whereby the users' orientation towards social media companies emerged as a social construction. In the heyday of platform diffusion, users put relative emphasis on the relational benefits of web-mediated interactions and accorded little or no attention to their privacy implications. Accordingly, the number of privacy-related trials remained contained. Conversely, as the initial frenzy for the novel socialization opportunities begun to wane, the privacy implications of web-mediated interactions became clearer and more massively addressed in courts. In a multiple equilibria framework like ours, sudden behavioral changes of this sort can be interpreted as a shift from one equilibrium configuration to another.

It should be noted that a number of reasons that are left outside the model may have played a key role in this transformation. Scandals like the Snowden Revelations and Cambridge Analitica, for instance, may have altered the collective perception of social media companies and thus modified the balance between the "social visibility" and the "privacy" effect. The changes in the orientation of public authorities and regulators described in section 2.1 may also have had a similar effect. In the context of our model, exogenous shocks of this sort can be rationalized as an increase of the coefficient γ in equation (1).

With this, we have completed the analysis of the users' behavior. The next task is to study the platform's data-gathering policy.

5. The policy stage

5.1. Social visibility and privacy: an ambiguous effect

In order to study the platform's policy in the first stage of the game, we need to understand how the intensity of data-gathering $\delta \geq 0$ affects the equilibrium share of litigators. To do so, we perform comparative statics on the stationary densities λ_T and λ_S. Recall that λ_S is a stable equilibrium, while λ_T is unstable, so at no time the economy will converge to such point. Due to the pervasiveness of legal uncertainty, however, both stationary densities convey a relevant information. On the one hand, λ_S measures the number of litigators in case the game reaches the litigation stage—which occurs whenever $\lambda_T < \lambda < 1$—and thus, it can be treated as a proxy of the intensity of litigation. On the other hand, λ_T measures the likelihood of reaching the litigation stage. When the equilibrium share of litigators λ_S increases, the conflict intensifies; when the threshold share of litigators λ_T increases, the conflict becomes less likely.

The signs of the comparative statics reported in Table 1 are intuitive and deserve no further attention, but for the cases in the last column of Table 1. Here, the effects of the platform's choice on the equilibrium and threshold shares of litigators are explicitly analyzed. Due to the interplay between the "social visibility" and the "privacy" mechanisms described in the above, it is straightforward to see that the provider's policy has an ambiguous effect on the users' decision to litigate, which is summarized in the following Proposition:

Proposition 2. *The effect of the provider's policy on both the intensity $\lambda_S$and the likelihood $\lambda_T$of the litigation stage is ambiguous and depends on the interplay between the "social visibility" and the "privacy" effect. When the former is stronger than the latter—$\beta \geq \gamma/4$—intensifying data-gathering decreases both the intensity and the likelihood of the litigation stage—$\partial\lambda_S/\partial\delta < 0$ and $\partial\lambda_T/\partial\delta > 0$. Conversely, when the former is weaker than the latter—$\gamma > 4\beta$—the effect of the platform's policy is mediated by the values of the equilibrium and threshold densities $\lambda_S$and λ_T. Defining $1/2 + [(\gamma + 4\beta)/4\gamma]^{1/2} \equiv \widehat{\lambda}$and $1/2 - [(\gamma + 4\beta)/4\gamma]^{1/2} \equiv \tilde{\lambda}$, we see that:*

(i) *If $\lambda_T < \lambda_S < \tilde{\lambda} < \widehat{\lambda}$ or $\tilde{\lambda} < \widehat{\lambda} < \lambda_T < \lambda_S$, intensifying data-gathering decreases both the intensity and the likelihood of the litigation stage—$\partial\lambda_S/\partial\delta < 0$ and $\partial\lambda_T/\partial\delta > 0$.*

(ii) *If $\lambda_T < \tilde{\lambda} < \lambda_S < \widehat{\lambda}$, intensifying data-gathering increases the intensity of the litigation stage but decreases its likelihood—$\partial\lambda_S/\partial\delta > 0$ and $\partial\lambda_T/\partial\delta > 0$.*

(iii) *If $\tilde{\lambda} < \lambda_T < \lambda_S < \widehat{\lambda}$, intensifying data-gathering increases both the intensity and the likelihood of the litigation stage—$\partial\lambda_S/\partial\delta > 0$ and $\partial\lambda_T/\partial\delta < 0$.*

(iv) *If $\tilde{\lambda} < \lambda_T < \widehat{\lambda} < \lambda_S$, intensifying data-gathering decreases the intensity of the litigation stage but increases its likelihood—$\partial\lambda_S/\partial\delta < 0$ and $\partial\lambda_T/\partial\delta < 0$.*

Proof: see the Appendix.

Fig. 2 depicts the pairs λ_S and λ_T in the space $0 < \tilde{\lambda} < \widehat{\lambda} < 1$ corresponding to the cases (i)-(iv) of Proposition 2, while Fig. 3 serves as

a supplementary tool to analyze the effect of δon the values of the threshold and equilibrium densities $\lambda_T$and λ_S. Consider a platform that initially sets $\delta = \delta_0$. In this case, if $0 < \lambda < \lambda_T(\delta_0)$, the equilibrium density of litigators will be pushed to $\lambda = 0$; conversely, if $\lambda_T(\delta_0) < \lambda < 1$, the equilibrium density will converge to $\lambda_S(\delta_0)$. In response to an increase in data-gathering by the provider from δ_0 to δ_1, both DS and $\dot{\lambda} = 0$ shift rightwards,[36] while both λ_S and λ_T shift downwards. In this case, the intensity of the litigation stage decreases, but its likelihood increases. This situation corresponds to case (iv) of Proposition 2.

5.2. The provider's policy

In what follows, we study the provider's decision in the context of the privacy/social visibility ambiguity analyzed in the previous section. Our working hypothesis is that the provider selects $\delta \geq 0$ considering both the likelihood and the intensity of the litigation stage, measured, respectively, by the threshold and equilibrium densities λ_T and λ_S. This amounts to assuming that the provider knows that a group of subscribers of size λ_S may decide to litigate in the second stage of the game, but that this group can only form if the initial share of litigators λ is sufficiently large, that is, if $\lambda > \lambda_T$. Foreseeing that the game may not reach the litigation stage, in fact, the provider may impose fewer limitations on its data-gathering activities. To allow for this possibility, we need to make a specific Assumption on the distribution of λ. To keep things simple, we assume that λ is uniformly distributed over the interval $[0, 1]$. Finally, we assume that the platform selects the intensity of data-gathering $\delta \geq 0$ by solving the following problem:

$$\max_{\delta \geq 0} \Pi = P(\lambda_T < \lambda \leq 1)(\pi(\delta) - \lambda_S q_P F) + [1 - P(\lambda_T < \lambda \leq 1)]\pi(\delta) \tag{8a}$$

where $\pi(\delta)$ is a revenue-generating function that depends positively on the intensity of data-gathering δsuch that $\pi(0) = 0$, $\pi'(\delta) > 0$ and $\pi''(\delta) < 0$ and $F > 0$ is the damage compensation the provider expects to pay when it loses the lawsuit, which happens with the subjective probability (belief) $0 \leq q_P \leq 1$. In addition, $P(\lambda_T < \lambda \leq 1)$is the probability that the initial share of litigators is above the critical threshold. In this case, the game reaches the litigation stage, and the provider discounts its profits for the expected damage compensation weighted for the density of the litigious group. Conversely, when λ is below the critical threshold—which happens with probability $1 - P(\lambda_T < \lambda \leq 1)$—the game does not reach the litigation stage, and the provider realizes its data-driven profits without any legal consequence. Given the Assumption of the uniform distribution of λ, it is easy to derive that $P(\lambda_T < \lambda \leq 1) = (1 - \lambda_T)$, so that $1 - P(\lambda_T < \lambda \leq 1) = \lambda_T$. Substituting these relationship in equation (8), we can rewrite the provider's problem as:

$$\max_{\delta \geq 0} \Pi = (1 - \lambda_T)(\pi(\delta) - \lambda_S q_P F) + \lambda_T \pi(\delta) = \pi(\delta) - \lambda_S(1 - \lambda_T) q_P F \tag{8b}$$

The first order condition for optimal profits are given by:

$$\frac{\partial \pi(\delta)}{\partial \delta} - \left[\frac{\partial \lambda_S}{\partial \delta}(1 - \lambda_T) - \frac{\partial \lambda_T}{\partial \delta}\lambda_S\right] q_P F = 0 \tag{9}$$

where we have already established that both $\partial\lambda_S/\partial\delta$ and $\partial\lambda_T/\partial\delta$ are ambiguously signed—see Table 1 and the discussion in section 5.1. Interestingly, when the providers' policy decreases both the intensity and likelihood of the litigation stage—i.e., $\partial\lambda_S/\partial\delta < 0$ and $\partial\lambda_T/\partial\delta > 0$—the first order condition is violated. In this case, the platform should impose no limitations to its data-gathering activities. Conversely, there exist parametrizations for which the argument in equation (9) is negatively signed. In this case, the platform should avoid collecting its users' information. In all other cases, we assume that an interior solution exists, is unique, and that the second order conditions are satisfied.

In the same spirit of the discussion at the end of section 4, we believe that these results can be used to remark on the platforms' strategic behavior over the last decade or so. Back in the days when users put little or no attention to privacy-related issues, social media companies imposed little or no limitation to their data-gathering activities, interpreting the diffusing hype for online interactions as a green light to their data-driven businesses. Accordingly, the number of privacy-related trial remained contained. Now that users are increasingly concerned with the problem of informational security and the number of privacy-related trials is mounting, service providers are seemingly reconsidering their business model. During Facebook's annual developer conference of 2019, for instance, Zuckerberg declared that "the future is private", stressing how the social media's configuration must evolve to adapt to its subscribers' novel demand for privacy.[37] During its keynote, he detailed six core pillars of what the new privacy-focused Facebook should look like (e.g., encryption, ephemeral messaging). All these pillars seem to require a radical downsizing of the platform's data-gathering activities. Whether and how these guidelines will actually translate in the platform's reorganization, is still to be seen.

[36] From equations (5) and (6) we have that $\partial\alpha/\partial\delta|_{\dot{\lambda}=0} = \beta/\lambda > 0$and $\partial\alpha/\partial\delta|_{DS} = (1 - \lambda)\gamma > 0$. Observe that the shift of the $\dot{\lambda} = 0$locus is governed by the "social visibility" effect (measured by the parameter $\beta > 0$), while the shift of the *DS*curve is governed by the "privacy" effect (measured by the coefficient $\gamma > 0$).

[37] Christian de Looper, (April 30, 2019) Facebook says the future is private, but what does that mean? Digitaltrends. Retrieved from https://www.digitaltrends.com/social-media/facebook-says-the-future-is-private-but-what-does-that-mean/.

6. The role of institutional incompleteness

In this section, we analyze the role of institutional incompleteness on the equilibrium outcome of the game. The intuition is as follows. When institutions are incomplete, the parties may develop different expectations on the outcome of judicial decisions and thus, base their strategies on a set of ex-ante diverging beliefs.[38] In the context of our model, this possibility is given by the fact that q_U and q_P may take different values, where we recall that $1 \leq q_U \leq 0$ (resp., $1 \leq q_P \leq 0$) measures the users' (resp., the provider's) subjective probability of winning (resp., losing) the trial. Hence, we can formulate the following Proposition:

Proposition 3. *For any given set* $\{\lambda, \gamma, \beta, \delta, \pi(\delta), F, C\}$*, there exist threshold beliefs* $\overline{q_P}$ *and* $\overline{q_U}$ *for which:*

(i) *If* $q_P > \overline{q_P}$*, the platform does not engage in data-gathering;*

(ii) *If* $q_P \leq \overline{q_P}$ *and* $q_U < \overline{q_U}$*, the platform engages in data-gathering but users do not litigate;*

(iii) *If* $q_P \leq \overline{q_P}$ *and* $q_U > \overline{q_U}$*, the platform engages in data-gathering and users litigate.*

Proof: see the Appendix.

Borrowing from Ichino et al. (2003), we visualize the equilibrium outcomes of the game in Fig. 4.[39] In dynamic terms, it is clear that unanticipated shifts in the players' expectations may transport the game from an equilibrium configuration to another, with offsetting implications for the parties involved. Ultimately, this results in a word of caution. When institutions are incomplete, the process of technological innovation unfolds over fragile legal foundations. Despite innovators may temporarily benefit from these periods of institutional uncertainty, unanticipated waves of behavioral change may rapidly backfire on the newborn activities, pushing entrepreneurs to ask for a bit of institutional clarity.[40]

The inability of institutions to keep up with the process of technological change is surely not new. This "pacing problem", according to Collingridge (1980), is twofold. On the one hand, the impact of new technologies cannot be anticipated before they are fully developed. On the other hand, the more these technologies are adopted, the harder it gets to control and modify their uses. In the face of such instability, a policy choice has to be done. It is that of deciding whether to delegate the edification of the legal foundations of the newborn industries to innovators ("decentralized" or "laissez-faire" regulation), or to resort to more comprehensive intervention with stronger recourse to top down solutions ("centralized" regulation).[41] Centralized regulation reduces legal uncertainty, but it may impose excessive limitations on the implementation of new technologies. Decentralized regulation, on the other hand, is innovation-enhancing, as it allows entrepreneurs to use their "Hayekian" knowledge (Hayek, 1945) and find a proper balance between their customers' wants and theirs. However, when entrepreneurs underestimate the risks associated with the emerging technologies, this mode of regulation may eventually result in waves of institutional tension, as exemplified by the recent boom of privacy-related litigation.

7. Conclusion

This article analyzes the effect of data-gathering by online platforms on their subscribers' willingness to litigate for privacy violations. It does so by developing a social custom model where a population of users interacts through a social media supplied by a single provider. By allowing the users' concerns for informational security to co-evolve with the number of privacy-related trials, it tries to make sense of a series of stylized facts related to privacy issues in online interactions. In both its simplicity and abstractedness, we believe that the model's message is twofold. First, it highlights a link between the users' orientation towards social media companies and the individual decision to litigate for privacy violations. Second, it provides a rationale to link the design of the platforms' data-gathering policies to the oscillating behavior of their subscribers.

Without putting excessive emphasis on the model's explanatory power, we believe that a couple of equilibrium configurations are worth mentioning for their ability to quasi-reproduce the coevolution of the platforms' policies and the users' behavior. In the first scenario, (i) users put relative emphasis on the relational benefits of online interactions, (ii) privacy-related trials remained contained and (iii) the provider imposes no limitations to its data-gathering activities. In the second scenario, (i) users put relative emphasis on the privacy costs of web-mediated interactions, (ii) privacy-related trials become endemic and (iii) platforms modulate their data-gathering activities by mediating between profitability and the legal implications of their choice.

[38] The law and economics literature acknowledged the possibility of diverging expectations as a key reason for the occurrence of trials—see e.g., Waldfogel (1998).

[39] From Fig. 4, it is clear that the possibility of diverging expectations is not the only reason for the occurrence of a trial. Indeed, there exists an area along the 45°diagonal where the parties have converging expectations and, nevertheless, litigation escalates. As recalled by Ichino et al. (2003), the existence of asymmetric stakes, in this case, is the reason why a trial occurs.

[40] Interestingly, platforms themselves have recently started to ask for a more severe regulation of the internet. "I believe we need a more active role for governments and regulators" Zuckerberg wrote in an editorial published in the Washington Post, "by updating the rules for the internet, we can preserve what's best about it". Mark Zuckerberg (March 30, 2019). The Internet needs new rules. Let's start in these four areas. The Washington Post Retrieved from https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

[41] Approaches to regulate risk in emerging technologies have been divided into technology-based, performance-based and management-based regulation, going from the more interventionist but less innovative-enhancing, to the more "laissez-faire" but also risky mode of regulation. For a review, see Fuchs et al. (2017).

Ultimately, we believe that the possibility of these multiple equilibria can be used to remark on the importance for institutions to promptly respond to the process of technological change. Despite various forms of laissez-faire regulation can foster innovation, they may also result in periods of institutional uncertainty and tension, with offsetting implications for profitability, organization and consumer well-being. In a world that is constantly transforming, it will be for policy-makers to decide which between the two is the lesser evil.

Compliance with ethical standards

This research did not receive any specific grant from funding agencies in the public, commercial or not-for-profit sectors.

Declaration of competing interest

None.

Data availability

No data was used for the research described in the article.

Acknowledgements

The authors would like to thank Alain Marciano, Fabio Landini, all the participants to the SIDE 2019 conference and to the Cognetti de Martiis seminar held on the 18th of June 2020 at the University of Turin for helpful comments on an earlier version of the paper. We are particularly indebted to two anonymous referees and the handling editor, Toke Aidt, whose suggestions considerably helped reshape the paper. All errors and omissions remain our own.

Appendix

1. Proof of Proposition 1

To prove the stability properties of λ_S and λ_T we need to take a closer look at Fig. 1. As anticipated, the relationship $\partial\dot{\lambda}/\partial\alpha > 0$ implies that the density of litigators will rise (resp., fall) in the region at the right (resp., left) of the $\dot{\lambda} = 0$ locus. In addition, observe that the condition derived in equation (5) is a definite relationship, so at no time the economy is allowed to deviate from it. Putting together these two insights, it is clear that the density λ_S is attractive while the density λ_T is repulsive, as suggested by the laws of motion in Fig. 1 As a further proof, observe that the $\dot{\lambda} = 0$ locus is steeper than the DS schedule at S. As the slope of the $\dot{\lambda} = 0$ curve is given by $\partial\lambda/\partial\alpha^*|_{\dot{\lambda}=0} = -\lambda/\alpha^*$ while the slope of the DS curve is given by $\partial\lambda/\partial\alpha^*|_{DS} = -1/\overline{\alpha}$, the stability requirement involves $-\lambda/\alpha^* < -1/\overline{\alpha}$, which entails $\lambda > 1/2$, which is always satisfied at S—since $\lambda_S = 1/2 - \varepsilon$—and never satisfied at T—since $\lambda_T = 1/2 - \varepsilon$, where $\varepsilon \equiv [\alpha_0 + \gamma\delta - 4(q_U F - C - \beta\delta)]^{1/2}/2(\alpha_0 + \gamma\delta)^{1/2}$ is derived by explicitly solving equation (6) for λ and is assumed to be > 0.

2. Proof of Proposition 2

The exact expressions for comparative statics concerning the effect of δ on λ is given by $\partial\lambda/\partial\delta|_{\dot{\lambda}=0} = [\lambda(1-\lambda)\gamma - \beta]/(2\lambda - 1)\overline{\alpha}$. Given the stability requirement $\lambda > 1/2$, the denominator is always positive (resp., negative) at λ_S (resp., λ_T), since $\lambda_S = 1/2 + \varepsilon$ and $\lambda_S = 1/2 - \varepsilon$, where $\varepsilon > 0$—see the Proof of Proposition 1. Hence, the sign of $\partial\lambda_S/\partial\delta$ (resp., $\partial\lambda_T/\partial\delta$) can be studied by imposing $\lambda_S(1-\lambda_S)\gamma - \beta > 0$ (resp., $\lambda_T(1-\lambda_T)\gamma - \beta < 0$) and solving for λ_S (resp., λ_T). The rest of the proof follows from the fact that $\lambda_S(1-\lambda_S)\gamma - \beta > 0$ if $\tilde{\lambda} < \lambda_S < \widehat{\lambda}$ and $\gamma > 4\beta$, while $\lambda_T(1-\lambda_T)\gamma - \beta < 0$ always if $\beta \geq \gamma/4$ or if $\lambda_T < \tilde{\lambda}$ or $\lambda_T > \widehat{\lambda}$ and $\gamma > 4\beta$.

3. Proof of Proposition 3

When the argument of the first order condition in equation (6) is non-negative, the provider collects, processes and monetizes a positive amount of its subscribers' information. Denote $\overline{q_P}$ as the cutoff value of q_P for which $\delta \geq 0$. Similarly, when $\lambda_T < \lambda \leq 1$, the initial share of litigators is large enough for the game to reach the litigation stage (so that $\lambda_S > 0$). Denote $\overline{q_U}$ as the cutoff value of q_U which satisfies $\lambda_T < \lambda$.

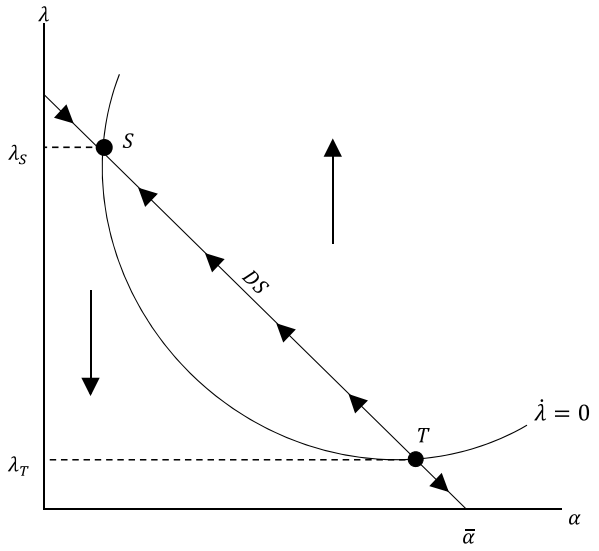

Fig. 1. Multiple equilibria of litigation.

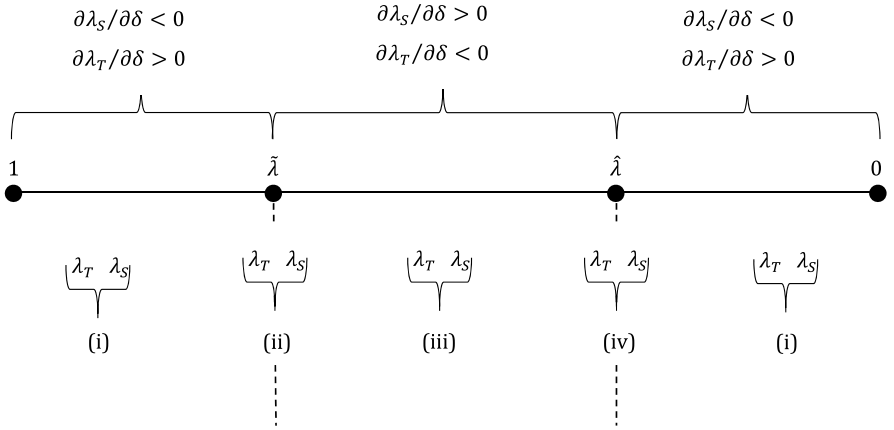

Fig. 2. Effects of δ on λ_S and λ_T when $\gamma > 4\beta$.

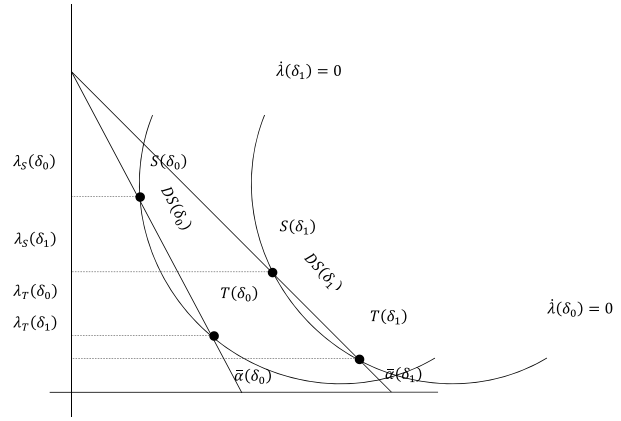

Fig. 3. Diagram of case (iv) of Proposition 2.

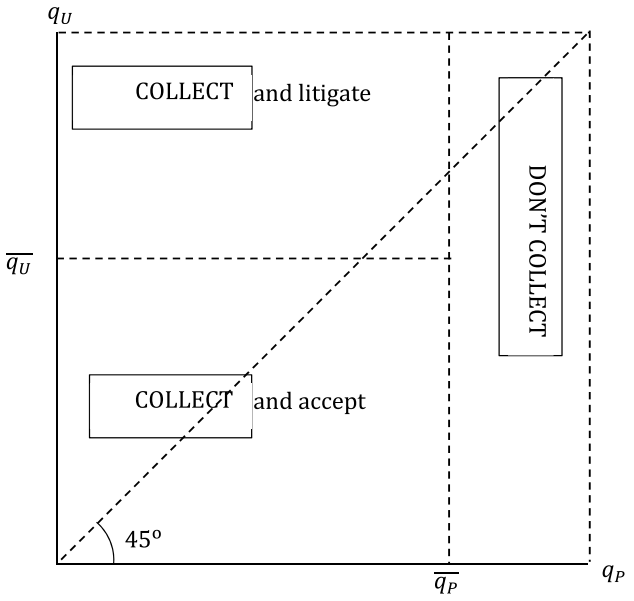

Fig. 4. The role of institutional incompleteness.

References

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347, 509–514.
Akerlof, G.A., 1980. A theory of social custom, of which unemployment may be one consequence. Q. J. Econ. 94, 749.
Antoci, A., Sabatini, F., Sodini, M., 2012. See you on Facebook! A framework for analyzing the role of computer-mediated interaction in the evolution of social capital. J. Soc. Econ. 41, 541–547.
Balkin, J.M., 2004. Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, vol. 79. New York University Law Review, pp. 1–55.
Ballon, I.C., 2016. Cyber boot camp: data security at the intersection of law and business. In: E-Commerce and Internet Law: A Legal Treatise with Forms. Thomson Reuters.
Ben-Shahar, O., 2009. The Myth of the opportunity to read in contract law. Eur. Rev. Contract Law 5, 1–28.
Booth, A.L., 1985. The free rider problem and a social custom model of trade union membership. Q. J. Econ. 100 (1), 253–261.
Burke, M., Marlow, C., Lento, T., 2010. Social network activity and social well-being. In: ACM CHI 2010: Conference on Human Factors in Computing Systems, pp. 1909–1912.

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., Viljoen, S., 2020. The chilling effects of algorithmic profiling: mapping the issues. Comput. Law Secur. Rep. 36 (10), 53–67.
Bygrave, L.A., 2015. Internet Governance by Contract. Oxford University Press, Oxford.
Chander, A., 2012. Facebookistan, vol. 90. North Carolina Law Review, pp. 1807–1844.
Chander, A., 2014. How law made silicon valley. Emory Law J. 63, 639–694.
Chang, J., Lai, C., 1999. Carrots or sticks? A social custom viewpoint on worker effort. Eur. J. Polit. Econ. 15, 297–310.
Chang, J., Lai, C., 2002. Is the efficiency wage efficient? The social norm and organizational corruption. Scand. J. Econ. 104 (1), 27–47.
Cherednychenko, O.O., 2016. The Impact of fundamental rights. In: Twigg-Flesner (Ed.), Research Handbook on EU Consumer and Contract Law. Edward Elgar Publishing, Cheltenham, Uk, pp. 109–137.
Chitkara, R., Gloger, M., McCaffrey, M., 2018. Technology Trends 2018–19. Address the risks and disruptive potential of products and services. PriceWaterhouseCooper.
Collingridge, D., 1980. The Social Control of Technology. St. Martin's Press, New York (London: Pinter).
Covello, V.T., Johnson, B.B. (Eds.), 1987. The Social and Cultural Construction of Risk. Springer, Berlin.
DeMarco, J.V., Fox, B.A., 2019. Data rights and data wrongs: civil litigation and the new privacy norms. Yale Law J. Forum 1, 1016–1028.
Ellison, N.B., Gray, R., Lampe, C., Stutzman, F., Vitak, J., 2012. Privacy in interaction: exploring disclosure and social capital in Facebook. In: Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media, pp. 330–337.
Ellison, N.B., Steinfield, C., Lampe, C., 2007. The benefits of Facebook "friends:" social capital and college students' use of online social network sites. J. Computer-Mediated Commun. 12, 1143–1168.
European Data Protection Supervisor (EDPS), 26 March 2014. Privacy and competitiveness in the age of big data: the interplay between data protection, competition law, and consumer protection in the digital economy. Preliminary Opinion.
Fuchs, et al., 2017. When risks cannot be seen: regulating uncertainty in emerging technologies. Res. Pol. 46 (7), 1215–1233.
Graham-Harrison, E., Cadwalladr, C., 2018. Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach (The Guardian).
Hayek, F., 1945. The use of knowledge in society. Am. Econ. Rev. 35 (4), 519–530.
Hermstrüwer, Y., Dickertb, S., 2017. Sharing is daring: an experiment on consent, chilling effects and a salient privacy nudge. Int. Rev. Law Econ. 51, 38–49.
Hijmans, H., 2016. The European Union as Guardian of Internet Privacy. Springer International Publishing, Berlin.
Hoffmann, A.L., Proferes, N., Zimmer, M., 2018. "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. New Media Soc. 20 (1), 199–218.
Horton, M., 1999. The internet and the empowered consumer: from the scarcity of the commodity to the multiplicity of subjectivity. Media Int. Aust. Inc. Cult. Policy 91, 111–123.
Ichino, A., Polo, M., Rettore, E., 2003. Are judges biased by labor market conditions? Eur. Econ. Rev. 47, 913–944.
Johnson, D.R., Post, G.D., 1996. Law and borders: the rise of law in cyberspace. Stanford Law Rev. 48, 1367–1402.
Jolls, C., 2013. Privacy and consent over time: the role of agreement in fourth amendment analysis. William Mary Law Rev. 54, 1693–1714.
Klonick, K., 2017. The new governors: the people, rules, and processes governing online Speech. Harv. Law Rev. 131, 1598–1670.
Kuran, T., 1989. Sparks and praise fires: a theory of unanticipated revolutions. Publ. Choice 61 (1), 41–74.
Lessing, L., 1997. Reading the constitution in the cyberspace. Emory Law J. 45, 869–886.
Miller, C.C., 2012. F.T.C. Fines Google $22.5 Million for Safari Privacy Violations (The New York Times).
Myles, G.D., Naylor, R., 1996. Social norms and conditional cooperative taxpayers. Eur. J. Polit. Econ. 12 (1), 49–66.
Naylor, R., 1990. A social custom model of collective actions. Eur. J. Polit. Econ. 6, 201–216.
Organization for Economic Cooperation and Development (OECD), October 2014. Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report.
Park, N., Kee, K.F., Valenzuela, S., 2009. Is there social capital in a social network site? Facebook use and college students' life satisfaction, trust, and participation. J. Computer-Mediated Commun. 14 (4), 875–901.
Posner, R.A., 1981. The economics of privacy. Am. Econ. Rev. 71, 405–409.
Rubinstein, I.R., Good, N., 2013. Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents. Berk. Technol. Law J. 28, 1333–1413.
Saint, N., 2010. Google Settles over Busg, Will Establish $8.5 Million Fund to Promote Education. Business Insider.
Schudy, S., Utikal, V., 2015. You Must Not Know about Me. On the Willingness to Share Personal Data, pp. 1–37. Munich Discussion Paper No. 2015-15.
Sloan, R.H., Warner, R., 2014. Beyond notice and choice: privacy, norms, and consent. J. High Technol. Law 14, 370–412.
Srinivasan, D., 2019. The Antitrust Case against Facebook: a Monopolist Journey towards pervasive surveillance in spite of consumers' preference for privacy. Berkeley Bus. Law J. 16, 39–101.
Stallings, R.A., 1980. Media discourse and the social construction of risk. Soc. Probl. 37 (1), 80–95.
Steinrötter, B., 2020. The (envisaged) Legal Framework for Commercialisation of digital data within the EU. In: Ebers, M., Navas, S. (Eds.), Algorithms and Law. Cambridge University Press, Cambridge, pp. 269–297.
Stigler, G.J., 1980. An introduction to privacy in economics and politics. J. Leg. Stud. 9, 623–644.
Stucke, M.E., Grunes, A.P., 2016. Big Data and Competition Policy. Oxford university press, Oxford.
Tene, O., Polonetsky, J., 2014. A theory of creepy: technology, privacy and shifting social norms. Yale J. Law and Technol. 16, 59–102.
Waldfogel, J., 1998. Reconciling asymmetric information and divergent expectations theories of litigation. J. Law Econ. 41, 451–476.
Willis, L., 2014. Why not privacy by default? Berk. Technol. Law J. 29, 61–134.
Wu, T., 2010. Is internet exceptionalism dead? In: Szoka, B., Marcus, A. (Eds.), The Next Digital Decade: Essays on the Future of the Internet. TechFreedom, Washington.